Université de Bordeaux

Préparation à l'Agrégation interne
Révisions d'algèbre élémentaire

Olivier Brinon

Table des matières

1. Compléments sur les ensembles

1.1. Relations d'ordre et relations d'équivalence.

Définition 1.1.1. Soit X un ensemble.
(1) Une *relation d'ordre* sur X est une relation binaire $\leqslant$ sur X vérifiant les propriétés suivantes :
- $x \leqslant x$ (réflexivité) ;
- $(x \leqslant y \text{ et } y \leqslant x) \Rightarrow x = y$ (antisymétrie) ;
- $(x \leqslant y \text{ et } y \leqslant z) \Rightarrow x \leqslant z$ (transitivité).

pour tous $x, y, z \in X$. Le couple $(X, \leqslant)$ s'appelle un *ensemble ordonné*. Lorsque deux éléments quelconques de X sont comparables (c'est-à-dire $(\forall x, y \in X)\, x \leqslant y$ ou $y \leqslant x$), on dit que l'ordre est *total*. Si toute partie de X admet un plus petit élément (c'est-à-dire $(\forall A \subset X)\,(\exists a \in A)\,(\forall x \in A)\, a \leqslant x$), on dit que $\leqslant$ est un *bon ordre*. Un bon ordre est total, mais la réciproque est fausse en général.
(2) Une *relation d'équivalence* sur X est une relation binaire $\mathcal{R}$ sur X vérifiant les propriétés suivantes :
- $x\mathcal{R}x$ (réflexivité) ;
- $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ (symétrie) ;
- $(x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$ (transitivité).

pour tous $x, y, z \in X$. La *classe d'équivalence* de $x \in X$ est alors $[x] := \{y \in X\,;\, x\mathcal{R}y\}$. C'est une partie de X, et si $x_1, x_2 \in X$, alors on a $[x_1] = [x_2]$ ou $[x_1] \cap [x_2] = \varnothing$: les classes d'équivalence forment donc une partition de X. Notons que cette partition détermine entièrement $\mathcal{R}$: on a $x\mathcal{R}y \Leftrightarrow [x] = [y]$. L'*ensemble quotient* $X/\mathcal{R}$ est la partie de $\mathscr{P}(X)$ constituée par les classes d'équivalence. Si $A \in X/\mathcal{R}$, on a $A = [x]$ pour tout $x \in A$: un tel élément x s'appelle un *représentant* de A.

Notons qu'il est parfois commode d'identifier une relation d'équivalence $\mathcal{R}$ à l'ensemble

$$\{(x, y) \in X \times X\,;\, x\mathcal{R}y\} \subset X \times X$$

(*idem* pour les relations d'ordre). Par exemple la relation d'égalité correspond à la diagonale $\Delta_X \subset X \times X$. Prendre garde que toute partie de $X \times X$ ne définit pas une relation d'équivalence : il faut que les axiomes soient vérifiés (exercice : comprendre cette partie en termes de la partition associée).

Exemple 1.1.2. (1) Soit $f\colon X \to Y$ une application. On définit une relation d'équivalence $\mathcal{R}_f$ sur X en posant $x_1\mathcal{R}_f x_2 \Leftrightarrow f(x_1) = f(x_2)$. Par définition, les classes d'équivalence sont les préimages non vides des singletons.
(2) Soient G un groupe et $H \subset G$ un sous-groupe. On définit une relation d'équivalence sur G en posant $g_1\mathcal{R}g_2 \Leftrightarrow g_1^{-1}g_2 \in H$. Les classes d'équivalence sont les *classes à gauche* modulo H : ce sont les parties de la forme gH. Bien entendu, on définit de façon analogue les classes à droite[1].

Version du 15 juin 2022

1. Lorsque H n'est pas distingué dans G, les relations d'équivalence (et donc les partitions) associées ne coïncident pas.

Définition 1.1.3. Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble X, on dispose de la *surjection canonique*

$$\pi_{\mathcal{R}} \colon X \to X/\mathcal{R}$$
$$x \mapsto [x].$$

Un *système (complet) de représentants* est une partie $T \subset X$ telle que la restriction de $\pi_{\mathcal{R}}$ à T induise une bijection $T \xrightarrow{\sim} X/\mathcal{R}$. Cela signifie que pour tout $A \in X/\mathcal{R}$, il existe un unique $t \in T$ tel que $A = [t]$, *i.e.* tel que t soit un représentant de A. Dans ce cas, tout élément de X est équivalent à un unique élément de T.

Remarque. Si on accepte l'axiome du choix, il existe toujours un système de représentants.

Proposition 1.1.4. Soient $\mathcal{R}$ une relation d'équivalence sur un ensemble X et $f \colon X \to Y$ une application. Supposons que $x_1 \mathcal{R} x_2 \Rightarrow f(x_1) = f(x_2)$. Alors il existe une unique application $\widetilde{f} \colon X/\mathcal{R} \to Y$ telle que $f = \widetilde{f} \circ \pi_{\mathcal{R}}$.

Démonstration. Si $A \in X/\mathcal{R}$, il existe $x \in X$ tel que $A = [x]$: si $\widetilde{f}$ existe, on a nécessairement $\widetilde{f}(A) = f(x)$, ce qui montre l'unicité de $\widetilde{f}$. Pour l'existence, il suffit de vérifier que $f(x)$ ne dépend pas du choix du représentant x de A, ce qui résulte précisément de l'hypothèse sur f. □

Corollaire 1.1.5. (Décomposition canonique d'une application) Soit $f \colon X \to Y$ une application. Il existe une unique application $\widetilde{f} \colon X/\mathcal{R}_f \to f(X)$ telle que $f = \iota \circ \widetilde{f} \circ \pi_{\mathcal{R}_f}$ où $\iota \colon f(X) \hookrightarrow Y$ est l'inclusion. L'application $\widetilde{f}$ est bijective.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \pi_{\mathcal{R}_f}}\downarrow & & \uparrow{\scriptstyle \iota} \\ X/\mathcal{R}_f & \xrightarrow{\tilde{f}} & f(X) \end{array}$$

Démonstration. f se factorise uniquement en $f = \iota \circ g$ où $g \colon X \to f(X)$ est surjective. La proposition précédente appliquée à $\mathcal{R} = \mathcal{R}_f$ fournit alors une unique application $\widetilde{f} \colon X/\mathcal{R}_f \to f(X)$ telle que $f = \iota \circ \widetilde{f} \circ \pi_{\mathcal{R}_f}$. Si $x_1, x_2 \in X$ sont tels que $\widetilde{f}([x_1]) = \widetilde{f}([x_2])$, alors $f(x_1) = f(x_2)$ *i.e.* $x_1 \mathcal{R}_f x_2$ d'où $[x_1] = [x_2]$, ce qui montre que $\widetilde{f}$ est injective. Elle est surjective parce que g l'est. □

Proposition 1.1.6. Soit G un groupe (resp. A un anneau). Les relations d'équivalence sur G (resp. sur A) qui sont compatibles avec la loi de groupe (resp. d'anneau) sont les relations modulo un sous-groupe distingué (resp. un idéal bilatère).

Démonstration. Soit $\mathcal{R}$ une relation d'équivalence sur G. Notons H la classe d'équivalence de l'élément neutre et $\pi \colon G \to G/\mathcal{R}$ la surjection canonique. Supposons $\mathcal{R}$ compatible à la loi de groupe : cela implique que si $g_1, g_2 \in G$, la classe $\pi(g_1 g_2)$ ne dépend que des classes $\pi(g_1)$ et $\pi(g_2)$, et pas des représentants g_1 et g_2. Cela implique qu'on a une loi de composition interne bien définie sur $G/\mathcal{R}$, définie par $\pi(g_1) \cdot \pi(g_2) = \pi(g_1 g_2)$. Les propriétés de groupe « passent au quotient » (vérification immédiate) : l'ensemble quotient est muni d'une loi de groupe telle que π soit un morphisme de groupes. Cela implique déjà que $H := \mathsf{Ker}(\pi)$ est un sous-groupe distingué de G. Si $g_1, g_2 \in G$, on a alors $g_1 \mathcal{R} g_2 \Leftrightarrow \pi(g_1) = \pi(g_2) \Leftrightarrow g_1^{-1} g_2 \in \mathsf{Ker}(\pi) = H$ ce qui montre que $\mathcal{R}$ coïncide avec la relation modulo H (à gauche ou à droite, c'est la même chose).
Pour les relations d'équivalence sur un anneau compatibles aux loi d'anneau, on procède de même, en se rappelant que le noyau d'un morphisme de groupes est un idéal bilatère. □

Exemple 1.1.7. Si $f \colon G \to G'$ est un morphisme de groupes, alors f induit un isomorphisme $G/\mathsf{Ker}(f) \xrightarrow{\sim} \mathsf{Im}(f)$. On a des énoncés analogues pour les anneaux ou les espaces vectoriels.

Par exemple, l'application naturelle $\mathbf{Z} \to (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})$ est un morphisme de groupes (et même d'anneaux, dont le noyau est $6\mathbf{Z}$: en passant au quotient, elle induit un morphisme injectif $\mathbf{Z}/6\mathbf{Z} \to (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})$. C'est un isomorphisme par cardinalité. C'est un cas particulier du théorème des restes chinois (*cf* théorème 2.1.31).

1.2. **Le monoïde N.** On admet l'existence d'un ensemble $\mathbf{N}$ (des *entiers naturels*) vérifiant les axiomes suivants (dits de Peano) :

(1) $\mathbf{N}$ contient un élément 0 (en particulier $\mathbf{N}$ n'est pas vide) ;
(2) il existe une application $\mathsf{s} \colon \mathbf{N} \to \mathbf{N}$ (successeur), ayant les propriétés suivantes :
  (i) $0 \notin \mathsf{Im}(\mathsf{s})$;
  (ii) s est injective ;
  (iii) si $E \subset \mathbf{N}$ vérifie $0 \in E$ et $\mathsf{s}(E) \subset E$, alors $E = \mathbf{N}$ (axiome de récurrence).

On définit alors l'addition sur $\mathbf{N}$ par récurrence : si $x, y \in \mathbf{N}$, on pose $x + 0 = x$ et $x + \mathsf{s}(y) = \mathsf{s}(x + y)$. Si on pose $1 = \mathsf{s}(0)$, alors on a $\mathsf{s}(x) = \mathsf{s}(x + 0) = x + \mathsf{s}(0) = x + 1$, de sorte que $\mathsf{s}(x) = x + 1$. De même la multiplication est définie par récurrence par $x0 = 0$ et $x\mathsf{s}(y) = xy + x$. On vérifie facilement que l'addition et la multiplication sont commutatives, associatives et que la multiplication est distributive sur l'addition.

On munit $\mathbf{N}$ d'une relation d'ordre en posant

$$x \leqslant y \Leftrightarrow (\exists z \in \mathbf{N})\, y = x + z.$$

(montrer-le). On vérifie facilement que $\leqslant$ est compatible à l'addition et à la multiplication.

Proposition 1.2.1. $\leqslant$ est un bon ordre sur $\mathbf{N}$, en particulier c'est un ordre total.

Démonstration. Commençons par montrer que c'est un ordre total : soient $x, y \in \mathbf{N}$. Montrons par récurrence sur y que $x \leqslant y$ ou $y \leqslant x$. Si $y = 0$, alors $y \leqslant x$: supposons $y \neq 0$. Si $x = 0$, alors $x \leqslant y$: on peut supposer que $x \neq 0$. Par hypothèse de récurrence, on a $x - 1 \leqslant y - 1$ ou $y - 1 \leqslant x - 1$, et donc $x \leqslant y$ ou $y \leqslant x$, ce achève la récurrence.
Soit $A \subset \mathbf{N}$ une partie non vide : il s'agit de montrer que A admet un plus petit élément. Comme A est non vide, il existe $n \in \mathbf{N}$ tel que $n \in A$. Posons $E_n = \{x \in \mathbf{N}\,;\, x \leqslant n\}$. Comme l'ordre est total, il suffit de montrer que $A \cap E_n$ a un plus petit élément. Il s'agit donc de vérifier que pour tout $n \in \mathbf{N}$, l'ensemble E_n muni de la relation d'ordre induite par $\leqslant$ est bien ordonné : on procède par récurrence sur n. Lorsque $n = 0$, on a $E_0 = \{0\}$, et c'est évident. Supposons $n \neq 0$ et soit $B \subset E_n$ non vide. Si $n \notin B$, alors $B \subset E_{n-1}$ et l'hypothèse de récurrence implique que B a un plus petit élément. Supposons donc que $n \in B$. Si $B = \{n\}$, c'est évident : supposons en outre $B \neq \{n\}$. Alors $B\backslash\{n\}$ est une partie non vide E_{n-1} : l'hypothèse de récurrence implique que $B\backslash\{n\}$ a un plus petit élément, qui est aussi le plus petit élément de B. □

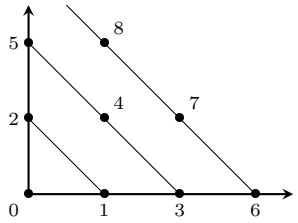
1.3. **Dénombrabilité.**

Définition 1.3.1. (1) Si $n \in \mathbf{N}$, on pose $[\![1, n]\!] = \{x \in \mathbf{N}\,;\, 1 \leqslant x \leqslant n\}$ (c'est l'ensemble vide lorsque $n = 0$).
(2) Un ensemble X est *fini* s'il existe $n \in \mathbf{N}$ et une bijection $X \xrightarrow{\sim} [\![1, n]\!]$. L'entier n est alors unique est s'appelle le *cardinal* de X.
(3) Un ensemble est *dénombrable* s'il est fini ou en bijection avec $\mathbf{N}$.

Remarque. (1) Généralement, on dit que deux ensembles X et Y ont *même cardinal* s'il existe une bijection $X \xrightarrow{\sim} Y$.
(2) L'unicité du cardinal d'un ensemble fini résulte du fait que si n et m sont des entiers et $[\![1, n]\!] \to [\![1, m]\!]$ une injection, alors $n \leqslant m$. Il se montre par récurrence sur m : si $m = 0$, cela résulte qu'il n'y a aucune application d'un ensemble non vide dans l'ensemble vide. Supposons $m \neq 0$ et soit $f : [\![1, n]\!] \to [\![1, m]\!]$ injective. Il n'y a rien à faire si $n = 0$: supposons $n \neq 0$. Soit τ la transposition qui échange $f(n)$ et m : quitte à remplacer f par $\tau \circ f$, on se ramène au cas où $f(n) = m$. Par restriction, f induit alors une injection $[\![1, n-1]\!] \to [\![1, m-1]\!]$ et l'hypothèse de récurrence implique $n - 1 \leqslant m - 1$, d'où $n \leqslant m$.
(3) Un ensemble X est dénombrable s'il existe une application injective $X \to \mathbf{N}$. Cela résulte du fait qu'une partie infinie de $\mathbf{N}$ est en bijection avec $\mathbf{N}$ (exercice).

Proposition 1.3.2. $\mathbf{N} \times \mathbf{N}$ est dénombrable (et donc $\mathbf{N}^d$ est dénombrable pour tout $d \in \mathbf{N}$).

Démonstration. Il s'agit de numéroter les éléments de $\mathbf{N}^2$. On se promène dans un quadrant diagonale par diagonale.



On pose $f(0) = (0,0)$, $f(1) = (1,0)$, $f(2) = (0,1)$, $f(3) = (2,0)$, $f(4) = (1,1)$, $f(5) = (0,2)$, $f(6) = (3,0)$... On numérote ainsi tous les couples d'entiers naturels. L'application réciproque est donnée par

$$f^{-1}(n,m) = m + \sum_{k=0}^{n+m-1} (k+1) = \frac{(n+m)^2 + n + 3m}{2}$$

□

Corollaire 1.3.3. $\mathbf{Q}$ est dénombrable.

Démonstration. Tout rationnel s'écrit de façon unique comme fraction réduite $x = \frac{p}{q}$ où $q \in \mathbf{N}_{>0}$ et $\mathsf{pgcd}(p, q) = 1$. L'application $f : \mathbf{Q} \to \mathbf{Z} \times \mathbf{N}; x \mapsto (p, q)$ est injective, c'est une bijection sur son image, un sous-ensemble de $\mathbf{Z} \times \mathbf{N}$. Comme $\mathbf{Z} \times \mathbf{N}$ est dénombrable, $\mathbf{Q}$ l'est aussi. □

Proposition 1.3.4. Soient Ω un ensemble et $(X_n)_{n \in \mathbf{N}}$ une suite de parties dénombrables de Ω. Alors $\bigcup_{n=0}^{\infty} X_n$ est dénombrable.

Démonstration. Pour $n \in \mathbf{N}$, posons $Y_n = X_n\backslash(X_1 \cup \cdots \cup X_{n-1})$: on a $\bigcup_{n=0}^{\infty} X_n = \bigcup_{n=0}^{\infty} Y_n$ et les Y_n sont deux à deux disjoints. Pour $n \in \mathbf{N}$, soit $f_n : X_n \to \mathbf{N}$ une injection. Pour $x \in Y_n$, posons $f(x) = (n, f_n(x))$. On obtient une injection $f : \bigcup_{n=0}^{\infty} Y_n \to \mathbf{N} \times \mathbf{N}$: la proposition 1.3.2 implique que $\bigcup_{n=0}^{\infty} X_n$ est dénombrable. □

Exercices.
(1) $\mathbf{Q}[X]$ est dénombrable.
(2) L'ensemble des parties finies de $\mathbf{N}$ est dénombrable.
(3) $\mathbf{Q} \cap [0, 1]$ et $\mathbf{Q} \cap [0, 1[$ sont en bijection.

Théorème 1.3.5. (Cantor) $\mathbf{R}$ n'est pas dénombrable.

Démonstration. Il suffit de trouver un sous-ensemble $A \subset \mathbf{R}$ qui n'est pas dénombrable. Notons A l'ensemble des éléments de $]0,1[$ dont le développement décimal ne comporte que des 1 et des 8 après la virgule. On raisonne par l'absurde : supposons qu'il existe une bijection $f\colon \mathbf{N} \to A$. Pour chaque $n \in \mathbf{N}$, on peut écrire

$$f(n) = 0.a_{n,1}a_{n,2}a_{n,3}\dots$$

où $a_{n,k}$ vaut 1 ou 8. Soient x le réel dont le développement décimal est

$$x = 0.a_{1,1}a_{2,2}a_{3,3}\dots$$

et $y = 1 - x$. Alors $y \in A$, car le développement décimal de y présente un 1 (resp. un 8) là où celui de x présente un 8 (resp. un 1). Il existe donc $n \in \mathbf{N}$ tel que $f(n) = y$. Or le n-ième chiffre de y vaut $9 - a_{n,n}$, alors que celui de $f(n)$ vaut $a_{n,n}$: contradiction. □

Théorème 1.3.6. (Cantor) Soit X un ensemble. Il n'existe pas de surjection $X \to \mathscr{P}(X)$.

Démonstration. Soit $f\colon X \to \mathscr{P}(X)$ une surjection. Posons $A = \{x \in X\,;\, x \notin f(x)\}$: on a $A \in \mathscr{P}(X)$. Comme f est surjective, il existe $x_0 \in X$ tel que $A = f(x_0)$. Si $x_0 \in A$, alors $x_0 \notin f(x_0) = A$, ce qui est absurde. Si $x_0 \notin A$, alors $x_0 \in f(x_0) = A$, ce qui est absurde. L'existence de f est donc contradictoire. □

Remarque. Cela fournit une autre rédaction de la non dénombrabilité de $\mathbf{R}$: le développement diadique fournit une bijection $2^{\mathbf{N}}\backslash 2^{(\mathbf{N})} \xrightarrow{\sim} [0,1[$ (la partie $2^{(\mathbf{N})}$ correspondant aux développements non admissibles, c'est-à-dire aux suites qui valent 1 à partir d'un certain rang). Comme $2^{(\mathbf{N})} = \bigoplus_{n=1}^{\infty} 2^{[\![1,n]\!]}$ est dénombrable en vertu de la proposition 1.3.4, la non dénombrabilité de $[0,1[$ (et donc de $\mathbf{R}$) résulte de la non dénombrabilité de $2^{\mathbf{N}} = \mathscr{P}(\mathbf{N})$ (*cf* théorème 1.3.6).

Théorème 1.3.7. (Cantor-Bernstein). Soient $f\colon X \to Y$ et $g\colon Y \to X$ deux applications injectives. Alors il existe une bijection $X \xrightarrow{\sim} Y$.

Démonstration. L'idée consiste à construire une partie $A \subset X$ telle que $g(Y\backslash f(A)) = X\backslash A$: l'application $h\colon X \to Y$ définie par

$$h(x) = \begin{cases} f(x) & \text{si } x \in A \\ g^{-1}(x) & \text{si } x \notin A \end{cases}$$

est alors bien définie et une bijection.
Comme $X\backslash A = g(Y\backslash f(A)) \subset g(Y)$, on a $A \supset A_0 := X\backslash g(Y)$. On a alors $f(A_0) \subset f(A)$, d'où $Y\backslash f(A_0) \supset Y\backslash f(A)$, et donc $g(Y) \supset g(Y\backslash f(A_0)) \supset g(Y\backslash f(A)) = X\backslash A$, de sorte que $A_0 \subset A_1 := X\backslash g(Y\backslash f(A_0)) \subset A$ en passant aux complémentaires. Cela suggère de définir la suite $(A_n)_{n\in\mathbf{N}}$ en posant $A_{n+1} = X\backslash g(Y\backslash f(A_n))$ pour tout $n \in \mathbf{N}$.
Si $n \in \mathbf{N}_{>0}$ vérifie $A_{n-1} \subset A_n$, on a $f(A_{n-1}) \subset f(A_n)$, d'où $Y\backslash f(A_{n-1}) \supset Y\backslash f(A_n)$, et $g(Y\backslash f(A_{n-1})) \supset g(Y\backslash f(A_n))$, et donc $A_n \subset A_{n+1}$ en passant aux complémentaires. Par récurrence, la suite $(A_n)_{n\in\mathbf{N}}$ est donc croissante. On montre de même que si A existe, alors $A_n \subset A$ pour tout $n \in \mathbf{N}$: cela suggère de poser $A = \bigcup_{n=0}^{\infty} A_n$ (c'est en quelque sorte le choix minimal pour A).
On a $X\backslash A = \bigcap_{n=0}^{\infty} (X\backslash A_{n+1}) = \bigcap_{n=0}^{\infty} g(Y\backslash f(A_n)) = g\Big(\bigcap_{n=0}^{\infty} (Y\backslash f(A_n))\Big)$ (la dernière égalité parce que g est injective).
Comme $\bigcap_{n=0}^{\infty} (Y\backslash f(A_n)) = Y\backslash \bigcup_{n=0}^{\infty} f(A_n) = Y\backslash f(A)$, il en résulte que $X\backslash A = g(Y\backslash f(A))$, comme requis. □

Exercices. (1) Soient E un ensemble non vide et $x \in E$. Montrer que E est infini si et seulement s'il existe une bijection $E \xrightarrow{\sim} E\backslash\{x\}$.

(2) Montrer que l'application

$$\begin{aligned} \mathbf{N}^2 &\to \mathbf{N} \\ (n,m) &\mapsto 2^n(2m+1) - 1 \end{aligned}$$

est bijective.

(3) Montrer que $\mathbf{N}^{(\mathbf{N})}$ (l'ensemble des suites d'entiers nuls à partir d'un certain rang) est dénombrable.

(4) Montrer que $\mathsf{Card}(\mathbf{R}^{\mathbf{N}}) = \mathsf{Card}(\mathbf{R})$.

