4.2 Le pgcd, plus grand diviseur commun

Rappels

- **Dans $\mathbb{Z}$, tout sous groupe est de la forme $n\mathbb{Z}$; on en déduit donc que tout idéal est de la forme $n\mathbb{Z}$**
- **Les idéaux de la forme $n\mathbb{Z}$ sont dits principaux : $\mathbb{Z}$ est appelé anneau principal**
- **On dit que n engendre $n\mathbb{Z}$**

4.2.1 Proposition

Pour tout $m \in \mathbb{Z}$ et tout $n \in \mathbb{Z}$, $m\mathbb{Z} \subset n\mathbb{Z}$, si et seulement si $n \mid m$

Remarque 7 :

1. Un diviseur propre n de m définit donc un idéal $n\mathbb{Z}$ plus grand que $m\mathbb{Z}$
2. **Exemple :**
   Nous avons $2 \mid 6$ et $6\mathbb{Z} \subset 2\mathbb{Z}$, les multiples de 6 étant aussi des multiples de 2. Par contre, $4 \notin 6\mathbb{Z}$: 4 est un multiple de 2, mais pas de 6

Démonstration

1. **Supposons $m\mathbb{Z} \subset n\mathbb{Z}$, et montrons que $n \mid m$**
   Si $m\mathbb{Z} \subset n\mathbb{Z}$, alors comme $m \in m\mathbb{Z}$ et que $m\mathbb{Z} \subset n\mathbb{Z}$, nous avons, en particulier $m \in m\mathbb{Z}$.
   Il existe donc $k \in \mathbb{Z}$ tel que $m = kn$, donc $n \mid m$
2. **Réciproquement, supposons $n \mid m$, et montrons que $m\mathbb{Z} \subset n\mathbb{Z}$**
   Si $n \mid m$, ceci veut dire qu'il existe $k \in \mathbb{Z}$ tel que $m = kn$, et donc $m \in n\mathbb{Z}$, et tout multiple de m devient donc un multiple de n, ce qui montre que $m\mathbb{Z} \subset n\mathbb{Z}$

4.2.2 Théorème admis

Soit $n_1\mathbb{Z} \subset n_2\mathbb{Z} \subset \cdots \subset n_k\mathbb{Z} \subset \cdots n_{p-1}\mathbb{Z} \subset n_p\mathbb{Z}$ une suite croissante d'idéaux de $\mathbb{Z}$
Alors, il existe un entier p tel que $n_p\mathbb{Z} = n_{p+1}\mathbb{Z} = n_{p+2}\mathbb{Z} = \cdots$

Remarque 8 :

Même si nous admettons ce théorème, nous pouvons en faire des commentaires.

1. Si $n_1\mathbb{Z} \subset n_2\mathbb{Z} \subset n_3\mathbb{Z} \subset n_4\mathbb{Z} \subset \cdots \subset n_k\mathbb{Z} \subset \cdots \subset n_{p-1}\mathbb{Z} \subset n_p\mathbb{Z}$, alors $n_p \mid n_{p-1}$, $n_{p-1} \mid n_{p-2}$, jusque $n_2 \mid n_1$. Par transitivité, $n_2, n_2, n_3, n_4, \cdots n_k, \cdots, n_{p-1}, n_p$ sont tous des diviseurs de n_1, et ces diviseurs sont en nombre fini.
   Soit u le plus petit diviseur de n_1, u est un nombre premier, et il n'existe pas d'autre diviseur de u, donc pas de diviseur plus petit de n_1
2. Tout idéal engendré par un nombre premier est appelé **idéal premier**.

4.2.3 Définition de pgcd

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$; on appelle plus grand diviseur commun à a et à b ou pgcd de a et de b, un entier $d \in \mathbb{Z}$ tel que la proposition suivante soit vraie :

$$(\forall c \in \mathbb{Z})\,(d|a \quad d|b \quad c|a \quad c|b) \Longrightarrow (c|d)$$

On note $d = \text{pgcd}\,(a, b)$ ou $d = a \wedge b$

Remarque 9 :

1. Si $d = \text{pgcd}(a, b)$, alors d est le multiple de tout nombre diviseur commun à a et b et tout diviseur commun à a et b divise d
2. 2 pgcd différents de a et b, sont en fait associés. *(Dans $\mathbb{Z}$, d et $-d$ sont en fait* pgcd *de a et b)*

