Chapitre 7

Bezout, Gauss, pgcd

Je révise et je me perfectionne

I. pgcd : Définition

Proposition 7.1

Toute partie majorée de $\mathbb{Z}$ admet un plus grand élément. Toute partie minorée de $\mathbb{Z}$ admet un plus petit élément.

Conséquence 7.2

Il s'ensuit que :

- toute partie finie de $\mathbb{Z}$ admet un plus petit et un plus grand élément,
- toute partie de $\mathbb{N}$ admet un plus petit élément

Exercice 7.1

1. Donner un exemple montrant que la proposition 7.1 n'est plus vraie si l'on remplace $\mathbb{Z}$ par $\mathbb{R}$.
2. La proposition est-elle encore vraie dans $\mathbb{Q}$?

Définition 7.3 : pgcd

Soient a et b deux entiers non tous deux nuls. L'ensemble des diviseurs communs de a et de b est fini et non vide, il possède donc un plus grand élément appelé **plus grand commun diviseur** (le « pgcd ») de a et b et noté $\text{pgcd}(a, b)$ ou parfois $a \wedge b$.

Remarque 7.4

Par définition un pgcd est positif.

II. Bézout, Gauss

Théorème 7.5

Égalité de Bézout

Quels que soient $a, b \in \mathbb{Z}^\star$ il existe $u, v \in \mathbb{Z}$ tels que
$$au + bv = \text{pgcd}(a, b).$$

Preuve

Considérons G l'ensemble des entiers strictement positifs de la forme $\lambda a + \mu b$ où $\lambda, \mu \in \mathbb{Z}$. G contient $|a|$, c'est donc une partie non vide de $\mathbb{N}$. Ainsi, d'après la proposition 7.1, G admet un plus petit élément d tel que $d = au + bv$.

Notons $D = \text{pgcd}(a, b)$. Comme $D \mid a$ et $D \mid b$ on a donc, par la proposition 6.7, $D \mid au + bv$, c'est à dire $D \mid d$.

Considérons par ailleurs la division euclidienne de a par d : on a $a = dq + r$ où l'entier r satisfait $0 \leq r < d$. On en tire :

$$\begin{aligned} r &= a - dq \\ &= a - auq - bvq \\ &= a(1 - uq) + b(-vq) \end{aligned}$$

Si $r > 0$ alors $r \in G$ et $r < d$, c'est absurde puisque d est le plus petit élément de G, donc $r = 0$. Mais $r = 0$ revient à dire que $a = dq$, autrement dit $d \mid a$.

Mutatis mutandis on obtient aussi $d \mid b$.

Or si $d \mid a$ et $d \mid b$ alors $d \mid D$.

Finalement $D \mid d$ et $d \mid D$, on a donc $D = d$. Ainsi D est bien de la forme $\lambda a + \mu b$ où $\lambda, \mu \in \mathbb{Z}$.

Définition 7.6 : nombres premiers entre eux

- On dit que deux entiers a et b sont **premiers entre eux** quand ils n'ont n'ont pas de diviseur dans $\mathbb{N}$ autre que 1.
- Plus généralement, on dit que des entiers a_1, a_2, ..., a_k sont premiers entre eux si il n'existe pas d'entier naturel divisant chacun de ces nombres, autre que 1.
- Attention, on dit que des entiers a_1, a_2, ..., a_k sont deux à deux premiers entre eux si, quels que soient $i, j \in [\![1, k]\!]$, tels que $i \neq j$ les entiers a_i et a_j sont premiers entre eux.

Exemple 7.7

Les entiers -6, 10 et 11 sont premiers entre eux car il n'existe pas d'autre entier naturel que 1 divisant ces trois nombres. Par contre ils ne sont pas deux à deux premiers entre eux puisque 2 divise -6 et 10.

Remarque 7.8

a et b sont premiers entre eux si, et seulement si, $\operatorname{pgcd}(a, b) = 1$.

Théorème 7.9

Théorème de Bézout

Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Exercice 7.2 Démontrer le théorème de Bézout.

Théorème 7.10

Théorème de Gauss

Si des entiers a, b et c sont tels que $a \mid bc$ et a est premier avec b, alors a divise c.

