2 Anneaux

2.1 Généralités

2.1 Définition. Un anneau est un ensemble A muni de deux lois : la première s'appelle en général l'addition et est notée $+$; la deuxième s'appelle en général la multiplication et est notée $(x, y) \mapsto xy$. On suppose que :

- Muni de l'addition A est un groupe abélien ; son élément neutre est noté en général 0 ou 0_A en cas d'ambiguïté ; le symétrique d'un élément $x \in A$ pour $+$ s'appelle l'opposé de x et se note $-x$.
- La multiplication est associative et possède un élément neutre, en général noté 1 ou 1_A en cas d'ambiguïté.
- La multiplication est distributive par rapport à l'addition : pour tout $a, b, c \in A$, on a $a(b+c) = ab+ac$ et $(a + b)c = ac + bc$.
  Lorsque la multiplication est aussi commutative, on dit que l'anneau A est abélien ou commutatif.

2.2 Exemples. a) Munis des opérations (addition et multiplication) usuelles, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs, ainsi que l'anneau $K[X]$ des polynômes sur un corps (ou un anneau) commutatif K.

b) L'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$, muni de l'addition et de la multiplication des matrices est un anneau non commutatif pour $n \geqslant 2$.

Si A et B sont deux anneaux, une application $f : A \to B$ est appelée un *homomorphisme (ou morphisme) d'anneaux* si pour tout $x, y \in A$ on a $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ et si $f(1_A) = 1_B$. (Remarquons qu'on a automatiquement $f(0_A) = 0_B$).

Soient A un anneau et $x \in A$. On définit nx pour $n \in \mathbb{Z}$ en posant $0x = 0$, $1x = x$, puis, pour tout $n \in \mathbb{N}$, $(n + 1)x = (xn) + x$; enfin pour n négatif $nx = -\big((-n)x\big)$. L'application $n \mapsto nx$ est un homomorphisme de groupes de $(\mathbb{Z}, +)$ dans $(A, +)$.

L'élément $n1_A$ se note parfois n même lorsque ce morphisme n'est pas injectif.

On définit de même x^n pour $x \in A$ et $n \in \mathbb{N}$: on pose $x^0 = 1_A$, $x^1 = x$ puis $x^{n+1} = x^n x (= xx^n)$.

2.3 Formule du binôme. Soient A un anneau et $a, b \in A$ deux éléments *permutables* - *i.e.* tels que $ab = ba$. Alors, pour tout $n \in \mathbb{N}$, on a

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

C'est faux si $ab \neq ba$. Par exemple $(a + b)^2 = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2$.

2.4 Définition. Soit A un anneau. Un élément $a \in A$ est dit *inversible* (on dit parfois une unité de A) s'il existe a' dans A (nécessairement unique) tel que $a'a = aa' = 1_A$. Si a est inversible, l'élément a' tel que $a'a = aa' = 1_A$ s'appelle l'inverse de a et se note a^{-1}.

2.5 Proposition. *L'ensemble (noté parfois A^{-1}) des éléments inversibles de A est un groupe pour la multiplication.*

2.6 Définition. Un corps est un anneau K tel que $K^{-1} = K - \{0_K\}$.

2.7 Exercice. Soient A un anneau et $a \in A$. Démontrer que a est inversible si et seulement si l'application $b \mapsto ab$ est bijective de A dans A.

2.2 Anneaux intègres ; anneaux principaux

Dans la suite, tous les anneaux seront supposés commutatifs.

2.8 Définition. On dit qu'un anneau commutatif A est *intègre* si le produit de deux éléments non nuls de A est non nul.

2.9 Division ; éléments associés. Dans un anneau commutatif intègre, on peut définir la divisibilité comme dans $\mathbb{Z}$. On dit que a divise b et on écrit $a|b$ s'il existe c (*nécessairement unique* si a n'est pas nul) tel que $b = ac$. Autrement dit $a|b$ si $b \in aA$.

On dira que deux éléments a et b de A sont *associés* si $a|b$ et $b|a$, c'est à dire s'il existe $u \in A$ inversible tel que $a = ub$.

Le sous-ensemble aA de A est un sous-groupe de A. Mais contrairement au cas de $\mathbb{Z}$, les sous-groupes de A sont loin d'être en général tous de cette forme.

2.10 Définition. Soit A un anneau commutatif. On appelle *idéal* de A une partie I de A qui est un sous-groupe de $(A, +)$ et telle que, pour tout $a \in A$ et tout $x \in I$ on ait $ax \in I$.

A un idéal on peut encore associer une relation d'équivalence et définir un anneau quotient :

2.11 Proposition. *Soient A un anneau commutatif et I un idéal dans A. La relation R définie sur A par $a\,R\,b$ si $b - a \in I$ est une relation d'équivalence.*

2.12 Définition. Soient A un anneau commutatif et I un idéal dans A. On note A/I le *quotient d'équivalence* pour la relation R.

2.13 Proposition. *Soient A un anneau commutatif et I un idéal dans A. L'addition et la multiplication de A passent au quotient et définissent une structure d'anneau sur A/I.*

En effet, si $a, b \in A$ et $x, y \in I$, alors $(a+x)+(b+y)\,R\,a+b$ et $(a+x)(b+y) = ab+(ay+x(b+y))\,R\,ab$.

2.14 A retenir. a) Si I est un idéal d'un anneau (commutatif) A, on peut construire un anneau A/I et un homomorphisme surjectif d'anneaux $\pi : A \to A/I$ de noyau I.

b) Inversement, le noyau d'un homomorphisme d'anneaux $\pi : A \to B$ est un idéal.