4.2.4 Théorème *(Important)*

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$

1. **Soit $I = a\mathbb{Z} + b\mathbb{Z} = \{z \in \mathbb{Z}$ tels que $\exists (k_1, k_2) \in \mathbb{Z}^2$ tels que $z = k_1 a + k_2 n\}$; alors, I est un idéal de $\mathbb{Z}$**
2. **I est engendré par $d = \text{pgcd}(a, b)$, c'est à dire que $I = a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$**
3. **Il existe donc $(u, v) \in \mathbb{Z}^2$ tels que $d = au + bv$**

Démonstration

1. Démontrons que $I = a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$
   — Tout d'abord, I est un sous-groupe de $\mathbb{Z}$
   En effet
   - $I \neq \emptyset$ puisque $0 = a \times 0 + b \times 0$ et donc $0 \in I$
   - D'autre part, si $u \in I$ et $v \in I$, alors $u = am + bn$ et $v = am' + bn'$ et donc $u - v = a(m - m') + b(n - n')$. Donc, $u - v \in I$
   - Des 2 items ci-dessus, on déduit que I est un sous-groupe de $\mathbb{Z}$

   — Soit $r \in \mathbb{Z}$ et $u \in I$. Alors $ru = r(am + bn) = a(mr) + b(nr)$
   Donc $ru \in I$
   I est donc un idéal de $\mathbb{Z}$
2. Démontrons que $a\mathbb{Z} + b\mathbb{Z}$ est engendré par $d = \text{pgcd}(a, b)$
   — $a\mathbb{Z} + b\mathbb{Z}$ étant un idéal de $\mathbb{Z}$, sachant que tous les idéaux de $\mathbb{Z}$ sont de la forme $\lambda\mathbb{Z}$ avec $\lambda \in \mathbb{N}$, il existe donc un nombre $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
   — Remarquons d'abord que $a\mathbb{Z} \subset d\mathbb{Z}$
   Soit $y \in a\mathbb{Z}$, alors, $y = ak$, et comme $ak = ak + b \times 0$, $ak \in d\mathbb{Z}$; donc $a\mathbb{Z} \subset d\mathbb{Z}$, et, de même, $b\mathbb{Z} \subset d\mathbb{Z}$, donc $d \mid a$ et $d \mid b$
   — Montrons que $d = \text{pgcd}(a, b)$.
   Soit donc $c \in \mathbb{Z}$ tel que $c \mid a$ et $c \mid b$; comme $d = sa + tb$, que $a = ck$ et $b = ck'$, nous avons $d = sck + tck'$, c'est à dire : $d = c(sk + tk')$, et donc $c \mid d$; ce qui traduit donc que $d = \text{pgcd}(a, b)$
3. Comme $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, il existe donc $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que $d = au + bv$

Remarque 10 :

1. Nous venons de montrer que **si** $d = \text{pgcd}(a, b)$, **alors** il existe donc $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que $d = au + bv$
2. Avons nous la réciproque ?
   C'est à dire que s'il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que $d = au + bv$ avons nous $d = \text{pgcd}(a, b)$?
   La réponse est non : nous avons $3 = \text{pgcd}(6, 15)$; il existe donc $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que $3 = 6u + 15v$: il suffit de choisir $u = -2$ et $v = +1$.
   Mais nous avons aussi $6 = 6 \times (-4) + 15 \times (2)$, alors que 6 n'est pas le pgcd de 6 et 15 car 6 ne divise pas 15.

Exercice 12 :

Généralisation :
Soit $(R, +, \times)$ un anneau, I et J, deux idéaux de R
Montrer que $I + J = \{z \in R$ tels que $\exists (x, y) \in I \times J$ tels que $z = x + y\}$ est un idéal de R

4.2.5 Nombres premiers entre eux

Soient $(a,b) \in \mathbb{Z} \times \mathbb{Z}$
On dit que a et b entiers naturels sont premiers entre eux si et seulement si $\text{pgcd}(a,b) = a \wedge b = 1$

Remarque 11 :

1. Deux nombres premiers sont forcément premiers entre eux.
2. Deux nombres premiers entre eux n'ont forcément aucun diviseur commun, sauf 1.
   Exemple : 45 et 14
   45 et 14 ne sont pas des nombres premiers, mais sont des nombres premiers entre eux puisque $45 = 5 \times 3^2$ et $14 = 2 \times 7$

4.2.6 Proposition

Soient a et b 2 entiers naturels non nuls, et $d = \text{pgcd}(a,b)$. Soient a' et b' tels que $a = a'd$ et $b = b'd$. Alors, a' et b' sont premiers entre eux.