Preuve

Comme a est premier avec b, on peut, d'après le théorème de Bézout, écrire $au+bv = 1$ pour des entiers u et v. Ainsi en multipliant par c on obtient $auc + bvc = c$. Comme a divise auc et bvc, il divise la somme qui vaut c.

Corollaire 7.11

Si b et c divisent a et si b et c sont premiers entre eux alors bc divise a.

Exercice 7.3 Démontrer ce corollaire à partir du théorème de Gauss.

Corollaire 7.12

Si a_1, a_2,..., a_n divisent b et si les a_i sont premiers entre eux deux à deux alors $a_1 a_2 \cdots a_n \mid b$.

Exercice 7.4 Démontrer ce corollaire à partir du précédent.

Proposition 7.13

Soit a, b, m et n des entiers, m et n étant premiers entre eux : $a \overset{[m]}{\equiv} b$ et $a \overset{[n]}{\equiv} b$ si, et seulement si, $a \overset{[mn]}{\equiv} b$.

Preuve

Implication : $a \overset{[m]}{\equiv} b$ et $a \overset{[n]}{\equiv} b$ équivaut à $\exists k, k' \in \mathbb{Z},\ a-b = km = k'n$. D'après le théorème de Gauss, m et m premiers entre eux et $km = k'n$ implique que $m \mid k'$, c'est-à-dire qu'il existe $k'' \in \mathbb{Z}$ tel que $k' = k''m$ donc tel que $a - b = k''mn$, ce qui traduit bien que $a \overset{[mn]}{\equiv} b$.

Réciproque : $a \overset{[mn]}{\equiv} b$ équivaut à $\exists k \in \mathbb{Z},\ a - b = kmn$. Ce que l'on peut écire aussi bien $\exists k \in \mathbb{Z},\ a - b = (km)n$ que $\exists k \in \mathbb{Z},\ a - b = (kn)m$.

III. Racines rationnelles d'un polynôme

Focus 7.14

Méthode de résolution

Résolvons $6x^3 - x^2 - 20x + 12 = 0$ dans $\mathbb{Q}$. On peut poser $x = \frac{p}{q}$ où $p \in \mathbb{Z}$, $q \in \mathbb{N}^\star$ et p et q sont premiers entre eux (fraction irréductible). L'équation s'écrit alors

$$6\left(\frac{p}{q}\right)^3 - \left(\frac{p}{q}\right)^2 - 20\left(\frac{p}{q}\right)x + 12 = 0.$$

Comme q ne peut pas être nul on peut multiplier par q^3 sans changer l'ensemble des solutions, ce qui donne $6p^3 - p^2q - 20pq^2 + 12q^3 = 0$, que l'on peut réécrire $p\left(6p^2 - pq - 20q^2\right) = -12q^3$. Puisque p et q sont premiers entre eux, p et q^3 le sont aussi, donc, d'après le théorème de Gauss, $p \mid -12$. Cela donne pour valeurs possibles de p les nombres -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6 et 12. De manière analogue $-6p^3 = q\left(p^2 - 20pq + 12q^2\right)$, donc $q \mid -6$, les valeurs possibles de q sont donc 1, 2, 3 et 6. Sachant que p et q sont premiers entre eux cela donne l'ensemble de solutions possibles 1, 2, 3, 4, 6, 12, $\frac{1}{2}$, $\frac{1}{2}$, $\frac{3}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{6}$ et leurs opposés. En les testant on trouve trois solutions -2, $\frac{2}{3}$ et $\frac{3}{2}$.

Proposition 7.15

Soit $P(x) = \sum_{i=0}^{n} a_i x^i$ un polynôme à coefficients entiers de degré n. Si l'équation $P(x) = 0$ admet une solution rationnelle qui s'exprime par la fraction irréductible $\frac{p}{q}$ alors $p \mid a_n$ et $q \mid a_0$.

Exercice 7.5 Résoudre dans $\mathbb{Q}$:

- $6x^3 + 7x^2 - 129x - 280 = 0$,
- $6x^3 + 5x^2 - 289x + 440 = 0$,
- $3x^4 + 29x^3 + 41x^2 - 145x - 280 = 0$,
- $3x^4 + x^3 - 117x^2 + 171x + 70 = 0$.