Pour $a \in A$, l'ensemble aA est un idéal de A. On l'appelle l'idéal principal associé à a.

2.15 Définition. On dit qu'un anneau commutatif est *principal* s'il est intègre et tous ses idéaux sont principaux.

Un idéal étant en particulier un sous-groupe, l'anneau $\mathbb{Z}$ est principal. Nous verrons que si K est un corps commutatif, l'anneau $K[X]$ des polynômes à coefficients dans K est aussi un anneau principal. D'autres exemples d'anneaux principaux et d'anneaux intègres non principaux seront donnés plus bas.

Dans un anneau principal, la division se comporte essentiellement comme dans $\mathbb{Z}$.

2.16 Théorème. *Soient A un anneau principal et $a, b \in A$.*

a) *Il existe un élément $m \in A$ tel que $aA \cap bA = mA$. L'élément m est un multiple commun de a et de b. Les multiples communs de a et b sont les multiples de m.*

b) *Il existe un élément $d \in A$ tel que $aA + bA = dA$. L'élément d est un diviseur commun de a et de b. Les diviseurs communs de a et b sont les diviseurs de d.*

2.17 Définition. L'élément d de ce théorème s'appelle un plus grand commun diviseur (PGCD) de a et b. L'élément m s'appelle un plus petit commun multiple (PPCM) de a et b.

Un *PGCD* de a et de b n'est en général pas unique : il est unique à multiplication par un élément inversible de A près. On a fait un choix dans $\mathbb{Z}$ en les prenant dans $\mathbb{N}$ ce qui les a rendus uniques. On fait un tel choix aussi dans $K[X]$, mais il n'y a pas en général un choix « meilleur que les autres ».

Comme dans le cas de $\mathbb{Z}$, on peut définir la notion d'éléments premiers entre eux : leurs seuls diviseurs communs sont les éléments inversibles. Alors 1_A est un PGCD, *i.e.* $aA+bA = A$. On a donc le théorème de Bézout dans ce cadre, dont découle le théorème de Gauss :

2.18 Théorème de Bézout. *Soit A un anneau principal. Soient $a, b \in A$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in A$ tels que $au + bv = 1$.*

2.19 Théorème de Gauss. *Soit A un anneau principal. Soient $a, b, c \in A$. Si a divise bc et est premier à b, alors a divise c.*

Le rôle des nombres premiers est ici joué par les éléments irréductibles.

2.20 Définition. Soit A un anneau intègre. Un élément $a \in A$ est dit *irréductible* s'il n'est pas inversible et dans toute décomposition $a = bc$ un des deux facteurs b ou c est inversible.

2.21 Proposition. *Soient A un anneau principal et $a \in A$ non nul. Alors a est irréductible si et seulement si l'anneau quotient A/aA est un corps.*

Pour établir la décomposition en produit d'éléments irréductibles dans un anneau principal, la difficulté est de démontrer que tout élément non nul et non inversible possède un diviseur irréductible, et qu'il n'en possède qu'un nombre fini. Nous esquissons une preuve ci-dessous :

2.22 Lemme. a) *Soit A un anneau principal. Toute suite croissante d'idéaux de A stationne.*

b) *Toute suite décroissante d'idéaux d'intersection non nulle stationne.*

Démonstration. Soit I_n une suite d'idéaux de A.

a) On suppose que la suite I_n est croissante, c'est à dire que, pour $k, \ell \in \mathbb{N}$ avec $k \leqslant \ell$, on a $I_k \subset I_\ell$. On veut démontrer qu'il existe n tel que, pour $k \geqslant \ell$ on a $I_k = I_n$.
Comme la suite I_n est croissante, on vérifie que la réunion des I_n est un idéal J de A.
Puisque A est principal, il existe $a \in A$ tel que $J = aA$. Alors $a \in J$ et il existe $n \in \mathbb{N}$ tel que $a \in I_n$ (par définition d'une réunion). On a alors $J = aA \subset I_n$ donc $J = I_n$ (puisque J est la réunion de I_k). Pour $k \geqslant n$, on a $I_n \subset I_k \subset J = I_n$.

b) On suppose que la suite I_n est décroissante, c'est à dire que, pour $k, \ell \in \mathbb{N}$ avec $k \leqslant \ell$, on a $I_k \supset I_\ell$. Soit a un élément non nul de l'intersection $\bigcap_{k\in\mathbb{N}} I_k$. Pour $k \in \mathbb{N}$, il existe b_k tel que $I_k = b_k A$ (A étant principal). Comme $a \in I_k$, il existe $c_k \in A$ tel que $b_k c_k = a$. Pour $k \leqslant \ell$, on a $I_k \supset I_\ell$, de sorte que $b_k \in I_\ell$: il existe $x \in A$ tel que $b_k = x b_\ell$. Comme $b_k c_k = a = b_\ell c_\ell$, il vient $x c_k = c_\ell$, soit $c_k | c_\ell$. Posons $J_k = c_k A$. La suite J_k est croissante, donc stationne d'après a). Il existe donc n tel que, pour $k \geqslant n$ on ait $J_k = J_n$. Pour $k \geqslant n$, on a $c_k \in J_n$, donc il existe $y \in A$ tel que $c_k = y c_n$; comme $b_k c_k = a = b_n c_n$ il vient $b_n = y b_k$, donc $I_n \subset I_k$, et l'on a l'égalité.