Démonstration

Soit c un diviseur commun de a' et b', c'est à dire que : $a' = cx$ et $b' = cy$
Alors, $a = cxd = (cd)\,x$ et $b = cyd = (cd)\,y$, ce qui montre que cd est un diviseur commun de a et b, donc, parce que $d = \text{pgcd}(a,b)$, $cd \mid d$.
Comme $d \mid cd$, nous avons $cd = d$, et donc, $c = 1$
C'est à dire $\text{pgcd}(a',b') = 1$

4.2.7 Identité de Bachet-Bezout

Soient a et b deux entiers de $\mathbb{Z}$; les propriétés suivantes sont équivalentes :

1. **Ces deux nombres a et b sont premiers entre eux**
2. **Il existe deux entiers u et v tels que : $au + bv = 1$**
3. **$a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$**

Démonstration

1. **Supposons que a et b soient premiers entre eux**
   Alors, $\text{pgcd}(a,b) = 1$, et, d'après le théorème 4.2.4 ci-dessus, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + bv = 1$
2. **Supposons qu'il existe deux entiers u et v tels que : $au + bv = 1$**
   Montrons que $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$
   - ⋆ Clairement, nous avons $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$
   - ⋆ Démontrons, maintnant, que $\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$
     Soit donc $m \in \mathbb{Z}$, alors :
     $$m = m \times 1 = m(au + bv) = a(mu) + b(mv)$$
     et donc $m \in a\mathbb{Z} + b\mathbb{Z}$
   Donc $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$
3. **Supposons qu' il existe deux entiers u et v tels que : $au + bv = 1$**
   Démontrons que $\text{pgcd}(a,b) = 1$
   1 est évidemment un diviseur de a et b.
   Soit d un diviseur commun à a et b. Alors, $a = da'$ et $b = db'$, et nous avons $da'u + db'v = d(a'u + b'v) = 1$, c'est à dire que $d \mid 1$; donc, tout diviseur commun de a et b divise 1 ; donc, $\text{pgcd}(a,b) = 1$

Remarque 12 :

1. Par rapport à la remarque précédente sur le pgcd, nous avons, ici, un résultat bien plus fort : **une équivalence.**
2. Nous pouvons, dès maintenant, donner une autre démonstration de la proposition 4.2.6
   Supposons donc que $d = \text{pgcd}(a,b)$ et soient $a' \in \mathbb{Z}$ et $b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$
   Comme $d = \text{pgcd}(a,b)$, il existe $u \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $ua + bv = d$. Or :
   $$ua + bv = d \iff u(a'd) + v(b'd) = d \iff ua' + vb' = 1$$
   Donc, d'après le théorème 4.2.7, $\text{pgcd}(a',b') = 1$, c'est à dire que a' et b' sont premier entre eux
3. Point d'Histoire : c'est plus un résultat dû à Bachet qu'à Bezout. Bezout a généralisé ce résultat aux polynômes, les nombres ne devenant qu'un cas particulier.

Exercice 13 :

a, b, c et d sont 4 entiers naturels non nuls tels que $ab - dc = 1$

1. Démontrer que cette relation est équivalente à $a(b+d) - d(c+a) = 1$
2. En déduire que les fractions $\dfrac{a}{a+c}$, $\dfrac{d}{b+d}$ et $\dfrac{a+c}{b+d}$ sont irréductibles

4.2.8 Conséquences de la définition de pgcd

Cette proposition contient des redites, notamment de 4.2.6 ; mais, elle a l'intérêt de faire une synthèse.