2. Algèbre générale

2.1. Extensions successives de la notion de nombre.

2.1.1. *Anneau* $\mathbf{Z}$ *des entiers relatifs.* Le monoïde additif $\mathbf{N}$ a un défaut : ce n'est pas un groupe (les éléments non nuls n'ont pas d'opposé). On l'enrichit donc en construisant le groupe associé de la façon suivante.
On munit $X = \mathbf{N} \times \mathbf{N}$ de la relation binaire $\mathcal{R}$ définie par

$$(a_1, b_1)\mathcal{R}(a_2, b_2) \Leftrightarrow a_1 + b_2 = a_2 + b_1$$

On vérifie facilement qu'il s'agit d'une relation d'équivalence, et on pose $\mathbf{Z} = X/\mathcal{R}$.
Soit $(a, b) \in X$. Si $(a_1, b_1)\mathcal{R}(a_2, b_2)$ dans X, alors $(a + a_1, b + b_1)\mathcal{R}(a + a_2, b + b_2)$. Cela montre que la loi d'addition sur $X = \mathbf{N} \times \mathbf{N}$ passe au quotient, et fournit une loi de composition interne $+$ sur $\mathbf{Z}$. Il est alors immédiat qu'il s'agit d'une loi de groupe abélien, pour laquelle la classe de $(0, 0)$ (notée 0) est l'élément neutre. Si $(a, b) \in X$, l'inverse (opposé) de la classe de (a, b) est celle de (b, a). Composée avec la surjection canonique, l'application $\mathbf{N} \to X$; $a \mapsto (a, 0)$ fournit une application injective $\mathbf{N} \to \mathbf{Z}$, compatible à l'addition. L'opposé de $a \in \mathbf{N}$ dans $\mathbf{Z}$ est la classe $-a$ de $(0, a)$. Il en résulte alors que la classe de $(a, b) \in X$ dans $\mathbf{Z}$ n'est autre que $a - b$.

L'application $\mathbf{N} \to \mathbf{Z}$ qu'on vient de construire jouit de la propriété universelle suivante : si G est un groupe et $f\colon \mathbf{N} \to G$ est un morphisme de monoïdes (c'est-à-dire tel que $f(0) = e_G$ et $f(a + b) = f(a)f(b)$ pour tout $a, b \in \mathbf{N}$), alors il existe un unique morphisme de groupes $\mathbf{Z} \to G$ qui prolonge f (il vérifie bien sûr $f(a - b) = f(a)f(b)^{-1}$). En ce sens, $\mathbf{Z}$ est le « plus petit » groupe monoïde qui contient $\mathbf{N}$. On dira qu'un élément de $\mathbf{Z}$ est *positif* s'il appartient à l'image de $\mathbf{N}$.

On vérifie aisément que la multiplication de $\mathbf{N}$ s'étend de façon unique en une multiplication sur $\mathbf{Z}$: si $a_1, a_2, b_1, b_2 \in \mathbf{N}$, il s'agit essentiellement de voir que $(a_1 - b_1)(a_2 - b_2) = (a_1a_2 + b_1b_2) - (a_1b_2 + b_1a_2)$ ne dépend que des classes de (a_1, b_1) et (a_2, b_2) dans $\mathbf{Z}$, ce qui est trivial. Il n'est pas très difficile (mais un peu fastidieux) de vérifier que $(\mathbf{Z}, +, .)$ est un anneau commutatif, d'unité la classe 1 de $(1, 0)$. L'anneau $\mathbf{Z}$ a la propriété universelle suivante : si A est un anneau unitaire, alors il existe un unique morphisme d'anneaux $\mathbf{Z} \to A$ (il envoie $n \in \mathbf{N}$ sur $n1_A = \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}$).

Observons enfin que la relation d'ordre $\leqslant$ sur $\mathbf{N}$ se prolonge à $\mathbf{Z}$: si $x, y \in \mathbf{Z}$, il existe $n \in \mathbf{N}$ tel que $x + n, y + n \in \mathbf{N}$, et on a $x \leqslant y \Leftrightarrow x + n \leqslant y + n$ (par définition de $\leqslant$, cela est indépendant de n). Bien entendu les règles de calcul (addition, multiplication par un entier positif) se vérifient aisément. Si $a \in \mathbf{Z}$, on pose $|a| = \max\{a, -a\} \in \mathbf{N}$.

2.1.2. *Division euclidienne dans* $\mathbf{Z}$ *et premières conséquences.* La division euclidienne est le point de départ de l'arithmétique de $\mathbf{Z}$.

Lemme 2.1.3. Toute partie non vide et minorée de $\mathbf{Z}$ admet un plus petit élément.

Démonstration. On sait que l'ordre sur $\mathbf{N}$ est bon. Soit $A \subset \mathbf{Z}$ non vide et minoré par x. Si $x \geqslant 0$ alors $A \subset \mathbf{N}$, et son plus petit élément dans $\mathbf{N}$ est aussi son plus petit élément dans $\mathbf{Z}$. Supposons maintenant $x < 0$ et posons $A - x = \{a - x\,;\, a \in A\}$. Si $a \in A$, on a $x \leqslant a$ *i.e.* $0 \leqslant a - x$ d'où $A - x \subset \mathbf{N}$. Soit b le plus petit élément de $A - x$. Il existe $c \in A$ tel que $b = c - x$ et pour tout $a \in A$, on a $b \leqslant a - x$, de sorte que $c = b + x$ est le plus petit élément de A dans $\mathbf{Z}$. □

Remarque. Cela implique que l'ordre sur $\mathbf{Z}$ est total. Cependant, il n'est pas bon : l'ensemble $\mathbf{Z}$ n'a pas de plus petit élément.

Théorème 2.1.4. (Division euclidienne dans $\mathbf{Z}$). Soient $a \in \mathbf{Z}$ et $b \in \mathbf{Z}\backslash\{0\}$. Il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$ tel que

$$a = bq + r \text{ et } 0 \leqslant r < |b|\,.$$

Les entiers q et r sont appelés, respectivement, le *quotient* et le *reste* de la *division euclidienne* de a par b.

Démonstration. Preuve de l'existence. Si $a = 0$, alors le couple $(0, 0)$ convient. Supposons désormais $a \neq 0$. Supposons $b > 0$: posons $A = \{n \in \mathbf{Z}\,;\, nb > a\}$. L'entier $(|a|+1)b$ est un multiple de b qui est strictement plus grand que a (en effet $(|a| + 1)b > |a|\, b = |a|\, (b - 1 + 1) \geqslant |a| \geqslant a$). On a donc [2] $A \neq \varnothing$. Par ailleurs, si $x < -|a|$, on a $xb < -|a|\, b \leqslant -|a| \leqslant a$ (vu que $b \geqslant 1$), donc $x \notin A$. Cela montre que A est minoré par $-|a|$. Soient n le plus petit élément de A (*cf* lemme 2.1.3) et $q = n - 1$. Comme $q < n$, on a $qb \leqslant a < nb$, ce qui montre que $0 \leqslant r < b$ avec $r = a - qb$: le couple (q, r) convient.
Si $b < 0$, le cas traité ci-dessus montre qu'il existe un couple (q, r) tel que $-a = q(-b) + r$ et $0 \leqslant r < -b$. On a alors $a = qb - r$ et $-b < -r \leqslant 0$: si $r = 0$, le couple $(q, 0)$ convient, et si $r < 0$, le couple $(q - 1, b - r)$ convient.
Preuve de l'unicité. Supposons $a = q_1b + r_1$ et $a = q_2b + r_2$ avec $0 \leqslant r_1, r_2 < |b|$. On a alors $(q_1 - q_2)b = r_2 - r_1$, de sorte que $-|b| < (q_1 - q_2)b < |b|$, soit encore $0 \leqslant |q_1 - q_2|\, |b| < |b|$, ce qui implique $|q_1 - q_2| < 1$ d'où $q_1 = q_2$, et donc $r_1 = r_2$. □

Théorème 2.1.5. Les sous-groupes de $\mathbf{Z}$ sont les parties de la forme $n\,\mathbf{Z}$ avec $n \in \mathbf{N}$.

Démonstration. Il est clair que si $n \in \mathbf{N}$, alors $n\,\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$. Réciproquement, soit $G \subset \mathbf{Z}$ un sous-groupe. Supposons $G \neq \{0\}$: l'ensemble $G \cap \mathbf{N}_{>0}$ n'est pas vide. Notons n son plus petit élément : on a $n \in G$, donc $n\,\mathbf{Z} \subset G$. Si $x \in G$, soit $x = qn + r$ la division euclidienne de x par n. Comme $n\,\mathbf{Z} \subset G$, on a $qn \in G$, donc $r = x - qn \in G$. Comme $0 \leqslant r < n$, on a nécessairement $r = 0$ par définition de n, si bien que $x = qn \in n\,\mathbf{Z}$, ce qui prouve $G = n\,\mathbf{Z}$. □

2. On vient de montrer que $\mathbf{N}$ est archimédien.

Remarque. L'entier $n \in \mathbf{N}$ du théorème est unique : c'est 0 lorsque $G = \{0\}$, et $\min\left(G \cap \mathbf{N}_{>0}\right)$ lorsque $G \neq \{0\}$.

Corollaire 2.1.6. Les idéaux de $\mathbf{Z}$ sont les parties de la forme $n\,\mathbf{Z}$ avec $n \in \mathbf{N}$.

Démonstration. Les parties $n\,\mathbf{Z}$ sont les idéaux de $\mathbf{Z}$. Réciproquement, si $I \subset \mathbf{Z}$ est un idéal, c'est en particulier un sous-groupe additif, donc de la forme $n\,\mathbf{Z}$ d'après le théorème 2.1.5. □

Remarque. Il en résulte que les quotients du groupe (et même de l'anneau, puisque sous-groupes et idéaux coïncident) de $\mathbf{Z}$ sont $\mathbf{Z}$ et les $\mathbf{Z}/n\,\mathbf{Z}$ pour $n \in \mathbf{N}_{>0}$.

Définition 2.1.7. (1) Soit A un anneau *intègre*, commutatif et unitaire. On dit que A est *principal* si ses idéaux sont principaux, *i.e.* engendrés par un élément, c'est-à-dire de la forme xA avec $x \in A$ (exercice : l'élément x est alors défini de façon unique à multiplication par un élément inversible près).
(2) Soit A un anneau unitaire. On sait qu'il existe un unique morphisme d'anneaux $\mathbf{Z} \to A$. Son noyau est un idéal de $\mathbf{Z}$: il existe un unique entier $c \in \mathbf{N}$ tel que ce noyau soit $c\,\mathbf{Z}$. Cet entier s'appelle la *caractéristique* de A. Lorsque $c = 0$, le morphisme $\mathbf{Z} \to A$ est injectif. Lorsque $c > 0$, il se factorise en un morphisme injectif $\mathbf{Z}/c\,\mathbf{Z} \to A$ (on dit que A est de caractéristique positive).

Exemple 2.1.8. $\mathbf{Q}$ est de caractéristique nulle. $(\mathbf{Z}/6\,\mathbf{Z})[X]$ est de caractéristique 6.

Exercice. La caractéristique d'un corps est soit 0, soit un nombre premier (*i.e.* un élément $p \in \mathbf{N}_{>1}$ qui n'a d'autres diviseurs dans $\mathbf{N}$ que 1 et lui-même). Si K est un corps de caractéristique $p > 0$, le morphisme $\mathbf{Z} \to K$ se factorise en un morphisme de corps $\mathbf{Z}/p\,\mathbf{Z} \to K$. Si K est de caractéristique nulle, il se prolonge de façon unique en un morphisme de corps $\mathbf{Q} \to K$. Dans le premier cas (resp. le deuxième cas) $\mathbf{Z}/p\,\mathbf{Z}$ (resp. $\mathbf{Q}$) est le sous-corps premier de K.

Théorème 2.1.9. (Systèmes de numération). Soit $b \in \mathbf{N}_{\geqslant 2}$ (la *base* de la numération). Si $a \in \mathbf{N}$, il existe un unique élément $(a_n)_{n\in\mathbf{N}} \in \{0, \dots, b-1\}^{(\mathbf{N})}$ tel que $a = \sum_{n=0}^{\infty} a_n b^n$ (la somme est finie). Il s'agit de l'écriture de a en base b.

Démonstration. On procède par récurrence sur a, le cas $a = 0$ étant trivial. Supposons $a > 0$. Si la décomposition existe, on a nécessairement $a = a_0 + bq$ avec $q = \sum_{n=1}^{\infty} a_n b^{n-1} \in \mathbf{N}$, de sorte que a_0 est le reste de la division euclidienne de a par b, et q le quotient. Comme $b > 1$ et $a > 0$, on a $q < a$: l'hypothèse de récurrence implique l'existence et l'unicité de $(a_n)_{n\in\mathbf{N}_{>0}} \in \{0, \dots, b-1\}^{(\mathbf{N}_{>0})}$ telle que $q = \sum_{n=1}^{\infty} a_n b^{n-1}$, de sorte que $a = \sum_{n=0}^{\infty} a_n b^n$. □

Définition 2.1.10. Soient $a, b \in \mathbf{Z}$ non tous les deux nuls. Comme $\mathbf{Z}$ est principal, il existe des entiers positifs uniques $d \in \mathbf{N}_{>0}$ et $m \in \mathbf{N}$ tels que $a\,\mathbf{Z} + b\,\mathbf{Z} = d\,\mathbf{Z}$ et $a\,\mathbf{Z} \cap b\,\mathbf{Z} = m\,\mathbf{Z}$. L'entier d (resp. m) est le *plus grand commun diviseur* (resp. le *plus petit commun multiple*) de a et de b. On le note $\mathsf{pgcd}(a, b)$ (resp. $\mathsf{ppcm}(a, b)$).
Par définition, il existe $u, v \in \mathbf{Z}$ tels que

$$\mathsf{pgcd}(a, b) = au + bv.$$

Une telle écriture s'appelle une *égalité de Bézout*. On dit que a et b sont *premiers entre eux* lorsque $\mathsf{pgcd}(a, b) = 1$.

Remarque. Si $p \in \mathbf{N}$ est premier et $a \in \mathbf{Z}\backslash\{0\}$, on a $\mathsf{pgcd}(a, p) \in \{1, p\}$ (car c'est un diviseur de p).

Théorème 2.1.11. (Algorithme d'Euclide). Soient $a, b \in \mathbf{Z}$ non tous les deux nuls. Leur pgcd se calcule récursivement par l'algorithme suivant :

$$\mathsf{pgcd}(a, b) = \begin{cases} |a| & \text{si } b = 0 \\ \mathsf{pgcd}(b, r) & \text{si } b \neq 0, \text{ où } r \text{ est le reste de la division euclidienne de } a \text{ par } b \text{ si } b \neq 0. \end{cases}$$

Remarque. Dans la pratique, on construit donc la *suite des restes* $(r_n)_{0\leqslant n\leqslant N}$ telle que

$$\begin{cases} r_0 = a, \\ r_1 = b, r_{n+1} \text{ est le reste de la division euclidienne de } r_{n-1} \text{ par } r_n \text{ si } r_n \neq 0. \end{cases}$$

Son dernier terme non nul est $\mathsf{pgcd}(a, b)$.

Démonstration. Par construction, $r_{n+1} < r_n$ pour tout $n > 0$ tel que $r_n \neq 0$. Il en résulte bien qu'il existe $N \in \mathbf{N}_{>0}$ tel que la suite $(r_n)_{1\leqslant n\leqslant N}$ soit strictement décroissante, et $r_N = 0$. Par ailleurs, on $\mathsf{pgcd}(r_{n+1}, r_n) = \mathsf{pgcd}(r_n, r_{n-1}) = \mathsf{pgcd}(a, b)$ pour tout $n \in \{1, \dots, N\}$, en particulier $r_{N-1} = \mathsf{pgcd}(a, b)$. □

Remarque. Nombre d'étapes de l'algorithme d'Euclide. Rappelons que la suite de Fibonacci $(F_n)_{n\in\mathbf{N}}$ est définie par $F_0 = F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$ pour tout $n > 1$. On a $F_n = \frac{1}{\sqrt{5}}\left(\phi^{n+1} - (-\phi)^{-n-1}\right)$ où $\phi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or (il en résulte que F_n est l'entier le plus proche de $\frac{\phi^{n+1}}{\sqrt{5}}$).

Proposition 2.1.12. (Lamé). Soient $0 < b < a$ des entiers et d leur pgcd. Si l'algorithme d'Euclide appliqué à (a, b) termine en N étapes, alors $dF_{N+1} \leqslant a$ et $dF_N \leqslant b$.

Démonstration. On raisonne par récurrence. Si $N = 1$, alors a est un multiple de b : on a $b = d = dF_1$ et $a \geqslant 2d = dF_2$. Supposons $N > 1$: la première étape transforme (a, b) en $(b, a - qb)$ où $r = a - qb \leqslant a - b$. Par hypothèse de récurrence, on a donc $dF_N \leqslant b$ et $dF_{N-1} \leqslant r \leqslant a - b$, de sorte que $a \geqslant dF_{N-1} + b \geqslant d(F_{N-1} + F_N) = dF_{N+1}$. □

Corollaire 2.1.13. Le nombre d'étapes dans l'algorithme d'Euclide appliqué à (a, b) tels que $0 < b < a$ est majoré par $1 + \frac{3}{2}\ln(b)$.

Démonstration. D'après ce qui précède, cet entier N vérifie $b \geqslant dF_N \geqslant F_N$: il suffit de vérifier que $n \leqslant \frac{3}{2}\ln(F_N) + 1$ pour tout $N \in \mathbf{N}$. □

En théorie et en pratique, il est très important de pouvoir trouver non seulement le pgcd de deux entiers $0 < b < a$, mais aussi une relation de Bézout. Pour ce faire, on applique l'*algorithme d'Euclide étendu*. Il est défini par trois suites $(r_n)_{0\leqslant n\leqslant N}$, $(u_n)_{0\leqslant n<N}$ et $(v_n)_{0\leqslant n<N}$ définies de la façon suivante. On initialise les suites en posant $r_0 = a$, $r_1 = b$, $(u_0, v_0) = (1, 0)$ et $(u_1, v_1) = (0, 1)$. Ces suites étant connues au rang n avec $r_n \neq 0$, soit $r_{n-1} = q_n r_n + r_{n+1}$ la division euclidienne de r_{n-1} par r_n. On pose alors $(u_{n+1}, v_{n+1}) = (u_{n-1}, v_{n-1}) - q_n(u_n, v_n)$. On l'a vu, il existe $N \in \mathbf{N}$ tel que $r_N = 0$ et $r_{N-1} = \mathsf{pgcd}(a, b)$. Une récurrence immédiate implique que pour tout $n \in \{0, \dots, N\}$, on a $r_n = u_n a + v_n b$: au rang $n = N - 1$, cela fournit une égalité de Bézout.
Dans la pratique, il est commode de présenter l'algorithme sous forme d'un tableau de la façon suivante :

a	1	0	
b	0	1	q_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_n	u_n	v_n	q_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$

La $n+1$-ième ligne n'est alors que la $n-1$-ième moins q_n fois la n-ième ($L_{n+1} \leftarrow L_{n-1} - q_n L_n$).

Exemple 2.1.14. Trouver une relation de Bézout pour $(57, 13)$:

r_n	u_n	v_n	q_n
57	1	0	
13	0	1	4
5	1	-4	2
3	-2	9	1
2	3	-13	1
1	-5	22	

donc $1 = (-5) \times 57 + 22 \times 13$.

Proposition 2.1.15. (Lemme de Gauss). Soient $a, b, c \in \mathbf{Z}$ tels que $a \mid bc$ et $\mathsf{pgcd}(a, b) = 1$. Alors $a \mid c$.

Démonstration. Soit $au + bv = 1$ une relation de Bézout : on a $a \mid acu + bcv = c$. □

Proposition 2.1.16. (Bachet-Bézout). Soient $a, b, c \in \mathbf{Z}\backslash\{0\}$ et $d = \mathsf{pgcd}(a, b)$. Si $d \nmid c$, l'ensemble des solutions de l'équation diophantienne $ax + by = c$ est vide. Si $d \mid c$, l'ensemble des solutions est de la forme

$$\big\{(x_0, y_0) + k\big(\tfrac{b}{d}, -\tfrac{a}{d}\big)\,;\, k \in \mathbf{Z}\big\}.$$

Démonstration. La condition $d \mid c$ est évidemment nécessaire à l'existence de solutions : supposons-la remplie. Écrivons $c = dn$. Il existe une égalité de Bézout $u_0 a + v_0 b = d$, de sorte que $ax_0 + by_0 = c$ avec $(x_0, y_0) = n(u_0, v_0)$. Si maintenant (x, y) est une solution, on a $a(x - x_0) + b(y - y_0) = 0$, d'où $\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$. Comme $\mathsf{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, le lemme de Gauss implique que $\frac{b}{d} \mid x - x_0$: écrivons $x - x_0 = \frac{b}{d}k$ avec $k \in \mathbf{Z}$. On a alors $y - y_0 = -\frac{a}{d}k$, de sorte que $(x, y) = (x_0, y_0) + k\big(\frac{b}{d}, -\frac{a}{d}\big)$. □

2.1.17. *Nombres premiers, factorisation des entiers.*

Lemme 2.1.18. Soient $a, b \in \mathbf{Z}$ et p un nombre premier tels que $p \mid ab$. Alors $p \mid a$ ou $p \mid b$.

Démonstration. Si $p \nmid a$, on a $\mathsf{pgcd}(a, p) = 1$ et le lemme de Gauss implique $p \mid b$. □

Théorème 2.1.19. Tout élément $n \in \mathbf{Z}\backslash\{0\}$ s'écrit $n = \pm p_1 \cdots p_r$ où $p_1, \dots, p_r$ sont des nombres premiers uniques à l'ordre près.

Démonstration. Existence. Comme $n = -(-n)$, il suffit de traiter le cas où $n > 0$. On procède par récurrence. C'est trivial lorsque $n = 1$: on a alors $r = 0$ (le produit est vide). Supposons $n > 1$. Si n est premier, on a $r = 1$ et $p_1 = n$, sinon il existe $m \in \mathbf{N}$ tel que $m \mid n$ et $1 < m < n$: on peut écrire $n = m\frac{n}{m}$. Comme $m, \frac{n}{m} < n$, l'hypothèse de récurrence implique l'existence de $p_1, \dots, p_s$ et $p_{s+1}, \dots, p_r$ premiers tels que $m = p_1 \cdots p_s$ et $\frac{n}{m} = p_{s+1} \cdots p_r$, de sorte que $n = p_1 \cdots p_r$, ce qui achève la récurrence.
Unicité. Supposons qu'on a deux écritures $a = \pm p_1 \cdots p_r = \pm q_1 \cdots q_s$. Montrons par récurrence sur s que ce sont les mêmes à permutation des facteurs près. Le signe est celui de a : quitte à multiplier par -1, on peut supposer que $a > 0$. Si $s = 0$, alors $a = 1$, ce qui implique nécessairement $r = 0$. Si $s > 0$, alors q_s divise le produit $p_1 \cdots p_r$: d'après le lemme 2.1.18, il existe $i \in \{1, \dots, r\}$ tel que $q_s \mid p_i$, et donc $p_i = q_s$ vu que p_i et q_s sont premiers. Quitte à renuméroter, on peut supposer $i = r$. En divisant par q_s, on a donc $p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$, et on peut conclure en vertu de l'hypothèse de récurrence. □

Définition 2.1.20. Soient $n \in \mathbf{Z}\backslash\{0\}$ et p un nombre premier. On pose

$$v_p(n) = \max\left\{k \in \mathbf{N}\,;\, p^k \mid n\right\}$$

(c'est bien défini vu que $p^k > n$ et donc $p^k \nmid n$ si $k \gg 0$). L'entier $v_p(n)$ s'appelle la *valuation p-adique* de n. On a donc $v_p(n) > 0 \Leftrightarrow p \mid n$. Il en résulte que l'ensemble des nombres premiers p tels que $v_p(n) > 0$ est fini, et une reformulation du théorème 2.1.19 est

$$n = \mathsf{sign}(n) \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

où $\mathbb{P}$ désigne l'ensemble des nombres premiers (le produit a bien un sens car fini en vertu de ce qui précède).
On étend v_p à $\mathbf{Z}$ en posant $v_p(0) = +\infty$.

Exercice. Propriétés des valuations. Si $x, y \in \mathbf{Z}$, alors :
(1) $v_p(x+y) \geqslant \min\{v_p(x), v_p(y)\}$ avec égalité si $v_p(x) \neq v_p(y)$;
(2) $v_p(xy) = v_p(x) + v_p(y)$;
(3) on a $x \mid y \Leftrightarrow (\forall p \in \mathbb{P})\, v_p(x) \leqslant v_p(y)$.