□

2.23 Théorème. *Soient A un anneau principal et $a \in A$ un élément non nul et non inversible.*

a) *Il existe un élément irréductible $p \in A$ tel que $p|a$.*

b) *Il existe un ensemble fini F d'éléments irréductibles de A tels que tout élément irréductible de A qui divise a est associé à un élément de F ; pour tout irréductible p, il existe $n \in \mathbb{N}$ tel que $p^n \not| a$.*

Une fois ce théorème établi, on en déduit immédiatement l'existence de la décomposition en facteurs irréductibles. L'unicité est plus difficile à énoncer mais se démontre comme dans le cas de $\mathbb{Z}$:

2.24 Théorème. *Soient A un anneau principal et $a \in A$ un élément non nul et non inversible. Il existe un entier $n \geqslant 1$ et des éléments irréductibles $p_1, \ldots, p_n \in A$ tels que $a = \prod_{j=1}^{n} p_j$. Cette décomposition est unique à l'ordre des facteurs près : si $a = \prod_{j=1}^{n} p_j = \prod_{j=1}^{m} q_j$, alors $n = m$ et il existe $\sigma \in \mathfrak{S}_n$, i.e. une bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ telle que p_j soit associé à $q_{\sigma(j)}$ (pour tout j).*

2.3 Anneaux euclidiens

Les anneaux euclidiens sont ceux pour lesquels on dispose d'une division euclidienne. La même preuve que pour $\mathbb{Z}$ démontre qu'ils sont principaux. De plus, dans un anneau euclidien, comme dans $\mathbb{Z}$, on peut calculer le PGCD, écrire une relation de Bézout, résoudre des équations diophantiennes ou de congruence, *etc.* de façon algorithmique.

2.25 Définition. Soit A un anneau commutatif et intègre. On dit que A est *euclidien* s'il existe une application $v : A - \{0\} \to \mathbb{N}$, - appelée *stathme euclidien* telle que pour tous $a, b \in A - \{0\}$ il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

2.26 Remarque. En général, on demande de plus que, pour tous $a, b \in A - \{0\}$ tels que $a|b$ on ait $v(a) \leqslant v(b)$. Cette condition est en pratique toujours vérifiée, mais n'est pas utile dans ce qui suit. On peut démontrer que si A possède un stathme qui ne vérifie pas cette propriété, il en possède un qui la vérifie.

L'anneau $\mathbb{Z}$ est euclidien de stathme $a \mapsto |a|$. Nous verrons plus bas que l'anneau $K[X]$ est aussi euclidien : l'application qui à un polynôme associe son degré est un stathme euclidien sur $K[X]$.

2.27 Théorème. *Tout anneau euclidien est principal.*

Soit A un anneau euclidien ; notons v son stathme. Soit I un idéal non nul de A et $a \in I - \{0\}$ tel que $v(a) = \inf\{v(x);\ x \in I - \{0\}\}$. Puisque $a \in I$, on a $aA \subset I$. Soit x un élément de I ; écrivons $x = aq + r$, avec $q, r \in A$ et $r = 0$ ou $r \neq 0$ et $v(r) < v(a)$. Or $r = x - aq \in I$, et on ne peut avoir $r \neq 0$ et $v(r) < v(a)$ par définition de a. Il vient $r = 0$, donc $x \in aA$. Cela prouve que $I = aA$.

2.28 Remarque. Dans un anneau euclidien, comme pour le cas de $\mathbb{Z}$, on dispose de l'*algorithme d'Euclide* qui permet de calculer en pratique le plus grand commun diviseur de deux éléments.

2.29 Exemples d'anneaux euclidiens. Soit $\tau \in \mathbb{C} - \mathbb{R}$ un entier quadratique, *i.e.* tel qu'il existe $a, b \in \mathbb{Z}$ avec $\tau^2 + a\tau + b = 0$. Il est alors immédiat que l'ensemble $\mathbb{Z} + \tau\mathbb{Z} = \{m + n\tau;\ (m, n) \in \mathbb{Z}^2\}$ est un sous anneau - noté $\mathbb{Z}[\tau]$ de $\mathbb{C}$. Inversement, si $\mathbb{Z} + \tau\mathbb{Z}$ est un anneau, alors $\tau^2 \in \mathbb{Z} + \tau\mathbb{Z}$, donc τ est racine d'un polynôme $X^2 + aX + b$ avec $a, b \in \mathbb{Z}$.

Les racines du polynôme $X^2 + aX + b$ sont τ et $\overline{\tau}$, de sorte que $\tau + \overline{\tau} = -a$ et $\tau\overline{\tau} = b$. En particulier $\overline{\tau} = -a - \tau \in \mathbb{Z}[\tau]$.

Pour $x \in \mathbb{Z}[\tau]$, on a $\overline{x} \in \mathbb{Z}[\tau]$, donc $|x|^2 = \overline{x}x \in \mathbb{Z}[\tau] \cap \mathbb{R}_+ = \mathbb{N}$ (et, de même, $\overline{x} + x \in \mathbb{Z}[\tau] \cap \mathbb{R} = \mathbb{Z}$). Posons $v(x) = |x|^2$. Nous allons voir que *pour des valeurs très particulières* de τ, l'anneau $\mathbb{Z}[\tau]$ est euclidien de stathme v, et que dans d'autres cas, il n'est pas principal.