1. **Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $k \in \mathbb{Z}$. Alors :**
   $$\text{pgcd}(ka, kb) = |k| \,\text{pgcd}(a,b)$$
2. **Soit $d \in \mathbb{Z}$, un diviseur commun à a et à b. Alors :**
   $$\text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{|d|}\text{pgcd}(a,b)$$
3. **Conséquence :**
   Soit d un diviseur commun à a et à b. On suppose donc que $a = da'$ et $b = db'$. Alors :
   $$d = \text{pgcd}(a,b) \iff \text{pgcd}(a',b') = 1$$

Démonstration

1. Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $k \in \mathbb{Z}$ et soit d le pgcd de a et b, c'est à dire $d = \text{pgcd}(a,b)$ et d' le pgcd de ka et kb, c'est à dire $d' = \text{pgcd}(ka, kb)$
   Alors, nous avons $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $ka\mathbb{Z} + kb\mathbb{Z} = d'\mathbb{Z}$
   — Soit $x \in d'\mathbb{Z}$; alors, il existe $\lambda \in \mathbb{Z}$ tel que $x = \lambda d'$. Mieux, il est possible d'écrire
   $$x = u(ka) + v(kb) = k(au + bv) \text{ avec } u \in \mathbb{Z} \text{ et } b \in \mathbb{Z}$$
   Or, $au + bv \in a\mathbb{Z} + b\mathbb{Z}$, c'est à dire $au + bv \in d\mathbb{Z}$, c'est à dire $x = k\mu d = \mu kd$.
   x est donc aussi un multiple de kd et donc $x \in kd\mathbb{Z}$. Nous avons donc $d'\mathbb{Z} \subset kd\mathbb{Z}$
   — Réciproquement, soit $x \in kd\mathbb{Z}$. Alors, il existe $\lambda \in \mathbb{Z}$ tel que $x = \lambda kd$. Comme il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $d = au + bv$, nous avons :
   $$x = \lambda kd = \lambda k(au + bv) = (\lambda u)ka + (\lambda v)kb$$
   Donc $x \in ka\mathbb{Z} + kb\mathbb{Z}$, c'est à dire $x \in d'\mathbb{Z}$. Nous avons donc $kd\mathbb{Z} \subset d'\mathbb{Z}$

Donc $kd\mathbb{Z} = d'\mathbb{Z}$. D'où $\text{pgcd}\,(ka, kb) = |k|\,\text{pgcd}\,(a, b)$

2. Soit $d \in \mathbb{Z}$, un diviseur commun à a et à b. Alors, nous avons $a = da'$ et $b = db'$. D'après le point précédent, nous avons :

$$\text{pgcd}\,(a, b) = \text{pgcd}\,(da', db') = |d|\,\text{pgcd}\,(a', b')$$

C'est à dire $\text{pgcd}\,(a, b) = |d|\,\text{pgcd}\,(a', b')$; si nous utilisons :$a = da' \iff a' = \dfrac{a}{d}$ et $b = db' \iff b' = \dfrac{b}{d}$, nous obtenons :

$$\text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{|d|}\text{pgcd}\,(a, b)$$

3. Cette fois ci, supposons $d = \text{pgcd}\,(a, b)$; alors, toujours d'après le point précédent,

$$d = \text{pgcd}\,(a, b) = d\text{pgcd}\,(a', b')$$

Donc, en simplifiant par d, $\text{pgcd}\,(a', b') = 1$

4.2.9 Théorème

Soit p un nombre premier.
Alors, pour tout nombre $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ $p \mid ab \Longrightarrow (p \mid a)$ ou $(p \mid b)$

Démonstration

Supposons $p \mid ab$, alors, $ab = pk$
p est un nombre premier ; donc, il y a deux possibilités : $\text{pgcd}\,(a, p) = 1$ ou bien $\text{pgcd}\,(a, p) = p$

- Si $\text{pgcd}\,(a, p) = p$, alors $p \mid a$, et c'est terminé
- Si $\text{pgcd}\,(a, p) = 1$, alors, il existe u et v tels que $au + pv = 1$, et donc, en multipliant par b, on obtient :

$$b\,(au + pv) = bau + bpv = pku + bpv = p\,(ku + bv) = b$$

C'est à dire $p \mid b$

4.2.10 Corollaire : lemme de Gauss

Si le nombre a divise le produit bc, et si $\text{pgcd}\,(a, b) = 1$, alors a divise c, c'est à dire, en langage formalisé :

$$a \mid bc \text{ et } \text{pgcd}\,(a, b) = 1 \Longrightarrow a \mid c$$

Démonstration

C'est la seconde partie de la démonstration du théorème 4.2.9 précédent.

4.2.11 Unicité de la décomposition en un produit de facteurs premiers

Tout élément de $m \in \mathbb{Z}$ se décompose de manière unique un produit $p_1 \times p_2 \times \cdots \times p_n$ de facteurs premiers.