2.1.21. *Congruences, anneaux quotients $\mathbf{Z}/n\mathbf{Z}$ et premières applications.*

Définition 2.1.22. Soit $n \in \mathbf{Z}\backslash\{0\}$. Deux entiers $x, y \in \mathbf{Z}$ sont *congrus* modulo n si $y - x \in n\mathbf{Z}$: on note alors

$$y \equiv x \mod n.$$

Cela définit une relation d'équivalence sur $\mathbf{Z}$, qui n'est autre que la relation d'équivalence modulo l'idéal $n\mathbf{Z} \subset \mathbf{Z}$. Les classes d'équivalences sont les parties de la forme $x + n\mathbf{Z}$.
Le quotient $\mathbf{Z}/n\mathbf{Z}$ est un anneau. Si $x \in \mathbf{Z}$, on note $\overline{x} = x + n\mathbf{Z}$ son image dans le quotient.

Remarque. Une congruence modulo n est exactement la même chose qu'une égalité dans $\mathbf{Z}/n\mathbf{Z}$. Comme ce dernier a le bon goût d'être un anneau et comme il est plus léger de manipuler des égalités que des congruences, il est souvent bien plus commode de travailler dans $\mathbf{Z}/n\mathbf{Z}$ qu'avec des congruences.

Proposition 2.1.23. $\#(\mathbf{Z}/n\mathbf{Z}) = n$.

Démonstration. C'est une conséquence de la division euclidienne. □

Remarque. Explicitement, on a $\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, mais il ne faut bien sûr pas confondre avec l'ensemble $\{0, 1, \ldots, n-1\}$.

Définition 2.1.24. Un groupe est *cyclique* s'il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour n convenable.

Exemple 2.1.25. Si $n \in \mathbf{N}_{>0}$, notons $U_n = \{z \in \mathbf{C}\,;\, z^n = 1\}$ le groupe des racines n-ièmes de l'unité. L'application

$$\begin{aligned} \mathbf{Z} &\to \mathbf{C}^\times \\ k &\mapsto e^{\frac{2ik\pi}{n}} \end{aligned}$$

est un morphisme de groupes surjectif, de noyau $n\mathbf{Z}$: il se factorise en un isomorphisme $\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} U_n$, ce qui montre que U_n est cyclique.

Proposition 2.1.26. Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont les quotients $d\mathbf{Z}/n\mathbf{Z}$ pour $d \in \mathbf{N}_{>0}$ divisant n. En particulier il y a bijection entre ces sous-groupes et l'ensemble des diviseurs de n. *Idem* en remplaçant « sous-groupes » par « idéaux ».

Démonstration. Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont les parties de la forme $H/n\mathbf{Z}$ où H est un sous-groupe de $\mathbf{Z}$ qui contient $n\mathbf{Z}$. Un tel sous-groupe est de la forme $d\mathbf{Z}$, et l'inclusion $n\mathbf{Z} \subset d\mathbf{Z}$ équivaut à $d \mid n$. □

Exercice. Déterminer $\mathsf{Hom}_{\mathsf{gr}}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})$.

Proposition 2.1.27. Soient $n \in \mathbf{Z}\backslash\{0\}$ et $x \in \mathbf{Z}$. Alors $\overline{x} \in (\mathbf{Z}/n\mathbf{Z})^\times$ si et seulement si $\mathsf{pgcd}(x, n) = 1$.

Démonstration. On a $\overline{x} \in (\mathbf{Z}/n\mathbf{Z})^\times$ si et seulement s'il existe $u \in \mathbf{Z}$ tel que $\overline{xu} = \overline{1}$, soit encore $xu \equiv 1 \mod n$, ce qui équivaut à l'existence de $v \in \mathbf{Z}$ tel que $xu + nv = 1$, soit encore $\mathsf{pgcd}(x, n) = 1$. □

Remarque. (1) Calcul explicite de l'inverse d'un élément de $(\mathbf{Z}/n\mathbf{Z})^\times$. Soit $x \in \mathbf{Z}$ tel que $\overline{x} \in (\mathbf{Z}/n\mathbf{Z})^\times$, *i.e.* tel que $\mathsf{pgcd}(x, n) = 1$: il existe une relation de Bézout $xu + nv = 1$. Dans $\mathbf{Z}/n\mathbf{Z}$, cela donne $\overline{xu} = \overline{1}$, de sorte que l'inverse de $\overline{x}$ est $\overline{u}$ (cela montre l'importance de l'algorithme d'Euclide étendu).
(2) Si $x \in \mathbf{Z}$, alors on a les équivalences

$$\mathsf{pgcd}(x, n) = 1 \Leftrightarrow \overline{x} \in (\mathbf{Z}/n\mathbf{Z})^\times \Leftrightarrow \left(\overline{x} \text{ engendre le groupe } \mathbf{Z}/n\mathbf{Z}\right).$$

Définition 2.1.28. Si $n \in \mathbf{N}_{>0}$, on pose $\varphi(n) = \#(\mathbf{Z}/n\mathbf{Z})^\times$. L'application φ s'appelle l'*indicatrice d'Euler*.

Proposition 2.1.29. Si $\alpha \in \mathbf{N}_{>0}$ et p est un nombre premier, on a $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. En particulier, $\varphi(p) = p - 1$, de sorte que $\mathbf{Z}/p\mathbf{Z}$ est un corps.

Démonstration. Il s'agit de compter le nombre d'éléments de $\{0,\dots,p^\alpha-1\}$ qui sont premiers à p : il s'agit de p^α moins le nombre d'éléments qui sont divisibles par p, *i.e.* de la forme pk avec $0 \leqslant k < p^{\alpha-1}$. Cela montre donc que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$. □

Exercice. Montrer que $\varphi(n) = n-1$ si et seulement si n est premier.

Théorème 2.1.30. (Euler). Si $n \in \mathbf{N}_{>0}$ et $a \in \mathbf{Z}$ est premier à n, on a

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Démonstration. C'est le théorème de Lagrange appliqué au groupe $(\mathbf{Z}/n\,\mathbf{Z})^\times$. □

Remarque. Lorsque $n = p$ est premier, on retrouve le petit théorème de Fermat : si $a \in \mathbf{Z}$ est non divisible par p, on a $a^{p-1} \equiv 1 \mod p$.

Théorème 2.1.31. (Théorème des restes chinois). Soient $a, b \in \mathbf{Z}\backslash\{0\}$. Alors $\mathsf{pgcd}(a,b) = 1$ si et seulement si l'application naturelle

$$\mathbf{Z}/ab\,\mathbf{Z} \to (\mathbf{Z}/a\,\mathbf{Z}) \times (\mathbf{Z}/b\,\mathbf{Z})$$

est un isomorphisme d'anneaux.

Démonstration. • Supposons $\mathsf{pgcd}(a,b) = 1$. Notons $f\colon \mathbf{Z} \to (\mathbf{Z}/a\,\mathbf{Z}) \times (\mathbf{Z}/b\,\mathbf{Z})$ le morphisme naturel. Si $z \in \mathsf{Ker}(f)$, alors $a \mid z$ et $b \mid z$. Comme $\mathsf{pgcd}(a,b) = 1$, le lemme de Gauss implique que $ab \mid z$. Cela implique que $\mathsf{Ker}(f) = ab\,\mathbf{Z}$, de sorte que l'application f se factorise en un morphisme injectif d'anneaux $\widetilde{f}\colon \mathbf{Z}/ab\,\mathbf{Z} \to (\mathbf{Z}/a\,\mathbf{Z}) \times (\mathbf{Z}/b\,\mathbf{Z})$. C'est un isomorphisme pour des raisons de cardinalité.
• Réciproquement, supposons que l'application naturelle $\mathbf{Z}/ab\,\mathbf{Z} \to (\mathbf{Z}/a\,\mathbf{Z}) \times (\mathbf{Z}/b\,\mathbf{Z})$ est un isomorphisme d'anneaux. Cela implique l'existence de $z \in \mathbf{Z}$ tel que $z \equiv 0 \mod a$ et $z \equiv 1 \mod b$: écrivons $z = au$ et $z - 1 = -bv$. On a alors $1 = au + bv$, ce qui montre que $\mathsf{pgcd}(a,b) = 1$. □

Remarque. (1) Bien entendu, une récurrence immédiate implique que si $a_1,\dots,a_r \in \mathbf{Z}\backslash\{0\}$ sont des entiers deux à deux premiers entre eux, alors l'application naturelle

$$\mathbf{Z}/a_1\cdots a_r\,\mathbf{Z} \to (\mathbf{Z}/a_1\,\mathbf{Z}) \times \cdots \times (\mathbf{Z}/a_r\,\mathbf{Z})$$

est un isomorphisme d'anneaux.
(2) Le théorème est une équivalence. Par exemple, $(\mathbf{Z}/2\,\mathbf{Z})^2$ et $\mathbf{Z}/4\,\mathbf{Z}$ ne sont pas isomorphes, parce que le premier est tué par 2, et le deuxième non.
(3) Soient $a, b \in \mathbf{Z}\backslash\{0\}$ premiers entre eux. Il est important de savoir calculer l'antécédent de $(\overline{x},\overline{y}) \in (\mathbf{Z}/a\,\mathbf{Z}) \times (\mathbf{Z}/b\,\mathbf{Z})$. On part d'une relation de Bézout $au + bv = 1$: l'image de au est $(\overline{0},\overline{1})$ et celle de bv est $(\overline{1},\overline{0})$. Celle de $bvx + auy$ est donc $(\overline{x},\overline{y})$: l'antécédent recherché est donc l'image de $bvx + auy$ modulo ab.

Corollaire 2.1.32. Soient $a, b \in \mathbf{Z}\backslash\{0\}$ deux entiers premiers entre eux. Alors $(\mathbf{Z}/ab\,\mathbf{Z})^\times \xrightarrow{\sim} (\mathbf{Z}/a\,\mathbf{Z})^\times \times (\mathbf{Z}/b\,\mathbf{Z})^\times$. En particulier, on a[3] $\varphi(ab) = \varphi(a)\varphi(b)$.

Il résulte de ce qui précède que si $n \in \mathbf{N}_{>0}$ a pour factorisation en produit de nombres premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ (où $p_1,\dots,p_r$ sont des entiers premiers deux à deux distincts et $\alpha_i \in \mathbf{N}_{>0}$ pour tout $i \in \{1,\dots,r\}$), alors

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \tfrac{1}{p_i}\right).$$

Proposition 2.1.33. Soient p un nombre premier impair, et $\alpha \in \mathbf{N}_{>0}$. Alors le groupe $(\mathbf{Z}/p^\alpha\,\mathbf{Z})^\times$ est cyclique.

Lemme 2.1.34. Soient G un groupe, $x, y \in G$ deux éléments qui commutent et d'ordres n et m respectivement. Si $\mathsf{pgcd}(n,m) = 1$, alors xy est d'ordre nm.

Démonstration. Comme x et y commutent, on a bien sûr $(xy)^{nm} = \left(x^n\right)^m \left(y^m\right)^n = e$, ce qui montre que l'ordre de xy divise nm. Réciproquement, si $k \in \mathbf{Z}$ est tel que $(xy)^k = e$, alors $e = (xy)^{km} = x^{km}y^{km} = x^{km}$, ce qui montre que n divise km. Comme $\mathsf{pgcd}(n,m) = 1$, le lemme de Gauss implique que $n \mid k$. On a de même $m \mid k$, d'où $nm \mid k$, ce qui achève la preuve. □

Remarque. Aucune hypothèse n'est superflue.

Définition 2.1.35. Si G est un groupe fini, l'*exposant* de G est le ppcm $\mu(G)$ des ordres de tous les éléments de G.

Lemme 2.1.36. Si G est un groupe abélien fini, il existe $x \in G$ d'ordre $\mu(G)$ (en particulier $\mu(G) \mid \#G$).

Démonstration. Soit $\mu(G) = \prod_{i=1}^{r} p_i^{\alpha_i}$ la factorisation de $\mu(G)$ en produit de nombres premiers (où $p_1,\dots,p_r$ sont des entiers premiers deux à deux distincts et $\alpha_i \in \mathbf{N}_{>0}$ pour tout $i \in \{1,\dots,r\}$). Par définition, pour tout $i \in \{1,\dots,r\}$, il existe $x_i \in G$ d'ordre divisible par $p_i^{\alpha_i}$. En remplaçant x_i par une puissance convenable, on peut supposer x_i d'ordre $p_i^{\alpha_i}$ exactement. Le lemme 2.1.34 implique alors que $x_1 \cdots x_r \in G$ est d'ordre $\mu(G)$. □

3. On dit que l'application $\varphi\colon \mathbf{N}_{>0} \to \mathbf{C}$ est *multiplicative*.

Lemme 2.1.37. Soit K un corps commutatif. Tout sous-groupe fini de $K^\times$ est cyclique.

Démonstration. Soit $G \leqslant K^\times$ un sous-groupe fini. Notons d son exposant. D'après le théorème de Lagrange, les éléments de G sont racines du polynôme $X^d - 1$. Dans un corps commutatif, un polynôme de degré d a au plus d racines : cela implique que $\#G \leqslant d$. Comme $d \mid \#G$, on a en fait $\#G = d$. D'après le lemme 2.1.36, G contient un élément d'ordre d : il est cyclique. □

Démonstration de la proposition 2.1.33. • Le lemme 2.1.37 appliqué à $G = (\mathbf{Z}/p\,\mathbf{Z})^\times$ et $K = \mathbf{Z}/p\,\mathbf{Z}$ implique que $(\mathbf{Z}/p\,\mathbf{Z})^\times$ est cyclique (dans la pratique, il n'est pas du tout évident de trouver un générateur explicitement) : soit θ un générateur. Soit $\overline{x} \in \mathbf{Z}/p^\alpha\,\mathbf{Z}$ un antécédent de θ par la surjection $\mathbf{Z}/p^\alpha\,\mathbf{Z} \to \mathbf{Z}/p\,\mathbf{Z}$: on a $\overline{x} \in (\mathbf{Z}/p^\alpha\,\mathbf{Z})^\times$. Comme θ est d'ordre $p-1$, l'ordre de $\overline{x}$ est divisible par $p-1$: quitte à remplacer $\overline{x}$ par une puissance, on peut supposer $\overline{x}$ d'ordre $p-1$ exactement.
• Montrons que l'image $\overline{y}$ de $y = 1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\,\mathbf{Z})^\times$. Il s'agit de voir que $(1+p)^{p^{\alpha-1}} \equiv 1 \mod p^\alpha$ mais que $(1+p)^{p^{\alpha-2}} \not\equiv 1 \mod p^\alpha$: il suffit de montrer que pour tout $k \in \mathbf{N}$, on a $v_p\big((1+p)^{p^k} - 1\big) = k+1$, ce qu'on fait par récurrence sur k. Le cas $k = 0$ est trivial : supposons $k > 0$. Par hypothèse de récurrence, on peut écrire $(1+p)^{p^{k-1}} = 1 + p^k\lambda_k$ avec $\lambda_k \in \mathbf{Z}\setminus p\,\mathbf{Z}$. D'après la formule du binôme, on a

$$(1+p)^{p^k} = (1+p^k\lambda_k)^p = 1 + p^{k+1}\lambda_{k+1}$$

avec $\lambda_{k+1} = \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} p^{k(i-1)}\lambda_k^i + p^{k(p-1)-1}\lambda_k^p$. On a $\lambda_{k+1} - \lambda_k = \sum_{i=2}^{p-1} \frac{1}{p}\binom{p}{i} p^{k(i-1)}\lambda_k^i + p^{k(p-1)-1}\lambda_k^p \in p\,\mathbf{Z}$ car $k > 0$ et $p > 2$, ce qui implique que $\lambda_{k+1} \notin p\,\mathbf{Z}$, et achève la récurrence.
• Comme les ordres de $\overline{x}$ et $\overline{y}$ sont $p-1$ et $p^{\alpha-1}$, premiers entre eux, le lemme 2.1.34 implique que $\overline{xy}$ est d'ordre $(p-1)p^{\alpha-1} = \varphi(p^\alpha)$ (*cf* proposition 2.1.29) : c'est un générateur de $(\mathbf{Z}/p^\alpha\,\mathbf{Z})^\times$. □

Remarque. On a $(\mathbf{Z}/2\,\mathbf{Z})^\times = \{\overline{1}\}$, $(\mathbf{Z}/4\,\mathbf{Z})^\times = \{\pm\overline{1}\}$. Lorsque $\alpha \geqslant 3$, le groupe $(\mathbf{Z}/2^\alpha\,\mathbf{Z})^\times$ n'est pas cyclique. On montre comme plus haut que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbf{Z}/2^\alpha\,\mathbf{Z})^\times$ (petite récurrence), puis que l'application

$$\begin{aligned}\{\pm 1\} \times (\mathbf{Z}/2^{\alpha-2}\,\mathbf{Z}) &\to (\mathbf{Z}/2^\alpha\,\mathbf{Z})^\times \\ (\varepsilon, \overline{k}) &\mapsto \varepsilon 5^k\end{aligned}$$

est un isomorphisme. En utilisant le théorème des restes chinois, cela montre que les seules valeurs de $n \in \mathbf{N}_{>0}$ pour lesquelles $(\mathbf{Z}/n\,\mathbf{Z})^\times$ est cyclique sont celle de la forme 2, 4, p^α et $2p^\alpha$ avec p premier impair et $\alpha \in \mathbf{N}_{>0}$.

Mentionnons quelques applications des anneaux $\mathbf{Z}/n\,\mathbf{Z}$.

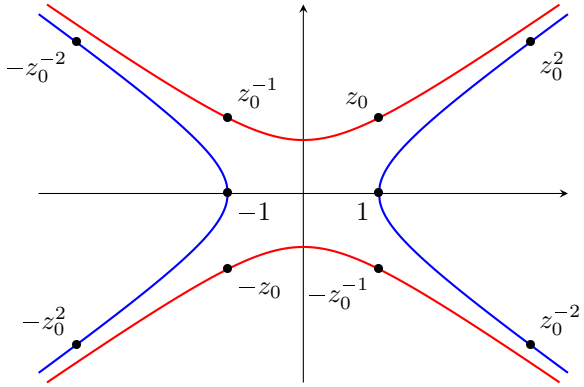
ÉQUATIONS DIOPHANTIENNES. Considérons l'équation diophantienne $3x^2 + 2 = y^2$: modulo 3, cela donne $\overline{y}^2 = \overline{2}$ dans $\mathbf{Z}/3\,\mathbf{Z}$. Comme les carrés de $\mathbf{Z}/3\,\mathbf{Z}$ sont $\overline{0}$ et $\overline{1}$, il n'y a pas de solution.
Considérons l'équation diophantienne $x^2 + y^2 = 2019$. Modulo 4, on a $\overline{x}^2 + \overline{y}^2 = \overline{3}$. Par ailleurs, on a $\overline{x}^2, \overline{y}^2 \in \{\overline{0}, \overline{1}\}$, de sorte que $\overline{x}^2 + \overline{y}^2 \in \{\overline{0}, \overline{1}, \overline{2}\}$: contradiction. L'équation n'a donc pas de solution. Par contre $x^2 + y^2 = 2020$ a des solutions $(\{(\pm 16, \pm 42), (\pm 42, \pm 16), (\pm 24, \pm 38), (\pm 38, \pm 24)\})$. L'équation $x^2 + y^2 = 2021 = 43 \times 47$ n'a quant à elle pas de solution : en réduisant modulo 43, on obtient $\overline{x}^2 + \overline{y}^2 = 0$ dans le corps $\mathbf{Z}/43\,\mathbf{Z}$; si x ou y n'est pas divisible par 43, alors $-\overline{1}$ est un carré dans $\mathbf{Z}/43\,\mathbf{Z}$, ce qui n'est pas (vérification facile) ; cela implique que x et y sont divisibles par 43, et donc $43^2 \mid 2021$, ce qui est absurde.
Les entiers n tels que l'équation diophantienne $x^2 + y^2 = n$ a des solutions sont décrits dans la proposition 2.6.31.

Un exemple classique est l'équation de Pell-Fermat : soit $d \in \mathbf{N}_{>0}$ sans facteur carré. On s'intéresse aux solutions entières de l'équation $x^2 - dy^2 = \pm 1$, c'est-à-dire aux points à coordonnées entières sur la réunion des deux hyperboles d'équations $x^2 - dy^2 = 1$ et $x^2 - dy^2 = -1$. On introduit $\mathbf{Q}(\sqrt{d}) = \{u + v\sqrt{d}\,;\, u, v \in \mathbf{Q}\}$: c'est un sous-corps de $\mathbf{R}$, extension de degré 2 de $\mathbf{Q}$. L'équation se réécrit $N(x + \sqrt{dy}) = \pm 1$, où

$$\begin{aligned}N \colon K &\to \mathbf{Q} \\ u + v\sqrt{d} &\mapsto u^2 - dv^2\end{aligned}$$

(on a $N(u + v\sqrt{d}) = (u + v\sqrt{d})(u - v\sqrt{d})$, où $u - v\sqrt{d}$ est la quantité conjuguée à $u + v\sqrt{d}$). On dispose de l'anneau $A = \mathbf{Z}[\sqrt{d}] \subset K$: c'est l'ensemble des $u + v\sqrt{d}$ avec $u, v \in \mathbf{Z}$. Tout le problème se ramène donc à déterminer l'ensemble des $z = x + y\sqrt{d} \in A$ tels que $N(z) \in \{\pm 1\}$, *i.e.* tels que $z \in A^\times$. Cela montre en particulier que l'ensemble des solutions de l'équation a une strucure de groupe abélien. Un théorème général de théorie des nombres implique que ce groupe isomorphe à $(\mathbf{Z}/2\,\mathbf{Z}) \times \mathbf{Z}$. En particulier, il existe une *unité fondamentale* $z_0 = x_0 + y_0\sqrt{d} \in A^\times$ telle que toute unité soit de la forme $\pm z_0^k$ avec $k \in \mathbf{Z}$. En développant, on peut écrire $z_0^k = x_k + y_k\sqrt{d}$ avec $x, k, y_k \in \mathbf{Z}$ pour tout $k \in \mathbf{Z}$, et l'ensemble des solutions de l'équation est alors $\{\pm(x_k, y_k)\}_{k \in \mathbf{Z}}$.

Exemple 2.1.38. Si $d = 2$, une unité fondamentale est $z_0 = 1 + \sqrt{2}$. Comme $z_0^8 = 577 + 408\sqrt{2}$, le couple $(577, 408)$ est solution de $x^2 - 2y^2 = 1$.



Remarque. Si $(x,y) \in \mathbf{Z}^2$ est solution de l'équation $x^2 - dy^2 = \pm 1$, avec $x, y > 0$, on a $x - y\sqrt{d} = \frac{\pm 1}{x+y\sqrt{d}}$, ce qui montre que $\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2\sqrt{y}}$. Le rationnel $\frac{x}{y}$ est donc une très bonne approximation du réel $\sqrt{d}$. En fait, les solutions de l'équation de Pell-Fermat sont reliées au *développement en fraction continue* du réel $\sqrt{d}$, qui permet de trouver une unité fondamentale.

Exercices. Montrer que $x^2 = 2^n - 1$ n'a pas de solution entière si $n > 1$.
Déterminer les entiers naturels y et n tels que $y^2 = 2^n + 1$.

Remarque. (Carrés de $\mathbf{Z}/n\mathbf{Z}$). C'est un problème classique et important. Le cas central est celui où n est premier. C'est trivial lorsque $n = 2$: supposons $n > 2$. Les applications

$$c\colon (\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times$$
$$\overline{x} \mapsto \overline{x}^2$$
$$\left(\tfrac{\div}{n}\right)\colon (\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times$$
$$\overline{x} \mapsto \overline{x}^{\frac{n-1}{2}}$$

sont des morphismes de groupes (multiplicatifs). Comme $\mathbf{Z}/n\mathbf{Z}$ est un corps, on a $\#\mathsf{Ker}(c) \leqslant 2$, et donc $\mathsf{Ker}(c) = \{\pm 1\}$. Cela implique que le groupe des carrés non nuls $\mathsf{Im}(c)$ est d'ordre $\frac{n-1}{2}$. D'après le théorème de Lagrange, on a $\mathsf{Im}(c) \subset \mathsf{Ker}\left(\frac{\div}{n}\right)$, ce qui montre que $\frac{n-1}{2} \mid \#\mathsf{Ker}\left(\frac{\div}{n}\right)$. Comme $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique, l'application $\left(\frac{\div}{n}\right)$ n'est pas triviale : on a nécessairement $\#\mathsf{Ker}\left(\frac{\div}{n}\right) = \frac{n-1}{2}$, de sorte que

$$\mathsf{Ker}\left(\tfrac{\div}{n}\right) = \mathsf{Im}(c)$$

est le groupe des carrés non nuls de $\mathbf{Z}/n\mathbf{Z}$. Par ailleurs, on a $\#\,\mathsf{Im}\left(\frac{\div}{n}\right) = 2$, ce qui montre que

$$\mathsf{Im}\left(\tfrac{\div}{n}\right) = \{\pm 1\}.$$

Par abus, on dispose donc d'un morphisme de groupes surjectif

$$\left(\tfrac{\div}{n}\right)\colon (\mathbf{Z}/n\mathbf{Z})^\times \to \{\pm 1\}$$

et $\overline{x} \in (\mathbf{Z}/n\mathbf{Z})^\times$ est un carré si et seulement si $\left(\frac{\overline{x}}{n}\right) = 1$. Cela montre en particulier que si $\overline{x}, \overline{y} \in (\mathbf{Z}/n\mathbf{Z})^\times$ ne sont pas des carrés, alors le produit $\overline{xy}$ est un carré dans $(\mathbf{Z}/n\mathbf{Z})^\times$.