2.30 Proposition. *Un élément x de $\mathbb{Z}[\tau]$ est inversible si et seulement si $v(x) = 1$.*

Si $xy = 1$, on a $v(x)v(y) = |x|^2|y|^2 = 1$ donc $v(x)$ est inversible dans $\mathbb{N}$: $v(x) = 1$.

Si $v(x) = 1$ alors $x\overline{x} = 1$, donc x est inversible dans $\mathbb{Z}[\tau]$.

2.31 Lemme. *On suppose que $|\mathrm{Im}(\tau)| < \sqrt{3}$. Alors pour tout $z \in \mathbb{C}$, il existe $q \in \mathbb{Z}[\tau]$ tel que $|z - q| < 1$.*

Démonstration. Soit $n \in \mathbb{Z}$ l'entier le plus proche de $\dfrac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}$, de sorte que $|\mathrm{Im}(z-n\tau)| \leqslant \dfrac{|\mathrm{Im}(\tau)|}{2}$. Soit aussi m le nombre entier le plus proche de la partie réelle de $z-n\tau$, de sorte que $|\mathrm{Re}(z-n\tau-m)| \leqslant \dfrac{1}{2}$. Posons $q = m+n\tau$. On a $|\mathrm{Re}(z-q)| \leqslant \dfrac{1}{2}$ et $|\mathrm{Im}(z-q)| \leqslant \dfrac{|\mathrm{Im}(\tau)|}{2}$, donc $|z-q|^2 \leqslant \dfrac{1+\mathrm{Im}(\tau)^2}{4} < 1$. □

2.32 Théorème. *Si $|\mathrm{Im}(\tau)| < \sqrt{3}$, l'anneau $\mathbb{Z}[\tau]$ est euclidien de stathme $v : x \mapsto |x|^2$.*

Démonstration. Soient $a, b \in \mathbb{Z}[\tau] - \{0\}$; posons $z = \dfrac{a}{b}$ et soit $q \in \mathbb{Z}[\tau]$ tel que $|z-q| < 1$. Posons $r = a - bq$. On a $a = bq + r$ et $|r| = |b||z-q| < |b|$ donc $v(r) < v(b)$. □

2.33 Remarque. Sans changer l'anneau $\mathbb{Z}[\tau]$, on peut remplacer τ par $\overline{\tau}$, de sorte que l'on peut supposer que $\mathrm{Im}(\tau) > 0$; on peut aussi remplacer τ par $\tau + n$ (avec n dans $\mathbb{Z}$). On peut donc supposer que la partie réelle de τ est dans $[0, 1[$; comme $\tau + \overline{\tau} \in \mathbb{Z}$, on a $\tau + \overline{\tau} = 0$ ou 1. Cela nous ramène à étudier seulement le cas où τ est racine d'un polynôme $X^2 + b$, ou $X^2 - X + b$ (avec $b \in \mathbb{N}^*$). Dans le premier cas, $\tau = i\sqrt{b}$; dans le deuxième $\tau = \dfrac{1+i\sqrt{4b-1}}{2}$.
Le théorème s'applique donc uniquement dans les cinq cas suivants :

$$\tau \in \left\{ i, i\sqrt{2}, \frac{1+i\sqrt{3}}{2}, \frac{1+i\sqrt{7}}{2}, \frac{1+i\sqrt{11}}{2} \right\}.$$

2.34 Exercice. On veut démontrer que pour $\tau = i\sqrt{b}$ avec $b \geqslant 3$ et pour $\tau = \dfrac{1+i\sqrt{15}}{2}$, l'anneau $\mathbb{Z}[\tau]$ n'est pas principal. En utilisant les égalités :
- pour $\tau = i\sqrt{3}$, on a $(1+\tau)(1+\overline{\tau}) = 4 = 2 \times 2$;
- pour $\tau = 2i$ ou $\tau = \dfrac{1+i\sqrt{15}}{2}$, on a $\tau\overline{\tau} = 4 = 2 \times 2$;
- pour $\tau = i\sqrt{5}$, on a $(1+\tau)(1+\overline{\tau}) = 6 = 2 \times 3$;

démontrer que l'on n'a pas l'unicité dans la décomposition en éléments irréductibles. Pour $b \geqslant 5$, et $\tau = i\sqrt{b}$, écrire une égalité de ce style en discutant la parité de p. En déduire que $\mathbb{Z}[\tau]$ n'est pas principal.

Commentaire. On peut démontrer (relativement facilement... mais cela nous mènerait trop loin) que dans tous les autres cas, l'anneau $\mathbb{Z}[\tau]$ n'est pas euclidien. Cependant, il y a quelques cas où $\mathbb{Z}[\tau]$ est quand même principal. Cela se produit pour $\tau = \dfrac{1+i\sqrt{19}}{2}$.

2.35 L'équation diophantienne $x^2 + y^2 = z^2$. On cherche à trouver tous les triples $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$. Si (x, y, z) est une solution et $k \in \mathbb{Z}$, alors (kx, ky, kz) est aussi une solution. On peut donc supposer que (x, y, z) sont premiers entre eux. Si d divise x et y, alors d^2 divise z^2, donc d divise z. On peut donc supposer que x et y sont premiers entre eux. Remarquons que x et y ne peuvent être tous deux impairs car alors $x^2 \equiv y^2 \equiv 1$ [4], donc $z^2 \equiv 2$ [4] ce qui est impossible. Donc l'un des deux est pair et l'autre impair.