IV. pgcd et ppcm

Proposition 7.16

Soit $a, b \in \mathbb{Z}$. On a les propriétés suivantes :

1. $b \mid a \quad \Rightarrow \quad \text{pgcd}(a,b) = |b|$.
2. $n \mid a$ et $n \mid b \quad \Leftrightarrow \quad n \mid \text{pgcd}(a,b)$.
3. $\forall k \in \mathbb{N}^\star,\ \text{pgcd}(ka,kb) = k \cdot \text{pgcd}(a,b)$.
4. Si $d = \text{pgcd}(a,b)$, on peut écrire $a = da'$ et $b = db'$ où a' et b' sont premiers entre eux.

Preuve

1. Notons $D = \text{pgcd}(a,b)$. D est un diviseur de b donc d'après la proposition 6.5 $D \leq |b|$. D'autre part $b \mid a$ donc $|b| \mid b$ et $|b| \mid a$. Ainsi $|b|$ appartient à l'ensemble des diviseurs positifs communs à a et b, donc $|b| \leq D$. Finalement $D \leq |b|$ et $|b| \leq D$ implique $|b| = D$.

2. Notons $D = \text{pgcd}(a,b)$. Si $n \mid D$ comme $D \mid a$ et $D \mid b$, par transitivité $n \mid a$ et $n \mid b$. Réciproquement,d'après l'égalité de Bezout il existe des entiers μ et ν tels que $D = \mu a + \nu b$. Si $n \mid a$ et $n \mid b$ alors $n \mid \mu a + \nu b = D$.

3. Notons $D = \text{pgcd}(ka,kb)$ et $d = \text{pgcd}(a,b)$. Comme $d \mid a$ et $d \mid b$ on a $kd \mid ka$ et $kd \mid kb$. Ainsi kd est un diviseur commun de ka et kb donc $kd \mid D$ d'après la propriété précédente 7.16.2. Par ailleurs, d'après l'égalité de Bezout il existe des entiers μ et ν tels que $d = \mu a + \nu b$ donc $kd = \mu ka + \nu kb$. Comme $D \mid ka$ et $D \mid kb$ alors $D \mid kd$ d'après la proposition 6.7.

4. Puisque $d \mid a$ et $d \mid b$ il existe de entiers naturels a' et b' tels que $a = da'$ et $b = db'$. Posons $d' = \text{pgcd}(a',b')$. Il existe de entiers naturels a'' et b'' tels que $a' = d'a''$ et $b' = d'b''$. Mais alors $a = dd'a''$ et $b = dd'b''$, c'est à dire que dd' est un diviseur commun de a et b. Ceci implique que $dd' \mid d$ d'après la propriété précédente 7.16.2. On en conclut que $d' = 1$ puisque $d \in \mathbb{N}$.

Définition 7.17 : ppcm

Soient a et b deux entiers non tous deux nuls. L'ensemble des multiples strictement positifs communs de a et de b est non vide, il possède donc, par la proposition 6.10, un plus petit élément appelé **plus petit commun multiple** (ppcm) de a et de b.

Remarque 7.18

> On note souvent le ppcm de a et b par $\mathrm{ppcm}(a,b)$ mais aussi par $a \vee b$.

Proposition 7.19

$$\forall a,b,k \in \mathbb{Z}^\star,\ \mathrm{ppcm}(ka,kb) = k \cdot \mathrm{ppcm}(a,b).$$

Preuve

Posons $P = \mathrm{ppcm}(ka,kb)$. Le produit $k \cdot \mathrm{ppcm}(a,b)$ est un multiple de ka et de kb, on a donc, par définition, $P \leq k \cdot \mathrm{ppcm}(a,b)$. Réciproquement : P est un multiple de ka donc $\frac{P}{k}$ est un multiple de a, de même $\frac{P}{k}$ est un multiple de b, par définition $\mathrm{ppcm}(a,b) \leq \frac{P}{k}$.

Proposition 7.20

$$\forall a,b \in \mathbb{Z}, |ab| = \mathrm{ppcm}(a,b) \cdot \mathrm{pgcd}(a,b).$$

Preuve

Pour $a,b \in \mathbb{N}^\star$ pour simplifier.