Méthodes de cryptage. On identifie un texte (ou une partie de texte) avec un élément de $\mathbf{Z}/n\mathbf{Z}$ avec $n \in \mathbf{N}_{>1}$ convenable fixé à l'avance. On cherche à crypter les textes au moyen d'une opération de codage

$$C\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$

et à les décoder au moyen d'une opération de décodage

$$D\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$

de sorte que $D \circ C = \mathsf{Id}_{\mathbf{Z}/n\mathbf{Z}}$. Les méthodes naïves ($C$ donné par une application affine) sont bien trop faibles. La méthode moderne la plus connue (et élémentaire) est la méthode RSA [4]. On se donne deux entiers premiers distincts p et q (très grands et secrets) et on pose $n = pq$. On dispose de $\varphi(n) = (p-1)(q-1)$ (secret lui aussi, et difficile à calculer en connaissant seulement n et pas sa factorisation). Choisissons un entier e (public) premier à $\varphi(n)$: il existe un entier d tel que $ed \equiv 1 \mod \varphi(n)$. Comme $\varphi(n)$ est secret, il en est de même de d. Posons

$$C\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$
$$\overline{x} \mapsto \overline{x}^e$$
$$D\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$
$$\overline{x} \mapsto \overline{x}^d$$

4. Initiales des inventeurs : Ronald Rivest, Adi Shamir et Leonard Adleman.

Comme $ed \equiv 1 \mod \varphi(n)$, on a $ed \equiv 1 \mod p-1$: le petit théorème de Fermat implique que $x^{ed-1} \equiv 1 \mod p$ et donc $x^{ed} \equiv x \mod p$ lorsque $x \in \mathbf{Z}\backslash p\mathbf{Z}$. C'est encore vrai lorsque $p \mid x$: on a $x^{ed} \equiv x \mod p$ pour tout $x \in \mathbf{Z}$. De même, on a $x^{ed} \equiv x \mod q$ pour tout $x \in \mathbf{Z}$. Comme $\mathbf{Z}/n\mathbf{Z} \simeq (\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ en vertu du théorème des restes chinois, on a donc $\overline{x}^{ed} = \overline{x}$ pour tout $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$. Cela prouve que C et D sont des bijections réciproques l'une de l'autre : elles permettent donc de coder et décoder des messages.

Définition 2.1.39. Le couple (n, e) s'appelle la *clé publique*, l'entier d la *clé privée*.

Remarque. Comme on le voit, cette méthode repose sur la difficulté de factoriser un grand nombre entier.

MÉTHODES DE CODAGE. Quand on transmet une information par un canal de communication (câble téléphonique, Internet, CD, DVD), les données peuvent être corrompues : on crée de la redondance pour pouvoir détecter, voire corriger les erreurs. La méthode standard consiste à utiliser des *codes correcteurs* (linéaires) : on prend les messages dans un sous-espace vectoriel $V \subset (\mathbf{Z}/2\mathbf{Z})^N$. Génériquement, une erreur fera « sortir » le message de V. Si le message transmis est suffisamment « proche » d'un *mot* dans V, on le corrige en le remplaçant par ce dernier. La notion d'écart entre deux mots correspond à une distance (la *distance de Hamming*) sur V : elle est donnée par le nombre de coordonées qui diffèrent entre les deux mots considérés. Pour être efficace, il faut faire un compromis entre la dimension de V (si elle est trop petite par rapport à N, on utilisera beaucoup d'octets pour coder peu de messages, si elle est trop grande, on pourra détecter et corriger moins d'erreurs) et la *distance minimale* du code (qui correspond à l'écart minimal entre deux mots du code, et détermine la capacité de correction du code).

2.1.40. *Les corps* $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. L'anneau $\mathbf{Z}$ est très beau, mais il a le « défaut » de ne pas être un corps (on ne peut pas inverser 2 dans $\mathbf{Z}$). On construit son *corps des fractions* $\mathbf{Q}$ par une construction analogue à celle qui nous a permis de construire $\mathbf{Z}$ à partir de $\mathbf{N}$.
On munit $X = \mathbf{Z} \times \mathbf{Z}\backslash\{0\}$ de la relation binaire $\mathcal{R}$ définie par

$$(a_1, b_1)\mathcal{R}(a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1.$$

C'est une relation d'équivalence : on note $\mathbf{Q} = X/\mathcal{R}$ l'ensemble quotient, et si $(a, b) \in X$, on note $\frac{a}{b}$ son image dans $\mathbf{Q}$. Soit $(a, b) \in X$. Si $(a_1, b_1)\mathcal{R}(a_2, b_2)$ dans X, alors $(ab_1 + a_1 b, bb_1)\mathcal{R}(ab_2 + a_2 b, bb_2)$ et $(aa_1, bb_1)\mathcal{R}(aa_2, bb_2)$. Cela montre que si $(a_1, b_1), (a_2, b_2) \in X$, les expressions $\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$ et $\frac{a_1 a_2}{b_1 b_2}$ ne dépendent que des classes $x_1 := \frac{a_1}{b_1}$ et $x_2 := \frac{a_2}{b_2}$: on les note $x_1 + x_2$ et $x_1 x_2$ respectivement. Il est élémentaire, mais assez fastidieux, de montrer que les opérations $+$ et $.$ ainsi définies munissent $\mathbf{Q}$ d'une structure d'anneau (l'élément neutre pour $+$ est $0 = \frac{0}{1}$ et l'élément neutre pour $.$ est $1 = \frac{1}{1}$). C'est en fait un corps : si $x \in \mathbf{Q}\backslash\{0\}$, on a $x = \frac{a}{b}$ avec $(a, b) \in X$ et $a \neq 0$, et on a $x\frac{b}{a} = 1$. L'application $\mathbf{Z} \to \mathbf{Q}$; $a \mapsto \frac{a}{1}$ est le morphisme canonique.
On a la propriété universelle suivante : si K est un corps de caractéristique 0, le morphisme canonique $f\colon \mathbf{Z} \to K$ est injectif. Il se prolonge de façon unique en un morphisme d'anneaux $f\colon \mathbf{Q} \to K$ (on a bien entendu $f\left(\frac{a}{b}\right) = f(a)f(b)^{-1}$ pour tout $(a, b) \in X$). On dit que $\mathbf{Q}$ est le *corps des fractions* de $\mathbf{Z}$: c'est le « plus petit » corps qui contient $\mathbf{Z}$. Ses éléments s'appellent les rationnels.
Soient $(a, b) \in X$ et $d = \mathsf{pgcd}(a, b)$: on peut écrire $a = da'$ et $b = db'$, et on a $\frac{a}{b} = \frac{a'}{b'}$. On peut donc toujours écrire un rationnel sous la forme $\frac{a}{b}$ avec $\mathsf{pgcd}(a, b) = 1$: on parle alors de *fraction irréductible*. Observons que quitte à multiplier $(a, b) \in X$ par -1, on peut se restreindre aux couples $(a, b) \in X$ pour lesquels $b > 0$.
La relation d'ordre $\leqslant$ s'étend à $\mathbf{Q}$: si $x_1 = \frac{a_1}{b_1}$ et $x_2 = \frac{a_2}{b_2}$ avec $b_1, b_2 > 0$, on a $x_1 \leqslant x_2 \Leftrightarrow a_1 b_2 \leqslant a_2 b_1$ (il faut vérifier que ça ne dépend effectivement que de x_1 et x_2, et que c'est bien une relation d'ordre, ce qui est trivial). Cela permet en particulier de prolonger la valeur absolue à $\mathbf{Q}$.
Signalons l'extension immédiate du théorème 2.1.19 : pour $p \in \mathbb{P}$, la valuation p-adique $v_p\colon \mathbf{Z} \to \mathbf{N} \cup \{+\infty\}$ se prolonge naturellement en $v_p\colon \mathbf{Q} \to \mathbf{Z} \cup \{+\infty\}$ en posant $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$ (cela ne dépend que de $\frac{a}{b}$ et pas de $(a, b) \in X$). Tout élément $x \in \mathbf{Q}^\times$ s'écrit alors de façon unique

$$x = \mathsf{sign}(x) \prod_{p \in \mathbb{P}} p^{v_p(x)}$$

(le produit est fini parce que $v_p(x) = 0$ pour tout $p \in \mathbb{P}$ sauf un nombre fini).

On est très contents avec $\mathbf{Q}$, mais il se révèle rapidement limité : les grecs savaient que l'hypoténuse d'un triangle rectangle isocèle de côté 1 n'est pas rationnel, *i.e.* que le polynôme $X^2 - 2$ n'a pas de racine dans $\mathbf{Q}$. Cela dit, il est possible de trouver des rationnels aussi « proches » d'être une solution qu'on veut. Il est donc nécessaire de compléter $\mathbf{Q}$, en lui adjoignant tous les éléments « limites » de rationnels (en un sens convenable). Bien entendu, comme on parle de limites, on commence à empiéter sur le monde de l'analyse : la construction n'est pas purement algébrique (mais un peu quand même).

Définition 2.1.41. Une suite $(x_n)_{n \in \mathbf{N}}$ de rationnels est dite de *Cauchy* (resp. tend vers 0) si pour tout $\varepsilon \in \mathbf{Q}_{>0}$, il existe $N \in \mathbf{N}$ tel que $|x_m - x_n| < \varepsilon$ dès que $N \leqslant n \leqslant m$ (resp. tel que $|x_n| < \varepsilon$ dès que $N \leqslant n$).

Remarque. L'ensemble des suites de Cauchy, muni de l'addition et de la multiplication terme à terme, est une anneau (et même une $\mathbf{Q}$-algèbre) : notons-le $\mathscr{C}$. L'ensemble $\mathscr{I}$ des suites qui tendent vers 0 est un idéal de $\mathscr{C}$. On dispose en outre du morphisme $\iota\colon \mathbf{Q} \to \mathscr{C}$ qui à $x \in \mathbf{Q}$ associe la suite constante égale à x.

Définition 2.1.42. On note $\mathbf{R} = \mathscr{C}/\mathscr{I}$ l'anneau quotient.

Notons $\pi\colon A \to \mathbf{R}$ la surjection canonique.

Théorème 2.1.43. (1) L'idéal $\mathscr{I} \subset \mathscr{C}$ est maximal, donc $\mathbf{R}$ est un corps. Le composé $\pi \circ \iota\colon \mathbf{Q} \to \mathbf{R}$ est injectif : il permet de voir $\mathbf{Q}$ comme un sous-corps de $\mathbf{R}$.
(2) Si $(x_n)_{n\in\mathbf{N}}, (y_n)_{n\in\mathbf{N}} \in \mathscr{C}$ ont pour images x et y dans $\mathbf{R}$, on écrit $x \leqslant y$ si $x = y$ ou s'il existe $\varepsilon \in \mathbf{Q}_{>0}$ tel que $x_n + \varepsilon \leqslant y_n$ pour $n \gg 0$. Cela définit une relation d'ordre total sur $\mathbf{R}$, qui prolonge celle sur $\mathbf{Q}$. Cela permet en particulier de définir la *valeur absolue* $|.|$ sur $\mathbf{R}$ (qui prolonge celle sur $\mathbf{Q}$).
(3) L'espace métrique $(\mathbf{R}, |.|)$ est complet (*i.e.* toutes les suites de Cauchy de $\mathbf{R}$ convergent).
(4) (Propriété universelle) Si $(K, |.|)$ est un corps valué complet contenant $\mathbf{Q}$, et dont la valeur absolue $|.|$ induit la valeur absolue « habituelle » sur $\mathbf{Q}$[5], alors il existe un unique morphisme de corps valués $\mathbf{R} \to K$.

Démonstration. Un peu longue est assez fastidieuse (mais facile). □

Remarques. (1) Si $(x_n)_{n\in\mathbf{N}} \in \mathscr{C}$ et $x = \pi((x_n)_{n\in\mathbf{N}}) \in \mathbf{R}$, la définition de la relation d'ordre sur $\mathbf{R}$ implique que si $\alpha \in \mathbf{Q}_{>0}$, il existe $N \in \mathbf{N}$ tel que $|x_n - x| < \alpha$ pour tout $n \in \mathbf{N}$. Cela montre que $x = \pi((x_n)_{n\in\mathbf{N}} = \lim\limits_{n\to\infty} x_n$: on a bien complété $\mathbf{Q}$ en lui adjoignant les limites de toutes ses suites de Cauchy.
(2) Le corps ordonné $\mathbf{R}$ a la propriété de la borne supérieure. En effet, soit $E \subset \mathbf{R}$ une partie non vide et majorée. Soient $x \in E$ et $M \in \mathbf{R}$ un majorant de E. On construit par dichotomie des suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$ de réels tels que la suite $(x_n)_{n\in\mathbf{N}}$ soit croissante, $(y_n)_{n\in\mathbf{N}}$ décroissante et $x_n \in E$ et y_n est un majorant de E pour tout $n \in \mathbf{N}$. On procède de la façon suivante. On pose $x_0 = x$ et $y_0 = M$. Si $x_0, \dots, x_n$ et $y_0, \dots, y_n$ sont construits, on pose

$$(x_{n+1}, y_{n+1}) = \begin{cases} \left(x_n, \frac{x_n+y_n}{2}\right) & \text{si } \frac{x_n+y_n}{2} \text{ est un majorant de } E, \\ \left(\frac{x_n+y_n}{2}, y_n\right) & \text{sinon.} \end{cases}$$

Les suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$ sont adjacentes : elles sont en particulier de Cauchy. Elles convergent donc dans $\mathbf{R}$ (par complétude) vers une limite commune ℓ, qui est la borne supérieure de E.

À partir de là, on peut faire de l'analyse sur $\mathbf{R}$: on définit en particulier la continuité, et on prouve le théorème des valeurs intermédiaires.

Remarque. Comme $\mathbf{R}$ n'est pas dénombrable alors que $\mathbf{Q}$ l'est, on a rajouté beaucoup d'éléments.

Tout cela est très beau, mais $\mathbf{R}$ est encore un peu trop petit : il y a encore des polynômes non constants qui n'ont pas de racine (comme $X^2 + 1$).

Définition 2.1.44. On note $\mathbf{C}$ un corps de rupture du polynôme $X^2 + 1$ sur $\mathbf{R}$. Il s'agit de l'anneau quotient

$$\mathbf{R}[X]/\langle X^2 + 1\rangle.$$

On a $\mathbf{C} = \mathbf{R}[i] = \mathbf{R} \oplus \mathbf{R}\, i$ où i désigne l'image de X dans le quotient.

Remarque. Il existe aussi une très jolie construction de $\mathbf{C}$ en le voyant plongé dans $\mathsf{M}_2(\mathbf{R})$.

Comme c'est un $\mathbf{R}$-espace vectoriel de dimension 2, il est essentiellement trivial que $\mathbf{C}$ est complet lui aussi. Le « miracle », c'est qu'en rajoutant seulement une racine carré de -1, on obtient un corps *algébriquement clos*, c'est-à-dire dans lequel tout polynôme non constant a une racine.

Théorème 2.1.45. (d'Alembert-Gauss). Le corps $\mathbf{C}$ est algébriquement clos.

Démonstration. Soit $P \in \mathbf{C}[X] \setminus \mathbf{C}$. On a $\lim\limits_{|z|\to\infty} |P(z)| = +\infty$. Il existe donc $r \in \mathbf{R}_{>0}$ tel que $|z| > r \Rightarrow |P(z)| > |P(0)|$. On a donc $\inf\limits_{z\in\mathbf{C}} |P(z)| = \inf\limits_{z\in D_r} |P(z)|$, avec $D_r = \{z \in \mathbf{C}\,;\, |z| \leqslant r\}$. Comme D_r est compact, l'inf est atteint : il existe donc $z_0 \in D_r$ tel que $|P(z)| \geqslant |P(z_0)|$ pour tout $z \in \mathbf{C}$. Supposons $P(z_0) \neq 0$: quitte à remplacer $P(X)$ par $P(z_0)^{-1}P(X + z_0)$, on peut supposer que $z_0 = 0$ et que $P(0) = 1$. On peut donc écrire $P(X) = 1 + aX^n(1 + XQ(X))$ avec $a \in \mathbf{C}^\times$, $n \in \mathbf{N}_{>0}$ et $Q \in \mathbf{C}[X]$. Écrivons $a = \rho e^{i\theta}$ avec $\rho \in \mathbf{R}_{>0}$ et $\theta \in \mathbf{R}$ et posons $z = te^{i\frac{\pi-\theta}{n}}$ avec $t \in \mathbf{R}_{>0}$: on a $P(z) = 1 - \rho t^n + \mathsf{O}(t^{n+1})$ quand t tend vers 0. Cela implique que $|P(z)| < 1$ pour t assez petit : contradiction. □

Remarque. Autre preuve (tirée de [3, p.53]), et ne faisant pas appel à l'exponentielle.
• Commençons par observer que tout polynôme de degré 2 à coefficients dans $\mathbf{C}$ est scindé. Cela provient de la formule pour les racines d'un polynôme de degré 2, et le fait que tout nombre complexe admet une racine carrée[6].
• Soit $P \in \mathbf{C}[X]$ un polynôme non constant : on veut montrer qu'il a une racine dans $\mathbf{C}$. Quitte à le remplacer par $P\overline{P} \in \mathbf{R}[X]$, on peut supposer que $P \in \mathbf{R}[X]$. On peut en outre supposer P unitaire. Écrivons alors $d = \deg(P) = 2^n m$ avec $m \in \mathbf{N}$ impair : on procède par récurrence sur n. Lorsque $n = 0$, le degré d est impair, et le résultat découle du théorème des valeurs intermédiaires (un a donc une racine dans $\mathbf{R}$). Supposons $n > 0$ et soit $K/\mathbf{C}$ un corps de décomposition (*i.e.* engendré par les racines $x_1, \dots, x_d$ de P sur $\mathbf{C}$). Soient $c \in \mathbf{R}$ et $y_{i,j} = x_i + x_j + cx_ix_j \in K$ (pour $1 \leqslant i \leqslant j \leqslant d$). Posons

$$Q(X) = \prod_{1\leqslant i\leqslant j\leqslant d} (X - y_{i,j}) \in K[X].$$

Ses coefficient sont, au signe près, les polynômes symétriques élémentaires en les $y_{i,j}$, donc des polynômes symétriques à coefficients dans $\mathbf{R}$ en les racines $x_1, \dots, x_d$. Ce sont donc des polynômes à coefficients dans $\mathbf{R}$ des coefficients de P : ce sont des réels. Il en résulte donc que $Q \in \mathbf{R}[X]$. Comme Q est de degré $\frac{d(d+1)}{2} = 2^{n-1}m(2^n m + 1)$ et $m(2^n m + 1)$ est impair, l'hypothèse de récurrence implique qu'il existe $1 \leqslant i(c) \leqslant j(c) \leqslant d$ tels que $y_{i(c),j(c)} \in \mathbf{C}$, *i.e.*

$$x_{i(c)} + y_{i(c)} + cx_{i(c)}x_{j(c)} \in \mathbf{C}\,.$$

Comme $\mathbf{R}$ est infini, il existe $c < c'$ des réels tels que $i(c) = i(c')$ et $j(c) = j(c')$. On a alors $x_{i(c)} + x_{j(c)}, x_{i(c)}x_{j(c)} \in \mathbf{C}$. Cela signifie que $x_{i(c)}$ et $x_{j(c)}$ sont racines d'un trinôme du second degré à coefficients dans $\mathbf{C}$: d'après ce qu'on a vu plus haut, cela montre que $x_{i(c)}, x_{j(c)} \in \mathbf{C}$, et achève la récurrence.

5. Il en existe beaucoup d'autres!
6. Résoudre $(x + iy)^2 = a + ib$, c'est résoudre les équations $x^2 - y^2 = a$ et $2xy = b$: on a $a^2 + b^2 = (x^2 + y^2)^2$, de sorte que $x^2 + y^2 = \sqrt{a^2 + b^2}$, ce qui permet de déterminer les valeurs de x^2 et y^2 d'où celles de x et y (avec la contrainte $\mathsf{sign}(xy) = \mathsf{sign}(b)$.

2.1.46. *Groupe des nombres complexes de module* 1. Posons

$$U = \{z \in \mathbf{C}\,;\, |z| = 1\}$$

c'est un sous-groupe de $\mathbf{C}^\times$. La série entière

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

a un rayon de convergence infini. Il est facile de vérifier l'équation fonctionnelle

$$(\forall z_1, z_2 \in \mathbf{C})\ \exp(z_1 + z_2) = \exp(z_1)\exp(z_2).$$

Si $z \in \mathbf{C}$, on a donc $\exp(z)\exp(-z) = \exp(0) = 1$, donc $\exp(z) \in \mathbf{C}^\times$. L'application exp est donc un morphisme de groupes $\mathbf{C} \to \mathbf{C}^\times$. Si $z = x + iy \in \mathbf{C}$, on a $\overline{\exp(z)} = \exp(x - iy)$, d'où $|\exp(z)| = \exp(x)$. Il en résulte que $\exp^{-1}(U) = i\,\mathbf{R}$, de sorte que $\mathsf{Ker}(\exp) \subset i\,\mathbf{R}$. Les sous-groupes de $\mathbf{R}$ étant soit denses, soit de la forme $\alpha\,\mathbf{Z}$, il existe $\pi \in \mathbf{R}_{>0}$ unique tel que $\mathsf{Ker}(\exp) = 2i\pi\,\mathbf{Z}$ (sinon, la densité de $\mathsf{Ker}(\exp)$ dans $i\,\mathbf{R}$ et la continuité de exp impliqueraient que $\mathsf{Ker}(\exp) = i\,\mathbf{R}$, ce qui impliquerait que exp est à valeurs réelles, ce qui est contredit par un développement limité en 0). L'application exp induit donc un morphisme injectif $i\,\mathbf{R}/2i\pi\,\mathbf{Z} \xrightarrow{\sim} \exp(i\,\mathbf{R}) \subset U$. Comme exp est continue, ouverte et $\mathbf{R}/2\pi\,\mathbf{Z}$ compact, cela montre que $\exp(i\,\mathbf{R}) = U$ (par connexité). Comme exp induit un isomorphisme $\mathbf{R} \xrightarrow{\sim} \mathbf{R}_{>0}$ (valeurs intermédiares), cela implique que exp: $\mathbf{C} \to \mathbf{C}^\times$ est surjective, et induit un isomorphisme de groupes $\mathbf{C}/2i\pi\,\mathbf{Z} \xrightarrow{\sim} \mathbf{C}^\times$. Comme on l'a vu,

$$\begin{aligned} \mathbf{R}/\mathbf{Z} &\to U \\ t &\mapsto \exp(2i\pi t) \end{aligned}$$

est un isomorphisme. En particulier, on a un isomorphisme de groupes

$$\begin{aligned} \mathbf{R}_{>0} \times (\mathbf{R}/\mathbf{Z}) &\xrightarrow{\sim} \mathbf{C}^\times \\ (r, t) &\mapsto r\exp(2i\pi t). \end{aligned}$$

Définition 2.1.47. Si $n \in \mathbf{N}_{>0}$, on pose $U_n = \{z \in \mathbf{C}\,;\, z^n = 1\}$. C'est un sous-groupe de $\mathbf{C}^\times$, dont les éléments sont appelé *racines n-ièmes de l'unité*.