Dans ce cas, l'idéal $(x+iy)\mathbb{Z}[i] + (x-iy)\mathbb{Z}[i]$ de $\mathbb{Z}[i]$ contient $(x+iy) + (x-iy) = 2x$, ainsi que $i\big((x-iy) - (x+iy)\big) = 2y$ donc il contient 2. Or il existe $q \in \mathbb{Z}[i]$ tel que $(x+iy) - 2q$ soit égal à 1 ou à i. Cela prouve que $(x+iy)$ et $(x-iy)$ sont premiers entre eux. Décomposons $z^2 = (x+iy)(x-iy)$ en éléments irréductibles dans $\mathbb{Z}[i]$; puisque c'est un carré, chacun figure un nombre pair de fois. Cela prouve que $x+iy$ est associé à un carré : il existe $(a, b) \in \mathbb{Z}$, tels que $x+iy$ soit associé à $(a+ib)^2$ c'est à dire $x + iy = \pm(a+ib)^2$ (si y est pair) ou $x + iy = \pm i(a+ib)^2$ (si x est pair). On en déduit que les solutions sont nécessairement de la forme $(k(a^2-b^2), 2kab, k(a^2+b^2))$ ou $(2kab, k(a^2-b^2), k(a^2+b^2))$ (avec $a, b, k \in \mathbb{Z}$).

2.36 Proposition. *On suppose que $\mathbb{Z}[\tau]$ est principal. Soit q un élément irréductible de $\mathbb{Z}[\tau]$. Alors deux cas sont possibles :*
- *il existe un nombre premier $p \in \mathbb{N}$ tel que $v(q) = p$;*
- *il existe un nombre premier $p \in \mathbb{N}$ tel que q soit associé à p (et l'on a $v(q) = p^2$).*

Décomposons $v(q) = q\overline{q}$ en facteurs premiers dans $\mathbb{Z}$. C'est une décomposition dans $\mathbb{Z}[\tau]$ qui ne peut donc avoir que un ou deux éléments : dans le premier cas $v(q)$ est premier ; dans le deuxième un des facteurs p est associé à q, donc $v(q) = v(p) = p^2$.

Pour finir, signalons sans démonstration quels nombres premiers de $\mathbb{N}$ ne sont plus irréductibles dans $\mathbb{Z}[i]$.

2.37 Proposition. *Soit $p \in \mathbb{N}$ un nombre premier. Les assertions suivantes sont équivalentes :*

(i) *il existe $x, y \in \mathbb{Z}$ tels que $x^2 + y^2 = p$;*

(ii) *l'élément $p \in \mathbb{Z}[i]$ n'est pas irréductible dans $\mathbb{Z}[i]$;*

(iii) *-1 est un carré modulo p ;*

(iv) *$p \not\equiv 3$ [4].*

2.4 Sous-corps

2.4.1 Caractéristique d'un corps ; sous-corps premier

Soit K un corps. Tout morphisme f d'anneaux de K dans un anneau non nul est injectif : si $x \in K^*$, alors $f(x^{-1})f(x) = 1$, donc $f(x) \neq 0$.

Soit K un corps et $f : \mathbb{Z} \to K$ l'unique homomorphisme d'anneaux (défini par $f(n) = n1_K$). Le noyau de f est un idéal $n\mathbb{Z}$ de $\mathbb{Z}$. L'image $f(\mathbb{Z})$ est un sous-anneau commutatif de $\mathbb{K}$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Puisque K est un corps, $f(\mathbb{Z})$ est un anneau intègre, donc ou bien n est premier, ou bien f est injective. Ce nombre n s'appelle la *caractéristique* de K.

- Lorsque la caractéristique p n'est pas nulle, l'image $f(\mathbb{Z})$ est un sous-corps de K isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Lorsque f est injective, on peut étendre f en un homomorphisme $\tilde{f} : \mathbb{Q} \to K$ en posant $\tilde{f}\left(\dfrac{p}{q}\right) = f(p)f(q)^{-1}$ pour $p, q \in \mathbb{Z}$ avec $q \neq 0$. L'image $\tilde{f}(\mathbb{Q})$ est un sous-corps de K isomorphe à $\mathbb{Q}$.
- Le corps ainsi obtenu, isomorphe selon les cas à $\mathbb{Z}/p\mathbb{Z}$ ou à $\mathbb{Q}$ est le plus petit sous-corps de K. On l'appelle le *sous-corps premier* de K.

2.4.2 Corps des fractions d'un anneau intègre

Soit A un anneau commutatif intègre non nul. On définit un corps K contenant A. Sa construction est la généralisation de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$. Les éléments de K sont des fractions $\dfrac{a}{b}$ où $a \in A$ et $b \in A - \{0\}$. On peut alors dire quand deux fractions sont égales, définir l'addition et la multiplication des fractions, et vérifier que l'on obtient ainsi un corps qui contient l'anneau A.

Pour formaliser cela, considérons la relation R sur $A \times (A - \{0\})$ définie par $(a, b)\, R\, (c, d)$ si $ad = bc$. On vérifie sans peine que R est une relation d'équivalence. Notons K l'ensemble quotient. La classe dans K d'un élément $(a, b) \in A \times (A - \{0\})$ se note $\dfrac{a}{b}$.