- On se place dans le cas particulier où $\mathrm{pgcd}(a,b) = 1$. Comme $a \mid \mathrm{ppcm}(a,b)$ il existe $k \in \mathbb{N}^\star$ tel que $\mathrm{ppcm}(a,b) = ka$. Mais on a aussi $b \mid \mathrm{ppcm}(a,b) = ka$, or a et b sont dans ce cas particulier, premiers entre eux, donc, d'après le théorème de Gauss (théorème 7.10), $b \mid k$, c'est-à-dire qu'il existe $k' \in \mathbb{N}^\star$ tel que $k = k'b$, donc $\mathrm{ppcm}(a,b) = k'ab$. Par ailleurs ab est un multiple commun de a et de b donc, par définition, $\mathrm{ppcm}(a,b) \leq ab$. On en tire $k' = 1$ et $\mathrm{ppcm}(a,b) = ab$.

- On passe au cas général et on pose $d = \mathrm{pgcd}(a,b)$. Comme $d \mid a$ on a $a = da'$ pour un $a' \in \mathbb{N}^\star$ et manière analogue $b = db'$ pour un $b' \in \mathbb{N}^\star$. Maintenant

$$\begin{aligned} \mathrm{pgcd}(a',b') &= \mathrm{pgcd}\left(\frac{a}{d},\frac{b}{d}\right) \\ &= \frac{1}{d}\,\mathrm{pgcd}\,(a,b) \qquad \text{propriété 7.16.3} \\ &= 1. \end{aligned}$$

Ce qui signifie que a' et b' sont premiers entre eux. On en tire :

$$\begin{aligned} \mathrm{ppcm}(a,b) &= \mathrm{ppcm}(da',db') \\ &= d\,\mathrm{ppcm}(a',b') \qquad \text{proposition 7.19} \\ &= da'b' \qquad \text{cas particulier précédent} \\ &= \frac{1}{d}ab. \end{aligned}$$

Remarque 7.21

Cette proposition sera démontrée à nouveau plus loin, cette fois-ci à l'aide des décompositions en produits de facteurs premiers.

Proposition 7.22

Soit $a, b \in \mathbb{N}$. On a les propriétés suivantes :

1. Si $d = \text{pgcd}(a, b)$, on a $a = da'$ et $b = db'$ où a' et b' sont premiers et $\text{ppcm}(a, b) = a'db'$.
2. n est un multiple a et de b si et seulement si n est un multiple de $\text{ppcm}(a, b)$.
3. $a \mid b \quad \Rightarrow \quad \text{ppcm}(a, b) = b$.
4. $\text{pgcd}(a, b) = 1 \quad \Rightarrow \quad \text{ppcm}(a, b) = ab$.

Preuve

1. On a d'une part, par la proposition 7.20, $d \cdot \text{ppcm}(a, b) = ab$ et d'autre part $ab = a'db'd$, par la proposition 7.16.4. Donc $d \cdot \text{ppcm}(a, b) = a'db'd$ soit $\text{ppcm}(a, b) = a'db'$.
2. Soit $d = \text{pgcd}(a, b)$, on peut écrire $a = da'$ et $b = db'$ où a' et b' sont premiers entre eux (voir 7.16.4). Si $a \mid n$ c'est à dire $a'd \mid n$ alors $d \mid n$. Posons $n = dn'$. On a donc $a' \mid n'$ et $b' \mid n'$ avec a', b' premiers entre eux, d'après le théorème de Gauss $a'b' \mid n'$ donc $\text{ppcm}(a, b) = a'b'd \mid n'd = n$. Réciproquement si $\text{ppcm}(a, b) \mid n$ comme $a \mid \text{ppcm}(a, b)$ on aura $a \mid n$ et de même pour b.
3. D'après la propriété 7.16.1, $\text{pgcd}(a, b) = a$ (ici $a, b \in \mathbb{N}$). Or, par la proposition 7.20, $ab = \text{ppcm}(a, b) \cdot \text{pgcd}(a, b)$ donc $ab = \text{ppcm}(a, b)a$ puis $\text{ppcm}(a, b) = b$.
4. Par la proposition 7.22.1, $\text{ppcm}(a, b) = a' \cdot \text{pgcd}(a, b) \cdot b'$ où a' et b' sont premiers entre eux et ici $\text{pgcd}(a, b) = 1$.