Lemme 2.1.48. Les sous-groupes finis de $\mathbf{R}/\mathbf{Z}$ sont cycliques, de la forme $\frac{1}{n}\,\mathbf{Z}/\mathbf{Z}$ pour $n \in \mathbf{N}_{>0}$.

Démonstration. Soit $G \subset \mathbf{R}/\mathbf{Z}$ un sous-groupe fini, n son ordre. Si $x \in \mathbf{R}$ est tel que $\overline{x} = x + \mathbf{Z} \in G$, le théorème de Lagrange implique que $n\overline{x} = nx + \mathbf{Z} = \mathbf{Z}$, *i.e.* que $nx \in \mathbf{Z}$ soit encore $x \in \frac{1}{n}\,\mathbf{Z}$. Cela montre que $G \subset \frac{1}{n}\,\mathbf{Z}/\mathbf{Z}$. Comme $\frac{1}{n}\,\mathbf{Z}/\mathbf{Z} \simeq \mathbf{Z}/n\,\mathbf{Z}$ est d'ordre n, on a nécessairement $G = \frac{1}{n}\,\mathbf{Z}/\mathbf{Z}$. □

Proposition 2.1.49. L'isomorphisme $\mathbf{R}/\mathbf{Z} \xrightarrow{\sim} U$ induit un isomorphisme $\frac{1}{n}\,\mathbf{Z}/\mathbf{Z} \xrightarrow{\sim} U_n$: les sous-groupes finis de U sont les U_n, et ils sont cycliques.

Démonstration. L'isomorphisme identifie les sous-groupes de n-torsion : ce sont $\frac{1}{n}\,\mathbf{Z}/\mathbf{Z}$ à gauche et U_n à droite. □

Définition 2.1.50. Une racine n-ième de l'unité est dite *primitive* si elle engendre le groupe cyclique U_n, soit encore si c'est un élément d'ordre n dans U. Il y a $\varphi(n)$ racines n-ièmes primitives de l'unité.

Remarque. (1) Si $n, m \in \mathbf{N}_{>0}$, on a $U_n \leqslant U_m \Leftrightarrow n \mid m$.
(2) Explicitement, on a $U_n = \left\{\exp\left(\frac{2ik\pi}{n}\right)\right\}_{k \in \mathbf{Z}/n\,\mathbf{Z}}$. La racine $\exp\left(\frac{2ik\pi}{n}\right)$ est primitive si et seulement si $k \in (\mathbf{Z}/n\,\mathbf{Z})^\times$.

Proposition 2.1.51. On a $n = \sum_{d|n} \varphi(d)$.

Démonstration. On partitionne U_n suivant l'ordre de ses éléments. L'ordre d'un élément de U_n divise n : on a donc $U_n = \bigsqcup_{d|n} U_n(d)$ où $U_n(d)$ désigne l'ensemble des éléments d'ordre d dans U_n. Ces derniers sont précisément les racines primitives d-ièmes de l'unité : il y en a $\varphi(d)$, l'égalité en résulte. □

Remarque. Lorsqu'on identifie « le » plan affine avec le corps $\mathbf{C}$ (en choisissant une base affine et en associant son affixe à un point), l'ensemble des nombres complexes de module 1 correspond au cercle unité. Si $n \in \mathbf{N}_{>1}$, les points de U_n forment les sommets d'un polygone régulier à n côtés.

Exercices. (1) Tout entier admet un multiple dont l'écriture en base 10 n'est composée que de 0 et de 1.

(2) Montrer que $\frac{(2n)!(2m)!}{n!m!(n+m)!}$ et $\frac{(5n)!}{40^n n!}$ sont entiers.

(3) Déterminer $\mathsf{Hom}_{\mathsf{gr}}(\mathbf{Z}/n\,\mathbf{Z}, \mathbf{Z}/m\,\mathbf{Z})$.

(4) Solutions entières de l'équation $x^3 + 2y^3 = 4z^3$.

(5) Quel est le dernier chiffre de $7^{7^{7^{7^{7}}}}$?

(6) Montrer que pour tout entier n premier à 63, on a $n^6 \equiv 1 \mod 63\,\mathbf{Z}$.

2.2. **Polynômes à une indéterminée sur un corps commutatif K.** On fixe un corps commutatif K.

Définition 2.2.1. On pose $K[X] = K^{(\mathbf{N})}$ (resp. $K[\![X]\!] = K^{\mathbf{N}} \supset K[X]$). Si $f = (a_n)_{n\in\mathbf{N}} \in K[\![X]\!]$, on écrit symboliquement $f = \sum_{n=0}^{\infty} a_n X^n$ (on a $X = (0, 1, 0, \ldots)$) : on a $f \in K[X]$ si et seulement si la somme est finie. On munit $K[\![X]\!]$ de la loi + composante par composante : cela munit $K[\![X]\!]$ d'une structure de K-espace vectoriel (et $K[X]$ est un sous-espace vectoriel). On le muni de la loi . définie de la façon suivante : si $f = \sum_{n=0}^{\infty} a_n X^n$ et $g = \sum_{n=0}^{\infty} b_n X^n$, alors $fg = \sum_{n=0}^{\infty} c_n X^n$ avec

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Cela munit $K[\![X]\!]$ d'une structure de d'anneau, et même de K-algèbre, qu'on appelle *algèbre des séries formelles* à coefficients dans K. Bien entendu $K[X]$ est une sous-algèbre : c'est l'*algèbre des polynômes* (à une indéterminée) à coefficients dans K.

Remarque. Si $\theta \in K$, on dispose de l'application

$$\begin{aligned} \mathsf{ev}_\theta \colon K[X] &\to K \\ P = \sum_{n=0}^{d} a_n X^n &\mapsto P(\theta) := \sum_{n=0}^{d} a_n \theta^n \end{aligned}$$

(c'est bien sûr complètement faux quand on remplace $K[X]$ par $K[\![X]\!]$). Il s'agit d'un morphisme de K-algèbres (d'*évaluation en θ*). Un élément $P \in K[X]$ définit donc une application

$$\begin{aligned} \tilde{P} \colon K &\to K \\ \theta &\mapsto P(\theta). \end{aligned}$$

Une telle application est dite *polynômiale*. Il est fondamental de ne pas confondre un polynôme avec l'application polynômiale qu'il définit. Par exemple, si p est un nombre premier et $K = \mathbf{Z}/p\mathbf{Z}$, l'application polynômiale associée à $X^p - X$ est l'application nulle.

Définition 2.2.2. Soit $P = \sum_{n=0}^{\infty} a_n X^n \in K[X]$. Si $P \neq 0$, l'ensemble $\{n \in \mathbf{N}\,;\, a_n \neq 0\}$ est fini non vide : il a un plus grand élément qu'on appelle le *degré* de P et qu'on note $\deg(P)$. Par convention, on pose $\deg(0) = -\infty$.

Proposition 2.2.3. Si $P, Q \in K[X]$, on a $\deg(PQ) = \deg(P) + \deg(Q)$ et $\deg(P + Q) \leqslant \max\{\deg(P), \deg(Q)\}$ (avec égalité lorsque $\deg(P) \neq \deg(Q)$). Par ailleurs, on a $\deg(P) = -\infty \Leftrightarrow P = 0$.

Corollaire 2.2.4. On a $K[X]^\times = K^\times$.

Exercice. Montrer que $K[\![X]\!]^\times = K^\times + XK[\![X]\!]$.

Théorème 2.2.5. (Division euclidienne). Soient $P, D \in K[X]$ avec $D \neq 0$. Il existe un unique couple $(Q, R) \in K[X]$ tel que

$$\begin{cases} P = QD + R \\ \deg(R) < \deg(D) \end{cases}$$

Cette décomposition s'appelle la *division euclidienne* de P par D, le polynôme Q (resp. R) s'appelle le *quotient* (resp. le *reste*) de la division.

Démonstration. • Unicité : soient (Q_1, R_1) et (Q_2, R_2) tels que $P = Q_1 D + R_1 = Q_2 D + R_2$ et $\deg(R_1), \deg(R_2) < \deg(D)$. On a $R_2 - R_1 = (Q_1 - Q_2)D$, donc $\deg(D) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg(D)$. Comme $\deg(D) \in \mathbf{N}$, cela implique que $\deg(Q_1 - Q_2) < 0$, d'où $Q_1 - Q_2 = 0$, *i.e.* $Q_2 = Q_1$, et donc aussi $R_2 = R_1$.
• Existence : si $\deg(D) = 0$, alors D est une constante non nulle, et on a $Q = D^{-1}P$, $R = 0$. Supposons désormais que $\deg(D) > 0$. On procède par récurrence sur $\deg(P)$. Si $0 \leqslant \deg(P) < \deg(D)$, alors $Q = 0$ et $R = P$. Supposons $n := \deg(P) \geqslant d := \deg(D)$. Écrivons $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ et $D = b_d X^d + \cdots + b_0$: on a $a_n, b_d \in K^\times$. Posons $\tilde{P} = P - \frac{a_n}{b_d} X^{n-d} D$: on a $\deg(\tilde{P}) < n$. Par hypothèse de récurrence, il existe $\tilde{Q}, R \in K[X]$ tels que $\tilde{P} = \tilde{Q}D + R$ et $\deg(R) < \deg(D)$. Posons alors $Q = \frac{a_n}{b_d} X^{n-d} + \tilde{Q} \in K[X]$: on a $P = QD + R$. □

Théorème 2.2.6. Les idéaux de $K[X]$ sont principaux, *i.e.* de la forme $\langle P \rangle = PK[X]$ pour $P \in K[X]$ convenable (le polynôme P est unique si on requiert qu'il soit unitaire).

Démonstration. Identique à celle pour les idéaux de $\mathbf{Z}$. □

Comme $K[X]$ est principal, on dispose « du » plus grand commun diviseur (pgcd) et « du » plus petit commun multiple (ppcm) de deux polynômes P et Q non tous nuls (ils sont définis à multiplication par un scalaire non nul près, et donc uniquement si on les prend unitaires). Ce sont des générateurs $\mathsf{pgcd}(P, Q)$ et $\mathsf{ppcm}(P, Q)$ des idéaux $\langle P \rangle + \langle Q \rangle$ et de $\langle P \rangle \cap \langle Q \rangle$ respectivement. Comme on le voit sur ces caractérisations, le pgcd et le ppcm sont bien définis non comme

éléments, mais comme idéaux. Cela dit, on les écrit comme des éléments dans la pratique, même si cela constitue un abus. On définit la notion d'égalité de Bézout comme dans $\mathbf{Z}$, et on dispose de l'algorithme d'Euclide (étendu), à savoir mettre en œuvre.

Définition 2.2.7. Un polynôme non constant $P \in K[X]$ est dit *irréductible* si l'égalité $P = P_1P_2$ dans $K[X]$ implique que P_1 ou P_2 est constant.

Remarque. Les polynômes irréductibles sont donc les éléments non inversibles de $K[X]$ qui sont indécomposables du point de vue de la multiplication (c'est bien entendu une propriété invariante par multiplication par une constante non nulle). Cette notion est l'avatar dans $K[X]$ de la notion de nombre premier dans $\mathbf{Z}$. Tout comme dans $\mathbf{Z}$, si $P \in K[X]$ est irréductible, et si $A \in K[X]$, on a $\mathsf{pgcd}(P, A) \in \{1, P\}$.

Lemme 2.2.8. Soient $P, A, B \in K[X]$ avec P irréductible. Si $P \mid AB$, alors $P \mid A$ ou $P \mid B$.

Démonstration. La preuve est essentiellement identique à celle dans $\mathbf{Z}$. □

Théorème 2.2.9. (Décomposition en produit de facteurs irréductibles). Soit $P \in K[X]\backslash\{0\}$. Il existe $u \in K^\times$ et $P_1, \dots, P_n$ des polynômes irréductibles et unitaires, uniques à l'ordre près, tels que

$$P = uP_1 \cdots P_n.$$

Démonstration. La preuve est là encore essentiellement identique à celle dans $\mathbf{Z}$, à ceci près que l'existence se fait par récurrence sur $\deg(P)$, et l'unicité utilise le lemme 2.2.8. □

Remarque. Une reformulation du théorème 2.2.9 est la suivante : notons $\mathbb{P}$ l'ensemble des polynômes irréductibles et unitaires de $K[X]$. Si $P \in K[X]$, il existe $(v_Q(P))_{Q\in\mathbb{P}} \in \mathbf{N}^{(\mathbb{P})}$ et $u \in K^\times$ uniques tels que

$$P = u \prod_{Q\in\mathbb{P}} Q^{v_Q(P)}.$$

L'entier $v_Q(P)$ s'appelle la valuation Q-adique de P, et les applications v_Q vérifient les mêmes propriétés vis-à-vis de l'addition et la multiplication que leurs homologues sur $\mathbf{Z}$.

Définition 2.2.10. Comme on l'a vu plus haut, un élément $P \in K[X]$ définit une application $\widetilde{P}\colon K \to K$ (la fonction polynômiale associée à P). Une *racine* de P est un élément $\alpha \in K$ tel que $P(\alpha) = 0$.

Remarque. L'application qui à un polynôme associe la fonction polynômiale associée est un morphisme d'anneaux, dont l'image s'appelle l'anneau des fonctions polynômiales.

Proposition 2.2.11. Soient $P \in K[X]\backslash\{0\}$ et $\alpha \in K$ une racine de P. Alors il existe $Q \in K[X]\backslash\{0\}$ unique tel que $P(X) = (X - \alpha)Q(X)$.

Démonstration. Cela résulte de la division euclidienne. □

Définition 2.2.12. Soient $P \in K[X]\backslash\{0\}$ et $\alpha \in K$. Il existe $m \in \mathbf{N}$ et $Q \in K[X]$ uniques tels que $P(X) = (X - \alpha)^m Q(X)$ et $Q(\alpha) \neq 0$. L'élément α est racine de P si et seulement si $m > 0$ (l'entier m s'appelle alors la *multiplicité* de la racine α).

Remarque. Pour des raisons de degré, un polynôme de degré 1 est toujours irréductible : l'entier m ci-dessus n'est autre que la valuation $(X - \alpha)$-adique de P.

Proposition 2.2.13. Soient $P \in K[X]\backslash\{0\}$ et $\alpha_1, \dots, \alpha_r \in K$ des racines de P (non nécessairement distinctes). Alors $r \leqslant \deg(P)$.

Démonstration. On peut écrire $P(X) = Q(X) \prod_{i=1}^{r} (X - \alpha_i)$, et donc $\deg(P) = \deg(Q) + r \geqslant r$. □

Corollaire 2.2.14. Un polynôme $P \in K[X]\backslash\{0\}$ a au plus $\deg(P)$ racines dans K (comptées avec multiplicités).

Définition 2.2.15. (1) Un polynôme $P \in K[X]\backslash\{0\}$ est dit *scindé* s'il est produit de $\deg(P)$ polynômes de degré 1. Explicitement, cela signifie qu'il existe $u, \alpha_1, \dots, \alpha_d \in K$ tels que $u \neq 0$ et $P(X) = u \prod_{i=1}^{d} (X - \alpha_i)$.

(2) Le corps K est dit *algébriquement clos* si tout élément de $K[X]\backslash\{0\}$ est scindé. Un corps est algébriquement clos si et seulement si les polynômes irréductibles sont précisément les polynômes de degré 1.

Remarque. On a vu (*cf* théorème 2.1.45) que $\mathbf{C}$ est algébriquement clos (théorème d'Alembert-Gauss).

Exercice. Montrer que les polynômes irréductibles dans $\mathbf{R}[X]$ sont les polynômes de degré 1 et les trinômes du second degré à discriminant strictement négatif.

Corollaire 2.2.16. Le morphisme qui à un polynôme associe la fonction polynômiale associée est injectif si K est infini.

Démonstration. Si P s'envoie sur 0, cela signifie que tous les éléments de K sont racines : il y a une infinité de racines. D'après le corollaire précédent, on a $P = 0$. □

Remarque. Soient p un nombre premier et $K = \mathbf{Z}/p\mathbf{Z}$. La fonction polynômiale associée à $X^p - X$ est nulle. Si la fonction polynomiale associée à $P \in K[X]$ est nulle, soit $P(X) = (X^p - X)Q(X) + R(X)$ la division euclidienne de P par $X^p - X$: la fonction polynômiale associée à R est nulle. Si $R \neq 0$, alors R a au plus $\deg(R) < p$ racines, ce qui n'est pas : on a $R = 0$, et $P \in \langle X^p - X \rangle$. Cela montre que l'anneau des fonctions polynômiales est isomorphe à $(\mathbf{Z}/p\mathbf{Z})[X]/\langle X^p - X \rangle$.

Définition 2.2.17. Soient $d \in \mathbf{N}_{>0}$ et $T_1, \dots, T_d$ des indéterminées. Si $1 \leqslant k \leqslant d$, le k-ième *polynôme symétrique élémentaire* est

$$\sigma_k(T_1, \dots, T_d) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} T_{i_1} \cdots T_{i_k} \in \mathbf{Z}[T_1, \dots, T_d].$$

Exemple 2.2.18. On a $\sigma_1(T_1, \dots, T_d) = T_1 + \cdots + T_d$ et $\sigma_d(T_1, \dots, T_d) = T_1 \cdots T_d$. Si $d = 3$, on a $\sigma_2(T_1, T_2, T_3) = T_1T_2 + T_2T_3 + T_1T_3$.

Théorème 2.2.19. (Relations entre coefficients et racines d'un polynôme scindé). Soit $P(X) = \sum_{k=0}^{d} a_{d-k}X^k \in K[X]\backslash\{0\}$ scindé, de racines $\alpha_1, \dots, \alpha_d \in K$. Alors on a

$$a_k = (-1)^k a_0 \sigma_k(\alpha_1, \dots, \alpha_d)$$

pour tout $k \in \{1, \dots, d\}$.

Démonstration. Cela résulte de l'égalité

$$\prod_{i=1}^{d}(X - T_i) = X^d + \sum_{k=1}^{d}(-1)^k \sigma_k(T_1, \dots, T_d)X^k$$

dans $\mathbf{Z}[X, T_1, \dots, T_d]$. □

Remarque. Bien entendu, il est facile de calculer les coefficients d'un polynôme connaissant ses racines (ce sont les formules précédentes), mais le contraire n'est pas vrai. Il existe des formules pour $d \in \{2, 3, 4\}$: pour $d = 2$, c'est la formule bien connue $r_\pm = \frac{-b \pm \sqrt{\Delta}}{2a}$ avec $\Delta = b^2 - 4ac$ lorsque $P(X) = aX^2 + bX + c$, pour $d = 3$ (resp. 4) c'est la formule de Cardan (resp. de Ferarri). Ce n'est qu'au XIX$^{\text{ème}}$ siècle qu'Abel et Galois ont montré (indépendamment) qu'il n'existe pas de formule pour $d \geqslant 5$: mieux (ou pire suivant le point de vue), on ne peut pas exprimer, en général, les racines d'un polynôme à partir de ses coefficients en utilisant seulement les quatre opérations et les extractions de racines multiples.

Définition 2.2.20. La *dérivation* sur $K[X]$ est l'unique endomorphisme D de $K[X]$ tel que $D(X^n) = nX^{n-1}$ pour tout $n \in \mathbf{N}$ (on a $D(1) = 0$). Lorsque $P \in K[X]$, on note usuellement $D(P) = P'$. Si $i \in \mathbf{N}$ et $P \in K[X]$, on pose

$$P^{(i)} = \underbrace{D \circ \cdots \circ D}_{i \text{ fois}}(P)$$

qu'on appelle la *dérivée i-ième* de P. Celle de X^n est donc $n(n-1)\cdots(n-i+1)X^{n-i} = i!\binom{n}{i}X^{n-i}$. Cela suggère de considérer l'unique endomorphisme de $K[X]$ qui envoie X^n sur $\binom{n}{i}X^{n-i}$: on le note $P \mapsto P^{[i]}$. Lorsque K est de caractéristique nulle, on a $P^{[i]}(X) = \frac{P^{(i)}}{i!}$.

Théorème 2.2.21. (Identité de Taylor). Soit $P \in K[X]$ de degré d. Alors on a $P(X) - P(T) = \sum_{i=1}^{d} P^{[i]}(T)(X - T)^i$ dans $K[X, Y]$.

Démonstration. Par linéarité des deux membres, il suffit de traiter le cas où $P(X) = X^n$: l'égalité à démontrer n'est alors que la formule de Newton. □

Remarque. Lorsque K est de caractéristique est nulle, en évaluant T en $a \in K$, on retrouve la formule de Taylor usuelle à l'ordre d :

$$P(X) - P(a) = \sum_{i=1}^{d} \frac{P^{(i)}(a)}{i!}(X - a)^i$$

(qui est une égalité).

Exercices. (1) Soient K un corps et $P, Q \in K[X]$. Montrer que P et Q sont premiers entre eux si et seulement si $P + Q$ et PQ sont premiers entre eux.

(2) Calculer le reste dans $\mathbf{Q}[X]$ de la division euclidienne de $(X+2)^{2019}$ par X^2+6X+8, puis de X^{2019} par X^2+2X+1.

(3) Pour tout $P \in K[X]$, montrer que $P(X) - X$ divise $(P \circ P)(X) - X$.

(4) Soient $m, q \in \mathbf{N}_{>0}$. CNS pour que $1 + X + \cdots + X^q$ divise $1 + X^m + \cdots + X^{qm}$.

(5) Soient $P(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{Z}[X]$ avec $a_n \neq 0$ et $x = \frac{u}{v} \in \mathbf{Q}$ une racine de P (avec $\mathsf{pgcd}(u, v) = 1$). Montrer que $u \mid a_0$ et $v \mid a_n$.

(6) Soient $n \in \mathbf{N}_{>0}$ et $P \in \mathbf{R}[X]$ un polynôme de degré n. Montrer qu'il existe $a_0, \dots, a_n \in \mathbf{R}$ tel que le polynôme $\sum_{i=0}^{n} a_iX^{2^i}$ soit divisible par P.

(7) Soit $P \in \mathbf{R}_n[X]$ positif (*i.e.* qui ne prend que des valeurs positives sur $\mathbf{R}$). Montrer qu'il en est de même de $Q = P + P' + P^{(2)} + \cdots + P^{(n)}$.

(8) Soit p un nombre premier. Nombre de polynômes irréductibles de degré 2 (resp. 3) dans $\mathbf{F}_p[X]$.

2.3. **Fractions rationnelles sur un corps commutatif K.** Tout comme on construit $\mathbf{Q}$ à partir de $\mathbf{Z}$ en prenant le corps des fractions, on définit le corps $K(X)$ des fractions rationnelles. Ses éléments peuvent s'écrire comme des fractions $\frac{P}{Q}$ avec $P, Q \in K[X]$ et $Q \neq 0$. Tout comme dans $\mathbf{Q}$, on dispose de la *forme irréductible* d'un élément de $K(X)$ (numérateur et dénominateur premiers entre eux).

Définition 2.3.1. Soient $R \in K(X)$ et $R = \frac{P}{Q}$ sa forme irréductible. Les zéros de P (resp. Q) s'appellent les *zéros* (resp. les *pôles*) de R.les ordres de multiplicité afférents sont ceux de P et Q respectivement.

Remarque. Avec les notations de la définition 2.3.1, la fraction rationnelle R définit l'application

$$\begin{aligned} R\colon K\backslash \mathsf{Z}(Q) &\to K \\ x &\mapsto \frac{P(x)}{Q(x)} \end{aligned}$$

qu'on appelle *fonction rationnelle* associée à R. Comme pour les polynômes, on veillera à ne point confondre fractions et fonctions rationnelles.

Définition 2.3.2. Si $R = \frac{P}{Q} \in K(X)$, on pose $\deg(R) = \deg(P) - \deg(Q) \in \mathbf{Z} \cup \{-\infty\}$, qu'on appelle le *degré* de R (il est immédiat que ça ne dépend que de R et pas de P et Q). Ce degré jouit des mêmes propriété que le degré sur $K[X]$.