On définit la somme et le produit d'éléments de K en posant pour des éléments a, b, c, d de A avec b, d non nuls

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Ces opérations sont bien définies : si $(a,b)\,R\,(a',b')$ et $(c,d)\,R\,(c',d')$, alors $(ad+bc,bd)\,R\,(a'd'+b'c',b'd')$ et $(ac,bd)\,R\,(a'c',b'd')$. De plus, on a

$$\frac{a}{d}+\frac{c}{d}=\frac{a+c}{d}$$

ce qui permet de démontrer facilement les règles des opérations : K est bien un anneau commutatif. De plus K est un corps : l'inverse de $\frac{a}{b}$ est $\frac{b}{a}$ (pour $a,b\in A-\{0\}$).

Le corps K s'appelle le *corps de fractions* de A.

Enfin, on plonge A dans K au moyen de l'application $a\mapsto\frac{a}{1}$: cette application est un morphisme injectif qui plonge l'anneau A dans K

2.38 Proposition. *Pour tout corps L et tout homomorphisme injectif $f:A\to L$, il existe un unique homomorphisme $\tilde{f}:K(A)\to L$ dont la restriction à $A\subset K(A)$ soit f*

2.4.3 Éléments algébriques, éléments transcendants

Soient L un corps commutatif et $K\subset L$ un sous-corps.

Soit $x\in L$. Considérons L comme espace vectoriel sur K et introduisons le sous-espace $K[x]\subset L$ engendré par les éléments x^n pour $n\in\mathbb{N}$. Cet espace est l'image de l'application $f:P\mapsto P(x)$ de $K[X]$ dans L. Cette application étant un homomorphisme d'anneaux, son noyau est un idéal de l'anneau principal $K[X]$. Il existe donc un polynôme $\varpi\in K[X]$ tel que $\ker f=\varpi K[X]$. Deux cas sont possibles :

a) Si $\varpi=0$, l'application $f:P\mapsto P(x)$ est injective de $K[X]$ dans L. On dit alors que x est *transcendant* sur K.

b) Si $\varpi\neq 0$. Remarquons que f n'est pas l'application nulle, donc ϖ n'est pas inversible ; si $\varpi=PQ$, on trouve $P(x)Q(x)=0$, ce qui implique que $P(x)=0$ ou $Q(x)=0$, *i.e.* l'un des deux est dans $\ker f$ donc multiple de ϖ. Il s'ensuit que ϖ est irréductible. On dit alors que x est *algébrique* sur K et le polynôme ϖ s'appelle le *polynôme minimal* de x.

Citons sans démonstration le résultat suivant :

2.39 Proposition. *Soient L un corps commutatif et $K\subset L$ un sous corps. Les éléments de L algébriques sur K forment un sous-corps de L.*

Cela signifie que la somme, le produit, l'inverse d'éléments algébriques est algébrique.

2.40 Proposition. *Le corps des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable.*

En effet, les éléments algébriques sont les racines de polynômes à coefficients rationnels (non nuls). Or $\mathbb{Q}$ étant dénombrable, l'ensemble des polynômes à coefficients rationnels est dénombrable, et chacun a un nombre fini de racines

On déduit de ce résultat qu'il y a « bien plus » de nombres transcendants que de nombres algébriques. On peut démontrer que les nombres e et π sont transcendants, mais ce n'est pas si facile.

2.5 Exercices

2.1 Exercice. *Le groupe $\mathbb{F}_p^*$ est cyclique. (1)*

1. Soit G un groupe commutatif fini.
   a) Soient $a,b\in G$. On note k_a et k_b leurs ordres respectifs. On suppose que k_a et k_b sont premiers entre eux. Démontrer que l'ordre de ab est k_ak_b.

b) Démontrer qu'il existe $n \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z};\ \forall x \in G;\ x^k = 1\} = n\mathbb{Z}$. Démontrer que n divise le cardinal de G.

Le nombre n s'appelle l'*exposant* de G.

c) Ecrivons $n = \prod p_j^{m_j}$ la décomposition de n en nombres premiers distincts. Démontrer que pour tout j, il existe $x_j \in G$ d'ordre $p_j^{m_j}$.

d) En déduire qu'il existe $x \in G$ d'ordre n.

2. Soit K un corps commutatif et G un sous-groupe fini à N éléments de K^*. Soit n son exposant.

a) Démontrer que l'équation $x^n = 1$ a au plus n solutions dans K. En déduire que $N \leqslant n$.

b) Démontrer que G est cyclique.

2.2 Exercice. *Le groupe $\mathbb{F}_p^*$ est cyclique. (2)*

1. Soit $n \in \mathbb{N}^*$. On considère l'ensemble $A_n = \left\{\frac{k}{n};\ k \in \mathbb{N},\ \ 0 \leqslant k < n\right\}$.

a) Soit d un diviseur de n. Combien d'éléments de A_n ont leur écriture irréductible de la forme $\frac{a}{d}$?

b) En déduire l'égalité $\sum_{d|n} \varphi(d) = n$.

2. Soit K un corps commutatif et G un sous-groupe fini à n éléments de K^*. Pour $d \in \mathbb{N}^*$, on note s_d le nombre d'éléments d'ordre d de G.

a) Démontrer que $\sum_{d|n} s_d = n$.

b) Soit $x \in G$; notons d son ordre et H le sous-groupe (cyclique) de G engendré par x. Démontrer que
- H a d éléments et $\varphi(d)$ éléments d'ordre d.
- Tout élément $y \in H$ vérifie $y^d = 1$.
- L'équation $y^d = 1$ a au plus d solutions dans K.
- Tout élément d'ordre d de G est dans H.

c) En déduire que si $s_d \neq 0$, alors $s_d = \varphi(d)$.

d) En déduire que pour tout diviseur d de n on a $s_d = \varphi(d)$, puis que G est cyclique.