Démonstration

L'existence a été démontrée dans le théorème 4.1.6. A l'aide du lemme de Gauss, il est venu le temps de la démonstration de l'unicité de cette décomposition.
Soit $N \in \mathbb{N}$ et supposons que N admette 2 décompositions en un produit de facteurs premiers, c'est à dire :

$$N = p_1 \times p_2 \times \cdots \times p_k = q_1 \times q_2 \times \cdots \times q_j$$

Où les p_i et les q_i sont des nombres premiers.
p_1 divise donc $q_1 \times q_2 \times \cdots \times q_j = N$ et p_1 est premier. Il existe donc i tel que $p_1 = q_i$; supposons, pour simplifier que $p_1 = q_1$. Nous avons donc :

$$p_2 \times p_3 \times \cdots \times p_k = q_2 \times q_3 \times \cdots \times q_j$$

Ce raisonnement peut être recommencé pour tout nombre p_i où $1 \leqslant i \leqslant k$ et donc $\{p_1, p_2, \cdots, p_k\} \subset \{q_1, q_2, \cdots, q_j\}$
Avec le même raisonnement, nous avons $\{q_1, q_2, \cdots, q_j\} \subset \{p_1, p_2, \cdots, p_k\}$, et donc nous avons :

$$\{q_1, q_2, \cdots, q_j\} = \{p_1, p_2, \cdots, p_k\}$$

Ce qui prouve donc l'unicité de la décomposition de N

4.2.12 Quelques exercices

Exercice 14 :

1. Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, si $\text{pgcd}\,(a, c) = 1$, alors $\text{pgcd}\,(a, b) = \text{pgcd}\,(a, bc)$
2. Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, nous avons

   $$\text{pgcd}\,(a, c) = 1 \text{ et } \text{pgcd}\,(a, b) = 1 \text{ équivalent à } \text{pgcd}\,(a, bc) = 1$$

   Ce résultat nous autorise à écrire :

   $$\text{pgcd}\,(a, b) = 1 \iff (\forall m \in \mathbb{N})\,(\forall n \in \mathbb{N})\,\text{pgcd}\,(a^m, b^n) = 1$$

3. Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, nous avons l'équivalence suivante :

   $$\text{pgcd}\,(a, b) = 1 \Leftrightarrow \text{pgcd}\,(ab, a + b) = 1$$

Exercice 15 :

Montrer que pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, si $\text{pgcd}\,(a, b) = 1$ et si $a \mid c$ et $b \mid c$ alors $ab \mid c$

Exercice 16 :

Montrer que pour tout $n \in \mathbb{N}^*$ nous avons :

1. $\left(n^2 + n\right) \wedge (2n + 1) = 1$
2. $\left(3n^2 + 2n\right) \wedge (n + 1) = 1$
3. $\left(2^n + 3^n\right) \wedge \left(3^{n+1} + 2^{n+1}\right) = 1$

Exercice 17 :

Trouver les nombres entiers naturels tels que :

$$\begin{cases} a + b = 182 \\ \text{pgcd}\,(a, b) = 13 \end{cases}$$

Exercice 18 :

1. On considère deux entiers quelconques $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On considère 2 nombres A et B tels que :

   $$A = 5a + 4b \qquad \text{et} \qquad B = 11a + 9b$$

   Démontrer que $\text{pgcd}\,(a, b) = \text{pgcd}\,(A, B)$
2. **Généralisation**
   On considère 2 nombres A' et B' tels que :

   $$A' = pa + qb \qquad \text{et} \qquad B' = ra + sb \qquad \text{avec } ps - qr = 1$$

   Démontrer que $\text{pgcd}\,(a, b) = \text{pgcd}\,(A', B')$

Exercice 19 :

1. Montrer que pour tout entier $n \in \mathbb{N}^*$, $n + 1$ et $2n + 1$ sont premiers entre eux.
2. En déduire que $n + 1 \mid \text{C}_{2n}^n = \binom{2n}{n}$

Exercice 20 :

1. Pour $n \in \mathbb{N}$, montrer qu'il existe un unique couple $(a_n, b_n) \in \mathbb{N}^2$ tel que :

   $$\left(1 + \sqrt{2}\right)^n = a_n + b_n\sqrt{2} \text{ et } \left(1 - \sqrt{2}\right)^n = a_n - b_n\sqrt{2}$$

2. Calculer $a_n^2 - 2b_n^2$
3. En déduire que a_n et b_n sont premiers entre eux