Remarque. On peut interpréter l'application $-\deg\colon K(X) \to \mathbf{Z} \cup \{\infty\}$ comme une valuation de la façon suivante. Posons $Y = \frac{1}{X}$: on a $K(X) = K(Y)$. Si $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in K[X]\backslash\{0\}$ avec $d = \deg(P)$, on a

$$P = X^d(a_0 Y^d + \cdots + a_{d-a} Y + a_d) = Y^{-d}(a_0 Y^d + \cdots + a_{d-a} Y + a_d).$$

Comme $a_d \neq 0$, on a $v_Y(a_0 Y^d + \cdots + a_{d-a} Y + a_d) = 0$, de sorte que $v_Y(P) = -d = -\deg(P)$. Il en résulte que $v_Y = -\deg$ sur $K(X)$, de sorte que $-\deg$ est la valuation $1/X$-adique, en d'autres termes, $\deg(R)$ est l'ordre du pôle $+\infty$.

2.4. **Décomposition en éléments simples.** Notons $\mathbb{P}$ l'ensemble des polynômes irréductibles et unitaires dans $K[X]$. La décomposition en produit de facteurs irréductibles dans $K[X]$ implique que si $R \in K(X)^\times$, il existe une famille $(v_P(R))_{P \in \mathbb{P}} \in \mathbf{Z}^{(\mathbb{P})}$ et $u \in K^\times$ uniques tels que

$$R = u \prod_{P \in \mathbb{P}} P^{v_P(R)}.$$

Cela donne une description du groupe multiplicatif $K(X)^\times$ (il est donc isomorphe à $K^\times \times \mathbf{Z}^{(\mathbb{P})}$). Ce qui suit a pour but de comprendre la structure additive de $K(X)$, plus précisément de donner une base de $K(X)$ sur K.

Théorème 2.4.1. La famille $\{X^n\}_{n \in \mathbf{N}} \cup \left\{\frac{X^j}{P^k}\right\}_{\substack{P \in \mathbb{P} \\ 0 \leqslant j < \deg(P) \\ k \in \mathbf{N}_{>0}}}$ est une base de $K(X)$ sur K.

Remarque. Explicitement, cela signifie que si $R = \frac{P}{Q} \in K(X)$ est écrit sous forme irréductible (avec Q unitaire), et si $Q = \prod_{i=1}^{r} P_i^{m_i}$ est la décomposition en produit de facteurs irréductibles de Q, alors il existe $E \in K[X]$ et des polynômes $(A_{i,j})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant m_i}}$ tels que $\deg(A_{i,j}) < \deg(P_i)$ uniques tels que

$$R = E + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{A_{i,j}}{P_i^j}.$$

Le polynôme E s'appelle la *partie entière* de R.

Lemme 2.4.2. Soit $R = \frac{P}{Q} \in K(X)$ tel que $\deg(R) < 0$. Supposons que $Q = Q_1 Q_2$ avec $\mathsf{pgcd}(Q_1, Q_2) = 1$. Alors il existe $P_1, P_2 \in K[X]$ uniques tels que $\deg(P_i) < \deg(Q_i)$ et $R = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}$.

Démonstration. Comme $\mathsf{pgcd}(Q_1, Q_2) = 1$, il existe $U, V \in K[X]$ tels que $UQ_1 + VQ_2 = 1$. En multipliant par R, il vient $R = \frac{VP}{Q_1} + \frac{UP}{Q_2}$. Soit $VP = E_1 Q_1 + P_1$ (resp. $UP = E_2 Q_2 + P_2$) avec $\deg(P_i) < \deg(Q_i)$ la division euclidienne de VP (resp. UP) par Q_1 (resp. Q_2). On a alors $R = E_1 + E_2 + \frac{P_1}{Q_1} + \frac{P_2}{Q_2}$. Comme $\deg(R), \deg\left(\frac{P_1}{Q_1}\right), \deg\left(\frac{P_2}{Q_2}\right) < 0$, on a $\deg(E_1 + E_2) < 0$, ce qui implique que $E_1 + E_2 = 0$, et donc l'existence de l'écriture.
Montrons l'unicité : supposons que $\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{\tilde{P_1}}{Q_1} + \frac{\tilde{P_2}}{Q_2}$ avec $\deg(P_i), \deg(\tilde{P_i}) < \deg(Q_i)$. On a alors

$$(P_1 - \tilde{P_1})Q_2 = (\tilde{P_2} - P_2)Q_1.$$

Comme $\mathsf{pgcd}(Q_1, Q_2) = 1$, cela implique que $Q_i \mid \tilde{P_i} - P_i$: comme $\deg\left(\tilde{P_i} - P_i\right) < \deg(Q_i)$, cela implique que $\tilde{P_i} = P_i$ pour $i \in \{1, 2\}$. □

Démonstration du théorème 2.4.1. Écrivons $R = \frac{P}{Q}$ sous forme irréductible (avec Q unitaire). Soit $P = QE + \tilde{P}$ avec $\deg\left(\tilde{P}\right) < \deg(Q)$ la division euclidienne de P par Q : on a $R = E + \frac{\tilde{P}}{Q}$: cela ramène à traiter le cas où $\deg(R) < 0$ (l'unicité de E, facile, se prouve comme dans la preuve du lemme 2.4.2 en utilisant le degré). Soit

$$Q = \prod_{i=1}^{r} P_i^{m_i}$$

la décomposition de Q en produit de facteurs irréductibles. Le lemme 2.4.2 montre qu'il existe $A_1, \dots, A_r \in K[X]$ uniques tels que $\deg(A_i) < m_i \deg(P_i)$ pour tout $i \in \{1, \dots, r\}$ et

$$R = \sum_{i=1}^{r} \frac{A_i}{P_i^{m_i}}$$

ce qui permet de se ramener au cas où $R = \frac{A_i}{P_i^{m_i}}$ avec $\deg(A_i) < m_i \deg(P_i)$. Si on a

$$R = \sum_{j=1}^{m_i} \frac{A_{i,j}}{P_i^j}$$

comme annoncé, on a $A_i = P_i^{m_i} R = \sum_{j=1}^{m_i} A_{i,j} P_i^{m_i - j}$. Cela montre que la suite $(A_{i,j})_{1 \leqslant j \leqslant m_i}$ est obtenue de la façon suivante : on pose $A_i^{(m_i)} = A_i$ et on construit les suites $(A_i^{(j)})_{1 \leqslant j \leqslant m_i}$ et $(A_{i,j})_{1 \leqslant j \leqslant m_i}$ en disant que

$$A_i^{(j)} = A_i^{(j-1)} P_i + A_{i,j}$$

avec $\deg(A_{i,j}) < \deg(P_i)$ est la division euclidienne de $A_i^{(j)}$ par P_i pour $j = m_i, m_i - 1, \dots, 1$. Cela prouve l'existence et l'unicité de $(A_{i,j})_{1 \leqslant j \leqslant m_i}$. □

Remarque. Avec les notations de la remarque 2.4, on a $\deg(E) = \deg(R)$.

Exemple 2.4.3. • $K = \mathbf{C}$. Comme $\mathbf{C}$ est algébriquement clos, on a $\mathbb{P} = \{X - a\}_{a \in \mathbf{C}}$. Si $R = \frac{P}{Q} \in \mathbf{C}(X)$ est sous forme irréductible, $Q(X) = \prod_{i=1}^{r} (X - a_i)^{m_i}$, il existe $E \in \mathbf{C}[X]$, et des éléments $(\alpha_{i,j})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant m_i}}$ dans $\mathbf{C}$ uniques tels que

$$R(X) = E(X) + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - a_i)^j}.$$

• $K = \mathbf{C}$. On a $\mathbb{P} = \{X - a\}_{a \in \mathbf{C}} \sqcup \left\{X^2 - sX + p\right\}_{\substack{s,p \in \mathbf{R} \\ s^2 - 4p < 0}}$. Si $R = \frac{P}{Q} \in \mathbf{C}(X)$ est sous forme irréductible, $Q(X) = \prod_{i=1}^{r} (X - a_i)^{m_i} \prod_{i=1}^{t} (X^2 - s_i X + p_i)^{n_i}$ (avec $s_i^2 - 4p_i < 0$ pour tout $i \in \{1, \dots, t\}$), il existe $E \in \mathbf{C}[X]$, et des éléments $(\alpha_{i,j})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant m_i}}$, $(\beta_{i,j})_{\substack{1 \leqslant i \leqslant t \\ 1 \leqslant j \leqslant n_i}}$, $(\gamma_{i,j})_{\substack{1 \leqslant i \leqslant t \\ 1 \leqslant j \leqslant n_i}}$ dans $\mathbf{C}$ uniques tels que

$$R(X) = E(X) + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - a_i)^j} + \sum_{i=1}^{t} \sum_{j=1}^{n_i} \frac{\beta_{i,j} X + \gamma_{i,j}}{(X^2 - s_i X + p_i)^j}.$$

Remarque. (1) Ce qui précède montre par exemple que $\dim_{\mathbf{C}}(\mathbf{C}(X)) = \mathsf{Card}(\mathbf{R})$ (alors que $\dim_{\mathbf{C}}(\mathbf{C}[X]) = \mathsf{Card}(\mathbf{N})$). (2) L'application de la décomposition en éléments simples qu'on enseigne en premier cycle est le calcule des primitives et intégrales de fractions rationnelles et rationnelles trigonométriques en utilisant les fonctions « usuelle ».

Exercice. Soit $P \in \mathbf{C}[X]$. Les racines de P' sont dans l'enveloppe convexe des racines de P.

2.5. Éléments algébriques, éléments transcendants.

2.5.1. *Extensions de corps.*

Définition 2.5.2. Une extension de corps est juste un morphisme de corps $K \to L$. Il est automatiquement injectif : on considère souvent $K \subset L$. Le *degré* de l'extension est alors $[L : K] := \dim_K(L)$.

Exemple 2.5.3. $\mathbf{C}/\mathbf{R}$, $\mathbf{R}/\mathbf{Q}$, $\mathbf{Q}(X)/\mathbf{Q}$ sont des extensions. On a $[\mathbf{C} : \mathbf{R}] = 2$, $[\mathbf{R} : \mathbf{Q}] = +\infty$ et $[\mathbf{Q}(X) : \mathbf{Q}] = \infty$. Si $n \in \mathbf{N}_{>0}$, alors $\mathbf{Q}(\sqrt[n]{2}) = \{x_0 + x_1 2^{1/n} + x_2 2^{2/n} + \cdots + x_{n-1} 2^{1-1/n} ; x_0 \dots, x_{n-1} \in \mathbf{Q}\}$ est une extension de degré n de $\mathbf{Q}$.

Théorème 2.5.4. (Transitivité des degrés). Si $K \subset L \subset M$ sont des extensions, alors

$$[M : K] = [M : L][L : K].$$

Démonstration. On se ramène immédiatement au cas où $[M : L]$ et $[L : K]$ sont finis. Soient $(y_j)_{1 \leqslant j \leqslant [M:L]}$ une base de M sur L et $(x_i)_{1 \leqslant i \leqslant [L:K]}$ une base de L sur K. On a $L = \bigoplus_{i=1}^{[L:K]} K x_i$ et $M = \bigoplus_{j=1}^{[M:L]} L y_j$, donc $M = \bigoplus_{\substack{1 \leqslant i \leqslant [L:K] \\ 1 \leqslant j \leqslant [M:L]}} K x_i y_j$ et $(x_i y_j)_{\substack{1 \leqslant i \leqslant [L:K] \\ 1 \leqslant j \leqslant [M:L]}}$ est une base de M sur K. □

2.5.5. *Éléments algébriques, éléments transcendants.* Soit $K \subset L$ des corps. Si $x \in L$, on dispose du morphisme d'anneaux (et même de K-algèbres)

$$\begin{aligned} \mathsf{ev}_x \colon K[X] &\to L \\ P &\mapsto P(x) \end{aligned}$$

On note $K[x] = \mathsf{Im}(\mathsf{ev}_x)$ (resp. $K(x) = \mathsf{Frac}(K[x])$) le sous-anneau (resp. le sous-corps) de L engendré par x.

Définition 2.5.6. On dit que x est *algébrique* (resp. *transcendant*) sur K si $\mathsf{Ker}(\mathsf{ev}_x) \neq \{0\}$ (resp. si $\mathsf{Ker}(\mathsf{ev}_x) = \{0\}$). Si x est algébrique sur K, il existe un unique polynôme *unitaire* $P_{x,K} \in K[X]$ tel que $\mathsf{Ker}(\mathsf{ev}_x) = \langle P_{x,K} \rangle$: on l'appelle le *polynôme minimal* de x sur K.

Supposons x algébrique sur K. Le morphisme ev_x induit, par passage au quotient, un morphisme d'anneaux injectif

$$K[X]/\langle P_{x,K} \rangle \to L.$$

Proposition 2.5.7. Le polynôme $P_{x,K}$ est irréductible dans $K[X]$.

Démonstration. Si $P_{x,K} = P_1 P_2$ dans $K[X]$, on a $P_1(x)P_2(x) = 0$, donc $P_1(x) = 0$ ou $P_2(x) = 0$, de sorte que $P_{x,K} \mid P_1$ ou $P_{x,K} \mid P_1$, et donc P_1 ou P_2 est constant pour des raisons de degré. □

Proposition 2.5.8. Réciproquement, soit $P \in K[X]$ un polynôme irréductible (et unitaire). Alors $K_P := K[X]/\langle P \rangle$ est un corps, extension de degré $d = \deg(P)$ de K (*i.e.* $[K_P : K] = \deg(P)$). Si $\alpha = \overline{X} \in K_P$, alors α est racine de P, et $(1, \alpha, \alpha^2, \dots, \alpha^{d-1})$ est une base de K_P sur K.

Démonstration. La division euclidienne montre que tout élément de K_P est la classe d'un unique élément de $K[X]$ de degré $< d$. Cela montre que $(\overline{1}, \overline{X}, \overline{X}^2, \dots, \overline{X}^{d-1})$ est une K-base de K_P. Si $x \in L\backslash\{0\}$, on peut donc écrire $x = \overline{A}$ avec $A \in K[X]\backslash\{0\}$ de degré $< d$ unique. Comme P est irréductible, on a nécessairement $\mathsf{pgcd}(A, P) = 1$: il existe une relation de Bézout

$$1 = UA + VP$$

de sorte que $1 = x\overline{U}$, ce qui montre que x est inversible dans K_P, qui est donc un corps. □

Définition 2.5.9. Sous les hypothèses de la proposition 2.5.8, un corps isomorphe à $K_P := K[X]/\langle P \rangle$ (c'est-à-dire de la forme $K(\alpha)$ avec α une racine de P dans une extension de K) s'appelle un *corps de rupture* de P.

Corollaire 2.5.10. Si $x \in L$ est algébrique sur K, le morphisme ev_x induit un isomorphisme

$$K_{P_{x,K}} = K[X]/\langle P_{x,K} \rangle \xrightarrow{\sim} K[x] = K(x) \subset L.$$

Une base du K-espace vectoriel $K[x]$ est donnée par $(1, x, x^2, \dots, x^{d-1})$ où $d = \deg(P_{x,K})$.

Remarque. (1) La preuve de la proposition 2.5.8 montre comment calculer l'inverse d'un élément non nul de $K(x)$ écrit dans la base $(1, x, \dots, x^{d-1})$.
(2) Lorsque x est transcendant sur K, le morphisme ev_x se prolonge en un morphisme d'anneaux injectif $K(X) \to L$.

Proposition 2.5.11. Soit $x \in L$. Les conditions suivantes sont équivalentes :
(i) x est algébrique sur K ;
(ii) $K[x]$ est un corps ;
(iii) $\dim_K(K(x)) < +\infty$.

Démonstration. On a vu (i)⇒(ii) ci-dessus. Supposons (ii) : on a $K[x] = K(x)$, et l'élément x est inversible dans $K[x]$: il existe $A \in K[X]$ tel que $1 = xA(x)$, de sorte que $XA(X) - 1 \in \mathsf{Ker}(\mathsf{ev}_x)\backslash\{0\}$. Cela montre (i) : on a $\dim_K(K(x)) = \dim_K(K[x]) = \deg(P_{x,K})$ d'après le corollaire qui précède, ce qui montre (ii)⇒(iii). Supposons (iii) : comme $\dim_K(K[X]) = +\infty$, le morphisme ev_x ne peut être injectif, ce qui montre (i). □

Corollaire 2.5.12. Si $x, y \in L^\times$ sont algébriques sur K, il en est de même de $x - y$ et x/y : l'ensemble des éléments de L qui sont algébriques sur K est donc un sous-corps de L.

Démonstration. On a $[K(x,y) : K] = [K(x,y) : K(x)][K(x) : K] \leqslant [K(y) : K][K(x) : K] < +\infty$: on applique la proposition 2.5.11 en observant que $x - y, x/y \in K(x,y)$. □

Définition 2.5.13. L'ensemble des *nombres algébriques* est l'ensemble des nombres complexes qui sont algébriques sur $\mathbf{Q}$. D'après le corollaire qui précède, c'est un sous-corps de $\mathbf{C}$. On le note $\overline{\mathbf{Q}}$ et on l'appelle le *corps des nombres algébriques*.

Proposition 2.5.14. (1) Le corps $\overline{\mathbf{Q}}$ est algébriquement clos.
(2) Le corps $\overline{\mathbf{Q}}$ est dénombrable.

Démonstration. (1) Il s'agit de montrer que tout polynôme $P(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \overline{\mathbf{Q}}[X]$ (avec $d > 1$) admet une racine dans $\overline{\mathbf{Q}}$. Comme $\mathbf{C}$ est algébriquement clos (*cf* théorème 2.1.45), on sait que P a une racine $\theta \in \mathbf{C}$. Considérons la suite d'extensions de corps :

$$\mathbf{Q} \subset \mathbf{Q}(a_1) \subset \mathbf{Q}(a_1, a_2) \subset \cdots \subset \mathbf{Q}(a_1, a_2, \dots, a_d) \subset \mathbf{Q}(a_1, \dots, a_d, \theta)$$

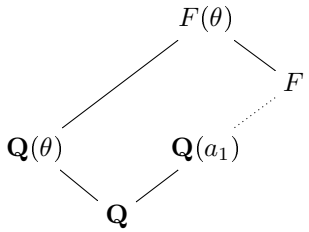
Comme $a_i \in \overline{\mathbf{Q}}$, l'élément a_i est algébrique sur $\mathbf{Q}(a_1, \dots, a_{i-1})$ et donc

$$[\mathbf{Q}(a_1, \dots, a_{i-1}, a_i) : \mathbf{Q}(a_1, \dots, a_{i-1})] < \infty$$

pour tout $i \in \{1, \dots, d\}$. De même, θ est algébrique sur $F := \mathbf{Q}(a_1, a_2, \dots, a_d)$ parce que $P \in F[X]$: on a

$$[F(\theta) : F] < \infty.$$

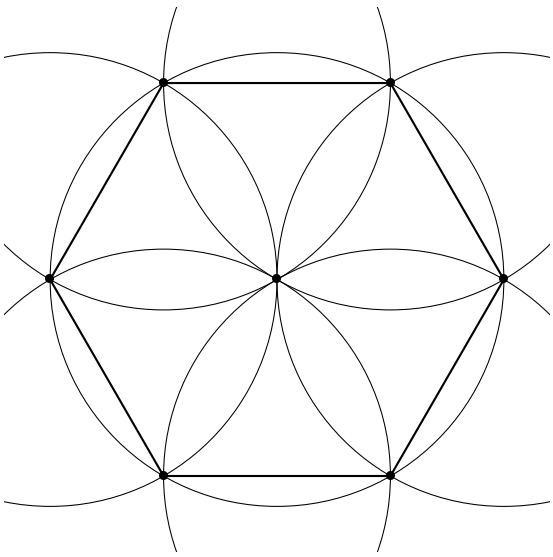
Par transitivité des degrés, on en déduit que $[F(\theta) : \mathbf{Q}] < \infty$, donc *a fortiori* $[\mathbf{Q}(\theta) : \mathbf{Q}] < \infty$, ce qui implique que $\theta \in \overline{\mathbf{Q}}$ en vertu de la proposition 2.5.11.



(2) On a bien sûr $\mathbf{Q} \subset \overline{\mathbf{Q}}$: il s'agit de montrer que $\mathsf{Card}(\overline{\mathbf{Q}}) \leqslant \mathsf{Card}(\mathbf{Q})$. Si $d \in \mathbf{N}_{>0}$, notons $\mathbb{P}_d$ l'ensemble des polynômes irréductibles unitaires dans $\mathbf{Q}[X]$ de degré d. Pour chaque $P \in \mathbb{P}_d$, l'ensemble $P^{-1}(0)$ est fini (de cardinal d) donc dénombrable. Comme $\mathsf{Card}(\mathbb{P}_d) \leqslant \mathsf{Card}(\mathbf{Q}^d) = \mathsf{Card}(\mathbf{N})$, cela montre que $\mathscr{A}_d := \bigcup_{P \in \mathbb{P}_d} P^{-1}(0)$ est dénombrable (*cf* proposition 1.3.4). Cela implique que $\overline{\mathbf{Q}} = \bigsqcup_{d=1}^{\infty} \mathscr{A}_d$ est dénombrable. □

Remarque. Comme $\mathbf{C}$ n'est pas dénombrable, cela montre que $\mathbf{C}$ est *beaucoup* plus gros que $\overline{\mathbf{Q}}$.

2.5.15. *Constructibilité à la règle est au compas.*



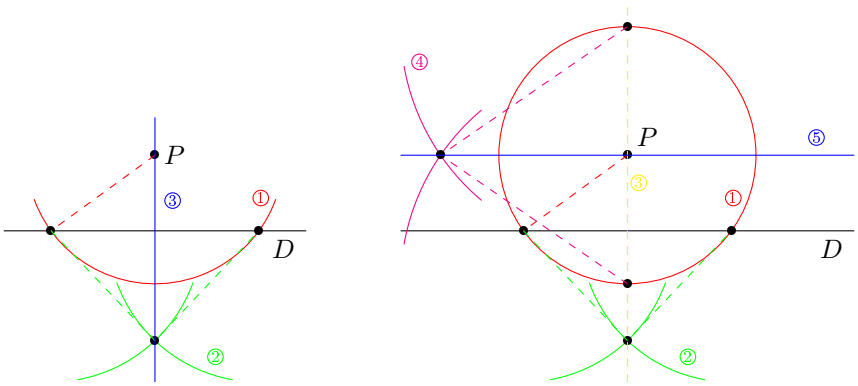
Soit $\mathscr{P}$ le plan affine euclidien. On s'intéresse au problème suivant. Étant donnés une droite Δ et deux points $P_0, P_1 \in \Delta$ distincts, quels sont les points $P \in \mathscr{P}$ qu'on peut construire avec une règle non graduée et un compas ? Il s'agit des points $P \in \mathscr{P}$ tels qu'il existe une suite $P_0, P_1, \dots, P_{n-1}, P_n = P$ telle que pour tout $i \in \{2, \dots, r\}$, le point P_i s'obtient à partir de $\mathcal{E}_i = \{P_0, P_1, \dots, P_{i-1}\}$ en effectuant deux des opérations suivantes

(1) tracer une droite passant par deux points de $\mathcal{E}_i$;

(2) tracer un cercle centré en un point de $\mathcal{E}_i$ et passant par un point de $\mathcal{E}_i$;

et en prenant l'intersection des figures ainsi obtenues.

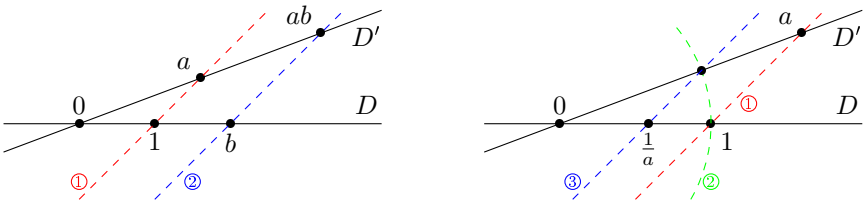
Remarquons déjà que si D est une droite et P un point (qui peut appartenir à D), on sait construire la perpendiculaire à D qui passe par P, et donc la projection de P sur D. Par ailleurs, en itérant cette opération, on sait construire la paralèlle à D passant par P.