2.3 Exercice. *Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est-il cyclique ?* Perrin, *Cours d'algèbre* p.24.

Cet exercice complète les précédents.

1. a) Soient G et H deux groupes commutatifs finis. Démontrer que $G \times H$ est cyclique si et seulement si G et H sont cycliques et que leurs ordres sont premiers entre eux.

b) Quels sont les nombres n tels que $\varphi(n)$ soit impair ?

c) Soient m et n deux nombres entiers premiers entre eux distincts de 1 et de 2. Démontrer que $(\mathbb{Z}/nm\mathbb{Z})^*$ n'est pas cyclique.

d) $\mathbb{Z}/8\mathbb{Z}^*$ est-il cyclique ?

2. Soient p un nombre premier distinct de 2 et $n \in \mathbb{N}$, $n \geqslant 2$.

a) Démontrer (par récurrence) que, pour tout $k \in \mathbb{N}$, $(1+p)^{p^k} \equiv 1 + p^{k+1}\ \ [p^{k+2}]$.

b) Quel est l'ordre de $1 + p$ dans le groupe $\mathbb{Z}/p^n\mathbb{Z}^*$?

c) Soit $a \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ engendre $\mathbb{Z}/p\mathbb{Z}^*$, et soit $x \in \mathbb{Z}/p^n\mathbb{Z}^*$ la classe de a. Démontrer que l'ordre de x dans $\mathbb{Z}/p^n\mathbb{Z}^*$ est un multiple de $p - 1$. En déduire qu'il existe dans $\mathbb{Z}/p\mathbb{Z}$ un élément d'ordre $p - 1$.

d) Démontrer que $\mathbb{Z}/p^n\mathbb{Z}^*$ est cyclique. Démontrer que $\mathbb{Z}/2p^n\mathbb{Z}^*$ est aussi cyclique.

3. Quels sont les entiers n tels que $\mathbb{Z}/n\mathbb{Z}^*$ soit cyclique ?

2.4 Exercice. Soit $a \in \mathbb{N}^*$ et $\tau \in \mathbb{C}$ une racine du polynôme $X^2 + X + a$. On note $\mathbb{Z}[\tau]$ l'anneau $\mathbb{Z} + \tau\mathbb{Z}$.

1. a) Soit $x \in \mathbb{Z}[\tau]$ non nul. Démontrer que $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est fini. Notons $n(x)$ le nombre de ses éléments.

   b) Soient $x, y \in \mathbb{Z}[\tau]$ non nuls. Donnons nous des représentants $r_1, \ldots, r_n$ des classes d'éléments de $\mathbb{Z}[\tau]$ modulo x et des représentants $s_1, \ldots, s_m$ des classes d'éléments de $\mathbb{Z}[\tau]$ modulo y. Démontrer que tout élément de $\mathbb{Z}[\tau]$ est congru modulo xy à un un et un seul élément de la forme $r_i + xs_j$. En déduire que $v(xy) = v(x)v(y)$.

   c) En calculant $v(k)$ pour $k \in \mathbb{Z}$, démontrer que, pour tout $x \in \mathbb{Z}[\tau]$ non nul, on a $v(x) = |x|^2$.

2. On suppose que $\mathbb{Z}[\tau]$ possède un stathme euclidien V.

   a) On suppose aussi que les seuls éléments inversibles de $\mathbb{Z}[\tau]$ sont ± 1. Soit $x \in \mathbb{Z}[\tau]$ non nul et non inversible de stathme minimal. Démontrer que tout élément de $\mathbb{Z}[\tau]$ est congru modulo x à $0, 1$ ou -1 ; en déduire que $v(x) \leqslant 3$.

   b) Démontrer que $\operatorname{Im} \tau \leqslant \sqrt{3}$.

2.5 Exercice. *Sous-groupes de* $\mathbb{Z}[\tau]$. Soit G un sous-groupe non nul de $\mathbb{Z}[\tau]$. Soit $\alpha \in G$ un élément non nul tel que $v(\alpha)$ soit minimal dans $\{v(x);\ x \in G \setminus \{0\}\}$. (Un tel élément existe d'après le « principe de récurrence »- puisque $v(x) \in \mathbb{N}$ pour tout $x \in \mathbb{Z}[\tau]$).

1. Démontrer que $G \cap \mathbb{R}\alpha = \mathbb{Z}\alpha$.
   On suppose désormais que $G \not\subset \mathbb{R}\alpha$. Soit $\beta \in G \setminus \mathbb{Z}\alpha$ tel que $v(\beta)$ soit minimal dans $\{v(x);\ x \in G \setminus \mathbb{Z}\alpha\}$. Quitte à remplacer β par $-\beta$, on peut supposer que $\operatorname{Im} \dfrac{\beta}{\alpha} > 0$.
2. Démontrer que $\left|\dfrac{\beta}{\alpha}\right| \geqslant 1$ et $\left|\operatorname{Re} \dfrac{\beta}{\alpha}\right| \leqslant \dfrac{1}{2}$.
3. Soit $x \in G$. Démontrer qu'il existe $m, n \in \mathbb{Z}$ tels que

$$\left|\operatorname{Im} \frac{x - n\beta}{\alpha}\right| \leqslant \frac{1}{2}\operatorname{Im} \frac{\beta}{\alpha} \quad \text{et} \quad \left|\operatorname{Re} \frac{x - (m\alpha + n\beta)}{\alpha}\right| \leqslant \frac{1}{2}.$$

   En déduire que $|x - (m\alpha + n\beta)| < |\beta|$, puis que $x = m\alpha + n\beta$.
   Il s'ensuit que $G = \alpha\mathbb{Z} + \beta\mathbb{Z}$.