Ainsi, on peut construire la perpendiculaire Δ' à Δ passant par P_0. Cela nous donne un repère : si P est un point de $\mathscr{P}$, on peut construire ses projections sur Δ et Δ'. Cela permet de décrire les points constructibles par leurs coordonnées (la longueur P_0P_1 étant l'unité). Tout le problème consiste donc à déterminer quels sont les nombres réels qui sont coordonnées de points constructibles. On appelle ces réels les *nombres constructibles*.

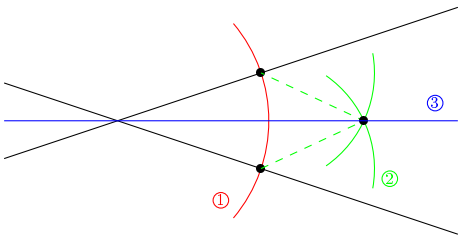
Proposition 2.5.16. L'ensemble des nombres constructibles est un sous-corps de $\mathbf{R}$.

Démonstration. Comme on peut reporter des longueurs avec le compas, il est clair que la somme et la différence de deux nombres constructibles est encore constructible. Il s'agit de prouver qu'on peut construire le produit de deux nombres constructibles, ainsi que l'inverse d'un nombre constructible non nul. Cela s'appuie sur le théorème de Thalès.



□

Rappelons qu'étant données deux droites de $\mathscr{P}$, leur bissectrice est constructible à la règle et au compas :



Proposition 2.5.17. Soit $x \in \mathbf{R}$. Alors x est constructible si et seulement si il existe un suite d'extensions $\mathbf{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r$ telle que $x \in K_r$ et $[K_i : K_{i-1}] = 2$ pour tout $i \in \{1, \ldots, r\}$. En particulier, il est nécessaire (mais pas suffisant en général) que $[\mathbf{Q}(x) : \mathbf{Q}]$ soit une puissance de 2.

Démonstration. Soit $K/\mathbf{Q}$ une extension constituée de nombres constructibles.

• Les droites (resp. les cercles) que l'on peut tracer à partir des points de $\mathscr{P}$ correspondants ont des équations de la forme

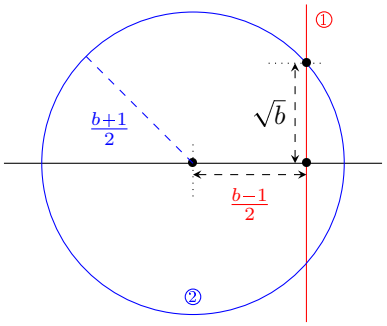
$$\alpha x + \beta y + \gamma = 0 \qquad (\text{resp. } x^2 + y^2 + ax + by + c = 0).$$

Les points d'intersections des objets ainsi construits sont solutions de systèmes linéaires ou de la forme

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 + ax + by + c = 0 \end{cases}$$

(le cas d'une intersection de deux cercles se ramenant à ce dernier système car la différence de deux équations de cercles donne une équation de droite). Par élimination, leurs coordonnées sont solutions d'équations du premier ou deuxième degré. Elles engendrent donc une extension de K de degreé 1 (auquel cas K ne change pas) ou 2.

• Réciproquement, si L est une extension quadratique réelle de K (c'est-à-dire telle que $[L : K] = 2$), montrons que les éléments de L sont constructibles. Soit $\alpha \in L \backslash K$. Alors $L = K(\alpha)$ et $P_{\alpha,K}$ est de degré 2 : on a $P_{\alpha,K} = X^2 - aX - b$. Quitte à remplacer α par $\beta = \alpha - a/2$ (on a bien sûr encore $\beta \in L \backslash K$), on peut supposer $a = 0$. On a alors $b > 0$ et b non carré de K. Il en résulte que $L = K(\sqrt{b})$: il s'agit de voir que $\sqrt{b}$ est constructible, ce qui résulte de la construction suivante.



Comme b est constructible, il en est de même de $\frac{b-1}{2}$ et $\frac{b+1}{2}$. On trace la perpendiculaire à (OP) d'abscisse $\frac{b-1}{2}$ et la cercle de centre O et de rayon $\frac{b+1}{2}$. Leurs points d'intersection ont pour ordonnées $-\sqrt{b}$ et $\sqrt{b}$. □

Corollaire 2.5.18. Les problèmes suivants ne peuvent pas se résoudre à la règle et au compas :

(1) La quadrature du cercle (*i.e.* étant donné un cercle, construire un carré de même aire), ceci parce que π est transcendant.

(2) Doubler le volume d'un cube (*i.e.* étant donné un cube, construire un cuble de volume double -c'est dans l'espace et pas le plan-), ceci parce que $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.

(3) La trisection de l'angle (sauf pour des angles particuliers bien sûr). En effet, en vertu de la formule $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$, cela revient à construire une racine du polynôme $4X^3 - 3X - \alpha$ pour $\alpha \in \mathbf{R}$ constructible, mais cela définit des éléments de degré 3 sur $\mathbf{Q}(\alpha)$ en général.

Corollaire 2.5.19. Soit p un nombre premier impair. Pour que le polygône régulier à p côtés soit constructible, il faut que $p = 2^{2^r} + 1$ avec $r \in \mathbf{N}$.

Démonstration. Il s'agit de construire les racines p-ièmes de l'unité. Le polynôme correspondant est le p-ième polynôme cyclotomique

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$$

dont on sait qu'il est irréductible (en utilisant le critère d'Eisenstein par exemple). L'extension correspondante est de degré $p-1$: il est nécessaire que $p-1$ soit une puissance de 2. Supposons $p = 2^n + 1$. Si n n'est pas une puissance de 2, on a $n = uv$ avec u impair et alors $p = 2^{uv} + 1 = (2^v + 1)(2^{v(u-1)} - 2^{v(u-2)} + \cdots - 2^v + 1)$ ce qui contredit le fait que p est premier. On a donc $n = 2^r$ avec $r \in \mathbf{N}$. □

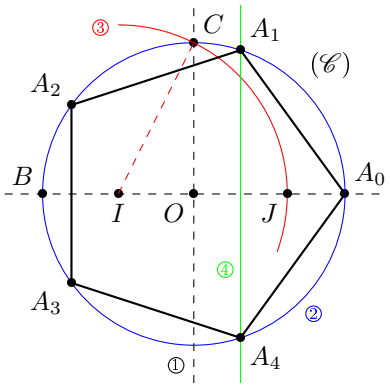
Remarque. Dans le corollaire précédent, la condition est *nécessaire*, pas suffisante *a priori*. Pour $r = 0, 1, 2, 3$, on obtient les nombres premiers $3, 5, 17$ et 257 respectivement, qui correspondent à des polygônes constructibles. Pour 17, cela a été prouvé par Carl Friedrich Gauss en 1796 (à 19 ans...)

Construction du pentagone (polygone à 5 côtés) d'après Ptolémée.

Posons $\zeta = e^{\frac{2i\pi}{5}}$. Il s'agit de construire le point $\zeta = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$, soit encore le réel $\gamma = \cos\left(\frac{2\pi}{5}\right) = \frac{\zeta+\zeta^{-1}}{2}$. Comme $\zeta \neq 1$ et $(\zeta-1)(\zeta^4+\zeta^3+\zeta^2+\zeta+1) = \zeta^5 - 1 = 0$, on a $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$, de sorte que $\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2} = 0$. On a $\gamma^2 = \frac{\zeta^2+2+\zeta^{-2}}{4}$, ce qui montre que $4\gamma^2 + 2\gamma - 1 = 0$, *i.e.* que γ est racine du polynôme $4X^2 + 2X - 1$: on a $\gamma = \frac{\sqrt{5}-1}{4}$.

Soient O et A_0 deux points deux points distincts du plan $\mathscr{P}$. Construisons le pentagone régulier de centre O qui admet A_0 comme sommet. On prend la droite (OA_0) comme axe des abscisses et longueur OA_0 comme unité. Il s'agit de construire les points A_1, A_2, A_3 et A_4 de coordonnées respectives ζ, ζ^2, ζ^3 et ζ^4.

On commence par tracer la droite (OA_0) et la perpendiculaire Δ à (OA_0) en O. On trace ensuite le cercle $(\mathscr{C})$ centre O qui passe par A_0. Il recoupe la droite (OA_0) en B, et coupe Δ en C. Notons I le milieu du segment $[OB]$ (on peut construire la médiatrice de $[OB]$). Le cercle de centre I et de rayon $[IC]$ coupe le segment $[OA_0]$ au point J. Comme I est d'abscisse $-\frac{1}{2}$, on a $IC = \frac{\sqrt{5}}{2}$ (Pythagore), et $OJ = \frac{\sqrt{5}-1}{2} = 2\gamma$. La médiatrice du segment $[OJ]$ coupe donc $(\mathscr{C})$ en A_1 et A_4. Le cercle de centre A_1 (resp. A_4) et de rayon $[A_1A_0]$ (resp. $[A_4A_0]$) recoupe le cercle $(\mathscr{C})$ en A_2 (resp. A_3), ce qui achève la construction.



Exercices. (1) Montrer que $\sqrt{2}+\sqrt[3]{3}$ est irrationnel.
(2) Quel est le polynôme minimal de $\sqrt{2}+\sqrt{3}$ sur $\mathbf{Q}$?

2.6. **Anneaux.** Dans tout ce qui suit, les anneaux sont supposés commutatifs et unitaires.

Commençons par observer que si A est un anneau intègre, on peut construire son *corps des fractions* $\mathsf{Frac}(A)$ par le même procédé qui nous a permis de construire $\mathbf{Q}$ à partir de $\mathbf{Z}$.

2.6.1. *Anneaux factoriels.* Soit A un anneau intègre.

Définition 2.6.2. Soit $a \in A\backslash\{0\}$.
(1) On dit que a est *irréductible* si $a \notin A^\times$ et

$$(\forall (b,c) \in A^2)\ a = bc \Rightarrow (b \in A^\times \text{ ou } c \in A^\times)$$

(2) On dit que a est *premier* si l'idéal principal aA est premier [7] (c'est-à-dire $a \mid xy \Rightarrow (a \mid x$ ou $a \mid y)$).
(3) On dit que $a, a' \in A\backslash\{0\}$ sont *associés* si $aA = a'A$. Cela définit une relation d'équivalence sur $A\backslash\{0\}$.

Remarque. (1) Un élément irréductible est donc par définition un élément minimal de $A\backslash(\{0\} \cup A^\times)$ pour la relation de divisibilité.
(2) Un élément premier est toujours irréductible. En effet, si $a \in A$ est premier et $a = bc$ avec $b, c \in A$, on a $bc \in aA$ qui est premier : on a $b \in aA$ ou $c \in aA$, disons $b \in aA$. On a donc $b = ad$ avec $d \in A$, et alors $a = adc$. Comme A est intègre, on a $cd = 1$ et $c \in A^\times$.
(3) Deux éléments $a, a' \in A\backslash\{0\}$ sont associés si et seulement si $(\exists u \in A^\times)\, a' = au$ (exercice : cela équivaut à l'égalité d'idéaux $aA = a'A$).

Définition 2.6.3. On dit que A est *factoriel* si tout élément $a \in A\backslash\{0\}$ peut s'écrire

$$a = up_1p_2\cdots p_r$$

avec $u \in A^\times$ et $p_1, \ldots, p_r$ irréductibles et si cette écriture est unique dans le sens suivant : si $a = vq_1q_2\ldots q_s$ avec $v \in A^\times$ et $q_1, \ldots, q_s$ irréductibles, alors $r = s$ et quitte à renuméroter les q_i, on a $p_iA = q_iA$ pour tout $i \in \{1, \ldots, r\}$.
Une telle écriture s'appelle une *factorisation en produit d'éléments irréductibles* de a.

Exemple 2.6.4. (1) Un corps est factoriel (tout élément non nul est inversible).
(2) Tout anneau principal est factoriel (*cf* proposition 2.6.10).
(3) On peut montrer (exercice) que le sous-anneau $\mathbf{Z}[i\sqrt{5}] = \{x + iy\sqrt{5} \in \mathbf{C}\,;\, x, y \in \mathbf{Z}\}$ de $\mathbf{C}$ n'est pas factoriel, parce que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles, les unités sont 1 et -1, mais que $2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ (*i.e.* on n'a pas unicité de la décomposition de 6).

Dans la pratique, si A est factoriel, on fixe une famille de représentants $\mathscr{P} = \{p_\lambda\}_{\lambda\in\Lambda}$ des classes des éléments irréductibles. Tout élément $a \in A\backslash\{0\}$ s'écrit alors de façon unique

$$a = u\prod_{\lambda\in\Lambda} p_\lambda^{n_\lambda}$$

avec $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre *fini*).

Définition 2.6.5. Soit p un élément irréductible de A. Il existe un unique $\lambda \in \Lambda$ tel que $pA = p_\lambda A$. La multiplicité n_λ s'appelle la *valuation* [8] de a en p. On la note $v_p(a)$. On pose $v_p(0) = +\infty$.

Proposition 2.6.6. (Propriétés des valuations). Supposons A factoriel et soient $a, b \in A$. On a
(1) $v_p(ab) = v_p(a) + v_p(b)$;
(2) $a \mid b$ si et seulement si pour tout $p \in A$ irréductible, on a $v_p(a) \leqslant v_p(b)$;
(3) $a \in A^\times$ si et seulement si pour tout $p \in A$ irréductible, on a $v_p(a) = 0$;
(4) $v_p(a + b) \geqslant \inf\{v_p(a), v_p(b)\}$ avec égalité si $v_p(a) \neq v_p(b)$.

Démonstration. (1)-(3) résultent immédiatement des définitions et de l'unicité de la décomposition en facteurs irréductibles. Pour (4), si $v = \inf\{v_p(a), v_p(b)\}$, on a $p^v \mid a$ et $p^v \mid b$ donc $p^v \mid a + b$, et donc $v_p(a + b) \geqslant v$. Supposons $v_p(a) \neq v_p(b)$: quitte à échanger a et b, on a $v = v_p(a) < v_p(b)$. On peut écrire $a = p^v a'$ avec $p \nmid a'$ et $b = p^v b'$ avec $p \mid b'$, de sorte que $a + b = p^v(a' + b')$ et $p \nmid a' + b'$: on a $v_p(a + b) = v$. □

Proposition 2.6.7. Soient A un anneau factoriel et $p \in A\backslash\{0\}$. Alors p est irréductible si et seulement si p est premier.

Démonstration. Si p est irréductible et $p \mid ab$, on a $v_p(a) + v_p(b) = v_p(ab) \geqslant 1$, donc $v_p(a) \geqslant 1$ ou $v_p(b) \geqslant 1$, *i.e.* $p \mid a$ ou $p \mid b$. Réciproquement un élément premier est toujours irréductible. □

7. Rappelons qu'un idéal $I \subset A$ est premier lorsqu'on a $(\forall x, y \in A)\, xy \in I \Rightarrow (x \in I$ ou $y \in I)$. Cela équivaut à l'intégrité de l'anneau quotient (exercice).
8. Elle ne dépend que de p et pas du choix de $\mathscr{P}$.

Définition 2.6.8. Soient A un anneau factoriel [9] et $a, b \in A\backslash\{0\}$. On appelle *pgcd* (plus grand commun diviseur) –resp. *ppcm* (plus petit commun multiple)– de a et b un plus grand minorant –resp. un plus petit majorant– de $\{a, b\}$ pour la relation de divisibilité. On les note $\mathsf{pgcd}(a, b)$ et $\mathsf{ppcm}(a, b)$ respectivement. On dit que a et b sont *premiers entre eux* si $\mathsf{pgcd}(a, b) = 1$.

Remarque. (1) Rigoureusement, $\mathsf{pgcd}(a, b)$ et $\mathsf{ppcm}(a, b)$ sont définis à multiplication par une unité près : ce sont les idéaux qu'ils engendrent qui sont bien définis.
(2) Cette définition affirme implicitement l'existence du pgcd et du ppcm. En fait, étant donnés $a, b \in A$, de décompositions en facteurs irréductibles

$$a = u \prod_{\lambda\in\Lambda} p_\lambda^{n_\lambda} \qquad b = v \prod_{\lambda\in\Lambda} p_\lambda^{m_\lambda}$$

on a

$$\mathsf{pgcd}(a, b) = \prod_{\lambda\in\Lambda} p_\lambda^{\min\{n_\lambda, m_\lambda\}} \qquad \mathsf{ppcm}(a, b) = \prod_{\lambda\in\Lambda} p_\lambda^{\max\{n_\lambda, m_\lambda\}}.$$

En d'autres termes, pour tout $p \in A$ irréductible, on a

$$v_p(\mathsf{pgcd}(a, b)) = \min\{v_p(a), v_p(b)\}$$
$$v_p(\mathsf{ppcm}(a, b)) = \max\{v_p(a), v_p(b)\}.$$

On remarque qu'on a $\mathsf{pgcd}(a, b)\,\mathsf{ppcm}(a, b)A = abA$.
Par induction, on peut facilement étendre la définition et parler du pgcd et du ppcm d'une famille *finie* d'éléments non nuls.

Proposition 2.6.9. (Lemme de Gauss). Soient A un anneau factoriel et $a, b, c \in A\backslash\{0\}$ tels que $\mathsf{pgcd}(a, b) = 1$. Si $a \mid bc$, alors $a \mid c$.

Démonstration. Si $p \in A$ est irréductible et divise a, on a $v_p(b) = 0$ vu que $p \nmid b$ (a et b étant premiers entre eux). On a donc $v_p(a) \leqslant v_p(bc) = v_p(c)$. Comme c'est vrai pour tout p premier divisant a, on a $a \mid c$ (*cf* proposition 2.6.6 (2)). □

Proposition 2.6.10. Tout anneau principal est factoriel.

Lemme 2.6.11. Soit A un anneau intègre dans lequel tout élément irréductible est premier (*cf* proposition 2.6.7). Alors *si* un élément admet une décomposition en facteur irréductibles, cette dernière est unique (au sens de la définition 2.6.3).

Démonstration. Soit $a = up_1p_2\cdots p_r = vq_1q_2\cdots q_s$ (avec $u, v \in A^\times$ et $p_1, \ldots, p_r, q_1, \ldots, q_s$ des éléments irréductibles) deux décompositions en facteurs irréductibles.
On procède par récurrence sur s. Si $s = 0$, alors $a = v \in A^\times$: le produit $up_1p_2\cdots p_r$ est inversible donc chacun de ses facteurs l'est, et on a nécessairement $r = 0$ et $u = v$. Supposons $s \geqslant 1$. Comme q_s est irréductible et divise le produit $up_1p_2\cdots p_r$, il divise l'un des facteurs (puisqu'il est premier). Comme u est inversible, il n'est pas divisible par q_s qui ne l'est pas : quitte à renuméroter les p_i, on peut supposer $q_s \mid p_r$ *i.e.* $q_sA = p_rA$. En divisant a par q_s, on se ramène au cas $s - 1$, ce qui permet de conclure. □

Proposition 2.6.12. Soit A un anneau principal. Toute suite croissante d'idéaux est stationnaire. En particulier, tout idéal strict de A est inclus dans un idéal maximal (au sens de l'inclusion).

Démonstration. Soit $(I_n)_{n\in\mathbf{N}}$ une suite croissante (au sens de l'inclusion) d'idéaux. Posons $I = \bigcup_{n=0}^{\infty} I_n \subset A$: c'est un idéal de A. Comme A est principal, il existe $\alpha \in A$ tel que $I = \alpha A$. On a $\alpha \in I$: il existe $n_0 \in \mathbf{N}$ tel que $\alpha \in I_{n_0}$. Comme la suite est croissante, on a donc

$$\alpha A \subset I_{n_0} \subset I_n \subset I = \alpha A$$

et donc $I_n = \alpha A$ pour tout $n \geqslant n_0$, ce qui conclut. □

Démonstration de la proposition 2.6.10. Soient A un anneau principal et $a_0 \in A\backslash\{0\}$. Supposons que a_0 n'admette pas de décomposition en facteurs irréductibles. Alors a_0 n'est pas irréductible : il s'écrit $a_0 = a_1b_1$ avec $a_1, b_1 \in A\backslash(\{0\}\cup A^\times)$. Si a_1 et b_1 admettent tous les deux une décomposition en facteurs irréductibles, il en est de même de leur produit a_0, ce qui n'est pas : quitte à échanger a_1 et b_1, on peut supposer que a_1 n'admet pas de décomposition en facteurs irréductibles. On peut appliquer de nouveau ce raisonnement avec a_1 à la place de a_0 : on construit ainsi par récurrence deux suites $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}_{>0}}$ d'éléments de $A\backslash(\{0\} \cup A^\times)$ telles que pour tout $n \in \mathbf{N}$, on a $a_n = a_{n+1}b_{n+1}$. La suite d'idéaux $(a_nA)_{n\in\mathbf{N}}$ est croissante (car $a_{n+1} \mid a_n$ pour tout $n \in \mathbf{N}$). Elle est donc stationnaire (*cf* proposition 2.6.12) : il existe $n \in \mathbf{N}$ tel que $a_nA = a_{n+1}A$. Comme on a $a_n = a_{n+1}b_{n+1}$, cela implique $b_{n+1} \in A^\times$, ce qui est contradictoire. Pour achever la preuve, il suffit (en vertu du lemme 2.6.11) de montrer que tout élément irréductible est premier. Soit $p \in A$ irréductible. Soit $\mathfrak{m} \subset A$ un idéal maximal de A contenant p (*cf* proposition 2.6.12). Comme A est principal, il existe $a \in A$ avec $\mathfrak{m} = aA$, et $p \in \mathfrak{m} \Rightarrow (\exists b \in A)\ p = ab$. Comme p est irréductible, on a $b \in A^\times$ (car $a \notin A^\times$ vu que $\mathfrak{m} = aA \neq A$). Ainsi $pA = \mathfrak{m}$ est maximal, donc premier. □

9. Cette définition garde un sens dans un anneau intègre quelconque, mais en général, le pgcd et le ppcm de deux éléments n'existent pas.

Remarque. Si A est un anneau principal, on a une autre caractérisation du pgcd et du ppcm de deux éléments $a, b \in A$. On a $\mathsf{pgcd}(a,b)A = aA+bA$ et $\mathsf{ppcm}(a,b)A = aA \cap bA$. Montrons-le pour le pgcd (la preuve pour le ppcm est analogue). Comme A est principal, il existe $d \in A$ tel que $aA + bA = dA$. Comme $x \in A$ divise a et b si et seulement si $aA \subset xA$ et $bA \subset xA$ *i.e.* $dA \subset xA$, on a bien $\mathsf{pgcd}(a,b) = d$.
Il ne faut pas croire que cette caractérisation est valable dans tout anneau factoriel. Par exemple, on peut montrer que $\mathbf{Q}[X,Y]$ est factoriel. Comme X et Y sont irréductibles et premiers entre eux, on a $\mathsf{pgcd}(X,Y) = 1$, bien que $X\,\mathbf{Q}[X,Y] + Y\,\mathbf{Q}[X,Y] \neq \mathbf{Q}[X,Y]$ (c'est l'idéal des polynômes qui s'annulent en $(0,0)$). Bien sûr, cela vient du fait que l'anneau $\mathbf{Q}[X,Y]$ n'est pas principal.

Exemple 2.6.13. Si K est un corps et $n \in \mathbf{N}_{>1}$, l'anneau $K[X_1, \ldots, X_n]$ est factoriel (*cf* théorème 2.6.23) mais pas principal (*cf* remarque précédente). De même, l'anneau $\mathbf{Z}[X]$ est factoriel (*cf loc. cit.*) mais pas principal (l'idéal engendré par 2 et X n'est pas principal).

Proposition 2.6.14. Si A est principal, ses idéaux premiers non nuls sont maximaux.

Démonstration. Soit $\mathfrak{p} \subset A$ premier non nul. D'après la proposition 2.6.12, il existe $\mathfrak{m} \subset A$ maximal tel que $\mathfrak{p} \subset \mathfrak{m}$. Comme A est principal, on a $\mathfrak{p} = pA$ et $\mathfrak{m} = aA$: on a $p = ab$ avec $b \in A$. Comme p est premier donc irréductible, on a $b \in A^\times$ (car $a \notin A^\times$ vu que $\mathfrak{m}$ est maximal), ce qui implique que $\mathfrak{p} = \mathfrak{m}$ est maximal. □

Définition 2.6.15. Soit A un anneau intègre.
- Un *stathme euclidien* est une application $\phi\colon A\backslash\{0\} \to \mathbf{N}$ telle que si $a, b \in A\backslash\{0\}$ sont tels que b divise a, alors $\phi(b) \leqslant \phi(a)$. Cette application sert de « mesure » pour la division euclidienne. Le stathme euclidien ϕ est dit *total* s'il est en fait à valeurs dans $\mathbf{N}_{>0}$.
- Un stathme euclidien ϕ définit une *division euclidienne* si pour tout $(a,b) \in A \times A\backslash\{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et ($r = 0$ ou $\phi(r) < \phi(b)$). L'élément q s'appelle alors « le » *quotient* et r « le » *reste* de la division.
- Un anneau est un anneau *euclidien* si et seulement s'il admet un stathme euclidien définissant une division euclidienne.

Remarque. Si A est un anneau euclidien, il n'y a pas unicité d'un stathme euclidien sur A. En outre, on ne requiert pas l'unicité du quotient et du reste.

Exemple 2.6.16. Tout corps est un anneau euclidien. L'anneau $\mathbf{Z}$ est euclidien, avec le stathme donné par $\phi(a) = |a|$ (valeur absolue). Dans ce cas, la division est la division euclidienne habituelle (on a unicité –au signe près– dans ce cas). Si K est un corps, l'anneau de polynômes $K[X]$ est euclidien, avec le stathme donné par $\phi(P) = \deg(P)$ si $P \neq 0$, et $\phi(0) = 0$. Là encore, la division est la division euclidienne habituelle et elle est unique.

L'anneau $\mathbf{Z}[i] = \{a + ib \in \mathbf{C},\ a, b \in \mathbf{Z}\}$ des *entiers de Gauss* est euclidien, muni du stathme donné par $\phi(a + ib) = a^2 + b^2$.

Proposition 2.6.17. Tout anneau euclidien est principal.

Démonstration. Soient A un anneau euclidien, $\phi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme euclidien et $I \subset A$ un idéal. Montrons que I est principal. On peut supposer $I \neq 0$. Dans ce cas, $\phi(I\backslash\{0\})$ est une partie non vide de $\mathbf{N}$, elle admet donc un plus petit élément : Soit $b \in I\backslash\{0\}$ un élément tel que $\phi(b)$ est minimal. On a bien sûr $bA \subset I$. Réciproquement, soit $a \in I$. Comme ϕ est euclidien, il existe $q, r \in A$ tels que $a = qb + r$ et $r = 0$ ou $\phi(r) < \phi(b)$. Supposons $r \neq 0$: on a $\phi(r) < \phi(b)$. Mais $r = a - qb \in I$, et comme $r \neq 0$, on a $\phi(b) \leqslant \phi(r)$ par minimalité de $\phi(b)$, ce qui est contradictoire. On a donc en fait $r = 0$, et $a = qb \in bA$. Ainsi $I = bA$ est principal. □

Remarque. Il existe des anneaux qui sont principaux, mais pas euclidiens.

Corollaire 2.6.18. Les anneaux $\mathbf{Z}$ et $K[X]$ (où K est un corps) sont principaux, donc factoriels (*cf* proposition 2.6.10).

2.6.19. *Transfert de la factorialité.* Si $f\colon A \to B$ est un morphisme d'anneaux, il induit un morphisme d'anneaux $A[X] \to B[X]$. Si A est un sous-anneau de B, alors $A[X]$ est naturellement un sous-anneau de $B[X]$.

Dans ce numéro, A désigne un anneau factoriel et K son corps des fractions.

Définition 2.6.20. Si $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]\backslash\{0\}$, ee *contenu* de P est

$$c(P) = \mathsf{pgcd}\{a_i/\ a_i \neq 0\}.$$

Lemme 2.6.21. Si $P, Q \in A[X]\backslash\{0\}$, on a $c(PQ) = c(P)c(Q)$.

Remarque. Le pgcd étant défini à multiplication par une unité près, on devrait plutôt écrire $c(PQ)A = c(P)c(Q)A$. Dans ce qui suit, on commettra systématiquement cet abus pour ne pas alourdir la rédaction.

Démonstration. On peut déjà écrire $P = c(P)\tilde{P}$ et $Q = c(Q)\tilde{Q}$ avec $c(\tilde{P}) = 1$ et $c(\tilde{Q}) = 1$: on a $PQ = c(P)c(Q)\tilde{P}\tilde{Q}$. Quitte à remplacer P et Q par $\tilde{P}$ et $\tilde{Q}$ respectivement, on peut supposer $c(P) = 1$ et $c(Q) = 1$, et il s'agit de prouver que $c(PQ) = 1$.

Supposons au contraire qu'il existe $p \in A$ premier tel que $p \mid c(PQ)$. Si on note $\overline{P}$ et $\overline{Q}$ les images dans $(A/pA)[X]$ de P et Q respectivement, cela implique que $\overline{PQ} = 0$ dans $(A/pA)[X]$. Mais comme p est premier, l'anneau A/pA est intègre : il en est de même de l'anneau $(A/pA)[X]$. On a donc $\overline{P} = 0$ ou $\overline{Q} = 0$, et donc $p \mid c(P)$ ou $p \mid c(Q)$, ce qui contredit $c(P) = 1$ et $c(Q) = 1$. □

Proposition 2.6.22. Soit $P \in A[X]$ tel que $c(P) = 1$. Alors P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$.

Démonstration. Supposons P irréductible dans $K[X]$ et $P = Q_1Q_2$ avec $Q_1, Q_2 \in A[X]$. Comme P est irréductible dans $K[X]$, quitte à échanger Q_1 et Q_2, le polynôme Q_1 est constant d'où $Q_1 = c(Q_1)$. Mais d'après le lemme 2.6.21, on a $1 = c(P) = c(Q_1)c(Q_2)$, donc $Q_1 \in A^\times$. Ainsi P est irréductible dans $A[X]$.

Réciproquement, supposons P irréductible dans $A[X]$ et $P = Q_1Q_2$ avec $Q_1, Q_2 \in K[X]$. Il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1Q_1 \in A[X]$ et $a_2Q_2 \in A[X]$. On a alors $a_1a_2 = c(a_1a_2P) = c(a_1Q_1)c(a_2Q_2)$ d'après le lemme 2.6.21, vu que $c(P) = 1$. Si on écrit $a_1Q_1 = c(a_1Q_1)\widetilde{Q}_1$ et $a_2Q_2 = c(a_2Q_2)\widetilde{Q}_2$ avec $\widetilde{Q}_1, \widetilde{Q}_2 \in A[X]$, on a donc $a_1a_2P = c(a_1Q_1)\widetilde{Q}_1c(a_2Q_2)\widetilde{Q}_2 = a_1a_2\widetilde{Q}_1\widetilde{Q}_2$ soit $P = \widetilde{Q}_1\widetilde{Q}_2$ (l'anneau A est intègre). Comme P est irréductible dans $A[X]$, quitte à échanger $\widetilde{Q}_1$ et $\widetilde{Q}_2$, on peut supposer $\widetilde{Q}_1 \in A^\times$. On a alors $Q_1 \in K^\times$ et P est irréductible dans $K[X]$. □

Théorème 2.6.23. (1) Les éléments irréductibles dans $A[X]$ sont
- les éléments irréductibles de A (vus comme polynômes constants) ;
- les polynômes $P \in A[X]$ de contenu 1 et irréductibles dans $K[X]$.

(2) L'anneau $A[X]$ est factoriel [10].

Démonstration. • Si $p \in A$ est irréductible, le polynôme constant p est irréductible dans $A[X]$. En effet, l'anneau A/pA est intègre : il en est de même de $A[X]/pA[X] \simeq (A/pA)[X]$ et p est premier donc irréductible dans $A[X]$.
• Si $P \in A[X]$ est de degré $\geqslant 1$ et irréductible, alors $c(P) = 1$. En effet, on peut écrire $P = c(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$, ce qui donne une factorisation non triviale si $c(P)$ est non inversible.
• Existence d'une factorisation en produit d'irréductibles. Soit $P \in A[X]\backslash\{0\}$. On peut écrire $P = c(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ de contenu égal à 1. Comme A est factoriel, on peut factoriser $c(P)$ en produit d'irréductibles dans A. Il suffit donc de montrer qu'on peut factoriser $\widetilde{P}$: on peut supposer $c(P) = 1$. Si $P \in A$, on a $P = 1$: on peut supposer $\deg(P) \geqslant 1$. Comme $K[X]$ est factoriel (*cf* corollaire 2.6.18), on peut écrire $P = P_1P_2\cdots P_r$ avec $P_i \in K[X]$ irréductible pour $i \in \{1, \ldots, r\}$. Pour tout $i \in \{1, \ldots, r\}$, soit $a_i \in A\backslash\{0\}$ tel que $a_iP_i \in A[X]$, et $\widetilde{P}_i = c(a_iP_i)^{-1}(a_iP_i) \in A[X]$. Comme $\widetilde{P}_i$ est de contenu 1 et irréductible dans $K[X]$ (car P_i l'est), il est irréductible dans $A[X]$ d'après la proposition 2.6.22. On a $a_1a_2\cdots a_r = c(a_1P_1)\cdots c(a_rP_r)$ en vertu du lemme 2.6.21, vu que $c(P) = 1$. On a donc la factorisation $P = \widetilde{P}_1\widetilde{P}_2\cdots\widetilde{P}_r$. On a montré au passage que les éléments irréductibles de $A[X]$ sont ceux annoncés dans la première partie de la proposition.
• Unicité de la factorisation en produit d'irréductibles. Soient $P \in A[X]\backslash\{0\}$ et $P = P_1P_2\cdots P_r$ et $P = Q_1Q_2\cdots Q_s$ deux factorisations dans $A[X]$. Quitte à renuméroter les P_i (resp. les Q_j), il existe $r_0 \leqslant r$ (resp. $s_0 \leqslant s$) tel que $P_i \in A\backslash\{0\}$ pour $i \leqslant r_0$ et $\deg(P_i) > 0$ pour $r_0 < i \leqslant r$ (resp. $Q_j \in A\backslash\{0\}$ pour $j \leqslant s_0$ et $\deg(Q_j) > 0$ pour $s_0 < j \leqslant s$). D'après la remarque faite plus haut, on a alors $c(P_i) = c(Q_j) = 1$ pour $r_0 < i \leqslant r$ et $s_0 < j \leqslant s$. En prenant le contenu de l'égalité $P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s$, il vient donc $P_1P_2\cdots P_{r_0} = Q_1Q_2\cdots Q_{s_0}$, qui est une égalité de deux décompositions en facteurs irréductibles dans A. Ce dernier étant factoriel, on a $r_0 = s_0$, et quitte à renuméroter, on peut supposer $P_iA = Q_iA$ pour tout $i \in \{1, \ldots, r_0\}$. En divisant P par $P_1P_2\cdots P_{r_0}$, il vient $P_{r_0+1}\cdots P_rA[X] = Q_{r_0+1}\cdots Q_sA[X]$. C'est une factorisation en produit d'irréductibles dans $K[X]$, qui est factoriel : on a $r = s$ et quitte à renuméroter, on peut supposer $P_iK[X] = Q_iK[X]$ pour $i \in \{r_0 + 1, \ldots, r\}$. Mais comme $c(P_i) = c(Q_i) = 1$, on a en fait $P_iA[X] = Q_iA[X]$ pour $i \in \{r_0 + 1, \ldots, r\}$. □

2.6.24. *Un exemple important : l'anneau des entiers de Gauss.* Soit $A = \mathbf{Z}[i] = \{a + ib\,;\, a, b \in \mathbf{Z}\} \subset \mathbf{C}$. C'est un anneau appelé *anneau des entiers de Gauss*. Son corps des fractions est l'extension $\mathbf{Q}(i)$ de $\mathbf{Q}$. Si $z \in A$, on pose

$$N(z) = |z|^2 = z\overline{z} \in \mathbf{N}\,.$$

On a bien sûr $N(z_1z_2) = N(z_1)N(z_2)$ pour tout $z_1, z_2 \in A$.

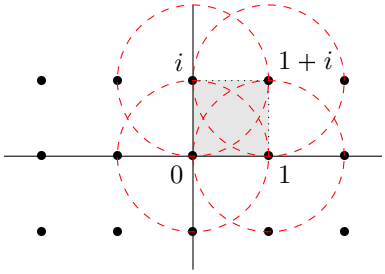
Proposition 2.6.25. (1) On a $A^\times = \{\pm 1, \pm i\}$.
(2) N est un stathme euclidien pour A.

Démonstration. (1) Si $z \in A^\times$, alors $z^{-1} \in A$ et $N(z)N(z^{-1}) = 1$, donc $N(z) \in \mathbf{Z}^\times = \{\pm 1\}$: comme $N(z) \geqslant 0$, on a $N(z) = 1$. Si $z = a + ib$, on a donc $a^2 + b^2 = 1$, ce qui implique $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$, *i.e.* $A^\times \subset \{\pm 1, \pm i\}$. L'inclusion réciproque est triviale.
Il est commode de représenter les éléments de A par les points du plan complexe dont ce sont les affixes : l'anneau A s'identifie alors à $\mathbf{Z}^2 \subset \mathbf{R}^2 \simeq \mathbf{C}$. Il s'agit alors de montrer que si $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que $a = qb + r$ et $N(r) < N(b)$, soit encore tels que

$$\frac{a}{b} = q + \frac{r}{b} \quad \text{et} \quad N\left(\tfrac{r}{b}\right) < 1.$$

En posant $z = \frac{a}{b} \in \mathbf{Q}(i) \subset \mathbf{C}$, il suffit de montrer qu'il existe $q \in A$ tel que $|z - q| < 1$ (on pose alors $r = a - qb \in A$). Géométriquement, cela revient à voir que les disques ouverts de rayon 1 centrés en les éléments de A recouvrent le plan, ce qui résulte du fait que $1 > \frac{1}{\sqrt{2}}$.

10. Il est facile de voir que la réciproque est vraie.



□

Corollaire 2.6.26. L'anneau des entiers de Gauss est principal, donc factoriel.

Une question naturelle est alors de déterminer les éléments irréductibles de A. Commençons par comprendre comment les nombres premiers (dans $\mathbf{Z}$) se factorisent dans A.

Proposition 2.6.27. Soit p un nombre premier. Les conditions suivantes sont équivalentes :
(i) p est réductible dans A ;
(ii) p est somme de deux carrés ;
(iii) -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$;
(iv) $p = 2$ ou $p \equiv 1 \mod 4$.

Démonstration. Supposons (i) : il existe $z_1, z_2 \in A \backslash A^\times$ tels que $p = z_1 z_2$, de sorte que $p^2 = N(p) = N(z_1)N(z_2)$ et $N(z_1) \neq 1$ et $N(z_2) \neq 1$. Cela implique que $p = N(z_1) = N(z_2)$. Si $z_1 = a + ib$, on a donc $p = a^2 + b^2$ ce qui prouve (ii). Réciproquement, si $p = a^2 + b^2$, alors $p = (a + ib)(a - ib)$ est réductible, ce qui montre (i) et donc (i)⇔(ii).
Supposons (ii) : il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + b^2$. On a bien sûr $p \nmid b$ (sinon on aurait $p \mid a$ puis $p^2 \mid p$, ce qui est idiot). Modulo p, on a donc $\overline{a}^2 = -\overline{b}^2$ et $\overline{b} \in (\mathbf{Z}/p\mathbf{Z})^\times$, ce qui montre que $-1 = (\overline{a}/\overline{b})^2$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ et donc (iii). Réciproquement, supposons (iii). Cela implique que le polynôme $X^2 + 1$ est scindé dans $(\mathbf{Z}/p\mathbf{Z})[X]$, et donc que le quotient

$$A/pA \simeq \mathbf{Z}[X]/\langle X^2 + 1, p\rangle \simeq (\mathbf{Z}/p\mathbf{Z})[X]/\langle X^2 + 1\rangle$$

n'est pas intègre, et donc que p est réductible dans A.
L'équivalence entre (iii) et (iv) est classique. □

Corollaire 2.6.28. Si $p \equiv 3 \mod 4$ est premier et $p \mid a^2 + b^2$, alors $p \mid a$ et $p \mid b$.

Démonstration. Si on avait $p \nmid a$ ou $p \nmid b$, la divisibilité $p \mid a^2 + b^2$ impliquerait que -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$, contredisant la proposition 2.6.27. □

Proposition 2.6.29. Un élément $z \in A$ est irréductible si et seulement si $N(z)$ est premier (nécessairement 2 ou congru à 1 modulo 4) ou le carré d'un nombre premier congru à 3 modulo 4.

Démonstration. Si $N(z)$ est premier, alors z est automatiquement irréductible : supposons $N(z)$ composé.
Comme $N(z)$ est une somme de deux carrés, la proposition 2.6.31 montre que $v_p(N(z))$ est pair dès que $p \equiv 3 \mod 4$. Si $N(z)$ n'est pas le carré d'un nombre premier congru à 3 modulo 4, on peut écrire $N(z) = xy$ avec $x, y \in \mathbf{N}$ sommes de deux carrés et $x, y > 1$. Écrivons $x = u^2 + v^2 = N(u + iv)$ et $y = w^2 + t^2 = N(w + it)$: on a $N(z) = N(z')$ c'est-à-dire $z\overline{z} = z'\overline{z'}$ avec $z' = (u + iv)(w + it) \in A$. Si z était irréductible, on aurait $z \mid z'$ ou $z \mid \overline{z'}$, par exemple $z \mid z'$: écrivons $z' = z\alpha$ avec $\alpha \in A$. On a alors $N(z) = N(z') = N(z)N(\alpha)$, ce qui implique $N(\alpha) = 1$ *i.e.* $\alpha \in A^\times$, de sorte que $z = \alpha^{-1}(u + iv)(w + it)$, contredisant l'irréductibilité de z. Il en résulte que si z est irréductible, on a $N(z) = p^2$ avec p un nombre premier congru à 3 modulo 4. La réciproque a été vue plus haut. □

Corollaire 2.6.30. À multiplication par unité près, les éléments irréductibles de A sont
- $1 + i$;
- les éléments $a + ib$ tels que $a^2 + b^2$ est un nombre premier $\equiv 1 \mod 4$;
- les nombres premiers $\equiv 3 \mod 4$.

Remarque. On a $1 - i = -i(1 + i)$, ce qui montre en particulier que $2A = \mathfrak{p}^2$ avec $\mathfrak{p} = (1 + i)A$. Si p est un nombre premier tel que $p \equiv 1 \mod 4$, il existe $a, b \in \mathbf{Z}$ tels que $p = a^2 + b^2$, et on a $pA = \mathfrak{p}_1\mathfrak{p}_2$ avec $\mathfrak{p}_1 = (a + ib)A$ et $\mathfrak{p}_2 = (a - ib)A$ (on a $\mathfrak{p}_1 \neq \mathfrak{p}_2$).

Notons $\Sigma \subset \mathbf{N}$ (resp. $\widetilde{\Sigma} \subset \mathbf{N}$) l'ensemble des entiers qui peuvent s'écrire comme la somme de deux (resp. quatre) carrés.

Proposition 2.6.31. Si $n \in \mathbf{N}_{>0}$, on a $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout nombre premier tel que $p \equiv 3 \mod 4$.

Démonstration. • Commençons par observer que si $a_1, a_2, b_1, b_2 \in \mathbf{Z}$ et $z_1 = a_1 + ib_2, z_2 = a_2 + ib_2 \in A$, l'égalité $N(z_1)N(z_2) = N(z_1 z_2)$ s'écrit

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$$

ce qui montre que Σ est stable par multiplication. Comme $2 \in \Sigma$ et $p \in \Sigma$ lorsque $p \equiv 1 \mod 4$ est premier, cela montre que si $v_p(n)$ est pair pour tout nombre premier tel que $p \equiv 3 \mod 4$, alors $n \in \Sigma$.
Réciproquement, soient $n \in \Sigma \backslash \{0\}$ et $p \equiv 3 \mod 4$ un nombre premier : écrivons $n = a^2 + b^2$. D'après le corollaire 2.6.28, on a $p \mid a$ et $p \mid b$: cela implique que $p^2 \mid n$, et $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \in \Sigma$. En itérant ce qui précède, on a donc $2 \mid v_p(n)$. □

Théorème 2.6.32. (Théorème des quatre carrés). On a $\widetilde{\Sigma} = \mathbf{N}$.

Démonstration. On prouve une identité (dite des quatre carrés d'Euler [11]) qui montre que $\widetilde{\Sigma}$ est stable par produit. Comme $0 \in \widetilde{\Sigma}$, il suffit de montrer que les nombres premiers sont sommes de quatre carrés (on peut même se restreindre à ceux qui sont congrus à 3 modulo 4 en vertu de la proposition 2.6.27.
Soit donc p premier impair. Il existe $a, b \in \mathbf{Z}$ tels que $p \mid 1 + a^2 + b^2$ (si C désigne l'ensemble des carrés de $\mathbf{Z}/p\mathbf{Z}$, on a $\#C = \frac{p+1}{2}$, donc $(1+C) \cap (-C) \neq \varnothing$). On peut même supposer que $|a|, |b| \leqslant \frac{p-1}{2}$: on a alors $1 + a^2 + b^2 \leqslant 1 + \frac{(p-1)^2}{2}$. Il en résulte qu'il existe $k \in \mathbf{Z}$ tel que $kp = 1 + a^2 + b^2$ avec $0 < k < p$. On peut donc parler du plus petit entier m tel que mp soit somme de quatre carrés (on a $m \leqslant k < p$). Supposons $m \neq 1$. Écrivons $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Soit y_i l'unique entier congru à x_i modulo m et tel que $-\frac{m+1}{2} \leqslant y_i \leqslant \frac{m}{2}$. Comme $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \mod m$, on a $m \mid y_1^2 + y_2^2 + y_3^2 + y_4^2$: écrivons $y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr$: comme $y_1^2 + y_2^2 + y_3^2 + y_4^2 \leqslant m^2$, on a $r \leqslant m$. Supposons $r = m$: on a nécessairement $y_i = \frac{m}{2} \in \mathbf{N}_{>0}$ pour tout i. Écrivons $x_i = \frac{m}{2} + mk_i$: on a $x_i^2 = y_i^2 + m^2(k_i + k_i^2)$, et donc

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 = y_1^2 + y_2^2 + y_3^2 + y_4^2 + m^2 \sum_{i=1}^{r} (k_i + k_i^2) \in m^2\,\mathbf{N}$$

ce qui montre que $m \mid p$, ce qui est impossible vu que p est premier et $1 < m < p$. On a donc $r < m$. En utilisant l'identité des quatre carrés de nouveau, il existe $z_1, z_2, z_3, z_4 \in \mathbf{Z}$ tels que

$$(mp)(mr) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

En utilisant les formules qui donnent z_1, z_2, z_3, z_4 à partir de $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ et le fait que $y_i \equiv x_i \mod m$ pour tout $i \in \{1, \ldots, 4\}$, on montre que $m \mid z_i$ pour $i \in \{1, \ldots, 4\}$. Il en résulte que

$$rp = \left(\tfrac{z_1}{m}\right)^2 + \left(\tfrac{z_2}{m}\right)^2 + \left(\tfrac{z_3}{m}\right)^2 + \left(\tfrac{z_4}{m}\right)^2$$

contredisant la minimalité de m. On a donc $m = 1$ et $p \in \widetilde{\Sigma}$. □

Exercice. Montrer que $\mathbf{Z}[j]$ est euclidien.

Références

[1] J.-M. Arnaudiès & H. Fraysse – *Cours de mathématiques. 1*, Dunod Université : Ouvrages de Base, Dunod, Paris, 1987, Algèbre.

[2] M. Demazure – *Cours d'algèbre*, Nouvelle Bibliothèque Mathématique, vol. 1, Cassini, Paris, 1997.

[3] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[4] J.-P. Serre – *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977, Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

11. Qui est

$$(x_1^2 + y_1^2 + z_1^2 + t_1^2)(x_2^2 + y_2^2 + z_2^2 + t_2^2) =$$
$$= (x_1x_2 + y_1y_2 + z_1z_2 + t_1t_2)^2 + (x_1y_2 - y_1x_2 + t_1z_2 - z_1t_2)^2$$
$$+ (x_1z_2 - z_1x_2 + y_1t_2 - t_1y_2)^2 + (x_1t_2 - t_1x_2 + z_1y_2 - y_1z_2)^2$$

et qui se démontre en considérant la norme dans les quaternions.