2.6 Exercice. *Un anneau principal non euclidien*

Le but de cet exercice est de démontrer que pour $\tau = \dfrac{1 + i\sqrt{19}}{2}$, l'anneau $\mathbb{Z}[\tau]$ est principal mais n'est pas euclidien. Soit J un idéal non nul de $\mathbb{Z}[\tau]$. Puisque J est un sous-groupe de $\mathbb{Z}[\tau]$, il existe d'après l'exercice 2.5 $\alpha, \beta \in \mathbb{Z}[\tau]$ tels que

$$\operatorname{Im} \frac{\beta}{\alpha} > 0, \quad \left|\frac{\beta}{\alpha}\right| \geqslant 1, \quad \left|\operatorname{Re} \frac{\beta}{\alpha}\right| \leqslant \frac{1}{2} \quad \text{et} \quad G = \alpha\mathbb{Z} + \beta\mathbb{Z}$$

(remarquons que $\tau\alpha \in J$, donc $J \not\subset \mathbb{R}\alpha$).

1. Démontrer qu'il existe $a, b, c, d \in \mathbb{Z}$ tels que $\tau\alpha = a\alpha + b\beta$ et $\tau\beta = c\alpha + d\beta$.
2. En regardant les signes des parties imaginaires de τ et $\dfrac{\beta}{\alpha}$, démontrer que $b > 0$.
3. Quelles sont les valeurs propres et espaces propres de la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$? Démontrer que $a + d = 1$ et $ad - bc = 5$. En déduire que $ad \leqslant 0$, que ad est pair, que $bc < 0$, que b et c sont impairs et que $4bc + (a - d)^2 = -19$.

4. Posons $x = \dfrac{\beta}{\alpha}$. Démontrer que $\begin{vmatrix} a+bx & 1 \\ c+dx & x \end{vmatrix} = 0$. En déduire que
   a) x et $\overline{x}$ sont racines du polynôme $bX^2 + (a-d)X - c$,
   b) $|x|^2 = -\dfrac{c}{b}$ et $\operatorname{Re} x = \dfrac{d-a}{2b}$.
5. Démontrer que $|a-d| \leqslant b$ et $b \leqslant -c$. En déduire que $3b^2 \leqslant 19$, puis que $b = 1$.
6. En déduire que $(\alpha, \tau\alpha)$ est une $\mathbb{Z}$-base de J et conclure.

On démontre de même que pour $D \in \{19, 43, 67, 163\}$, l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{D}}{2}\right]$ est principal.

2.7 Exercice. Démontrons que pour $\tau = i\sqrt{b}$ avec $b \geqslant 3$ et pour $\tau = \dfrac{1+i\sqrt{15}}{2}$, l'anneau $\mathbb{Z}[\tau]$ n'est pas principal. En utilisant les égalités :
- pour $\tau = i\sqrt{3}$, on a $(1+\tau)(1+\overline{\tau}) = 4 = 2 \times 2$;
- pour $\tau = 2i$ ou $\tau = \dfrac{1+i\sqrt{15}}{2}$, on a $\tau\overline{\tau} = 4 = 2 \times 2$;
- pour $\tau = i\sqrt{5}$, on a $(1+\tau)(1+\overline{\tau}) = 6 = 2 \times 3$;

démontrer que l'on n'a pas l'unicité dans la décomposition en éléments irréductibles. Pour $b \geqslant 5$, et $\tau = i\sqrt{b}$, écrire une égalité de ce style en discutant la parité de p. En déduire que $\mathbb{Z}[\tau]$ n'est pas principal.

2.8 Exercice. Soient L un corps commutatif et $K \subset L$ un sous-corps. Remarquons que L est un espace vectoriel sur K et que tout sous-anneau de L contenant K est un sous-K-espace vectoriel de L.

1. Soit K_1 un sous-corps de L contenant K. Démontrer que tout élément algébrique sur K est algébrique sur K_1.
2. Soit $x \in L$. Démontrer que x est algébrique sur K si et seulement s'il existe un sous-corps K_1 de L contenant K et x et qui soit un espace vectoriel de dimension finie sur K.
3. Soient K_1, K_2 des sous-corps de L tels que $K \subset K_1 \subset K_2$. Démontrer que K_2 est un K-espace vectoriel de dimension finie si et seulement si K_2 est un K-espace vectoriel de dimension finie et K_1 est un K-espace vectoriel de dimension finie, et que dans ce cas, on a $\dim_K(K_2) = \dim_{K_1}(K_2)\dim_K(K_1)$.
4. Soient $\alpha, \beta \in L$ des éléments algébriques sur K. Soit K_1 un sous-corps de L contenant K et α et de dimension finie sur K.
   a) On suppose que $\alpha \neq 0$. Démontrer que α^{-1} est algébrique sur K.
   b) Démontrer qu'un élément $x \in L$ est algébrique sur K si et seulement s'il est algébrique sur K_1.
   c) Démontrer que $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur K.
5. Démontrer que les éléments de L algébriques sur K forment un sous-corps de L.