Sous-groupes additifs de Z. Égalité de Bézout. Résolution dans Z d'une équation de la forme ax+by=c.

Il s'agit de l'exposé de CAPES numéro 12 (2006). Les prérequis principaux sont les suivants :

- Le fait que toute partie non vide de $\mathbf{N}$ admet un plus petit élément.
- La division euclidienne.
- La notion de divisibilité.
- Les généralités sur les groupes, sous-groupes, etc. En particulier le fait que, si on a deux sous-groupes H, K d'un groupe abélien G, $H \cap K$ et $H + K$ sont des sous-groupes.

1 Sous-groupes additifs de Z

1.1 Description des sous-groupes

On note $n\mathbf{Z}$ ou (n) l'ensemble des multiples de l'entier n (i.e. l'ensemble des nx, pour $x \in \mathbf{Z}$). Il est clair que c'est un sous-groupe additif de $\mathbf{Z}$. On dit que n est un générateur de $n\mathbf{Z}$ et que ce sous-groupe est monogène.

1.1 *Remarque.* Si I est un sous-groupe additif de $\mathbf{Z}$ et si on a $n \in I$ et $q \in \mathbf{Z}$, on a aussi[1] $qn \in I$. En effet, si q est ≥ 0, qn c'est $n + n + \cdots + n$ (q fois), de sorte que qn est dans I et si q est < 0, on a $q = -q'$, avec $q' > 0$, donc $q'n \in I$ et $qn = -(q'n) \in I$.

Le théorème suivant montre que tous les sous-groupes de $\mathbf{Z}$ sont monogènes :

[1] Cela signifie que I est automatiquement un idéal de $\mathbf{Z}$, bien entendu, mais comme le titre de l'exposé ne fait plus référence aux idéaux on n'est pas obligé de prononcer le mot. Si on le fait il faut être capable de répondre à quelques questions : donner un exemple d'un sous-groupe qui n'est pas un idéal (les polynômes de degré $\leq n$), ou donner un exemple d'anneau non principal (les polynômes à plusieurs variables), etc.

1.2 Théorème. *Tout sous-groupe additif de* $\mathbf{Z}$ *est de la forme* $n\mathbf{Z}$ *avec* $n \in \mathbf{N}$.

Démonstration. Soit I un sous-groupe. Le résultat est évident si I ne contient que 0. Sinon, I contient un élément $n > 0$ (si $n \neq 0$ est dans I, $-n$ aussi et l'un des deux est > 0). L'ensemble non vide $I \cap \mathbf{N}^*$ admet alors un plus petit élément n. Je dis qu'on a $I = n\mathbf{Z}$. La remarque 1.1 montre que $n\mathbf{Z}$ est contenu dans I. Réciproquement, si a est dans I on effectue la division euclidienne de a par n : $a = nq + r$ avec $0 \leq r < n$. Comme n est dans I, il en est de même de nq (toujours par 1.1), donc aussi de $r = a - nq$. Comme n est le plus petit élément > 0 de I, cela impose $r = 0$, donc $a \in n\mathbf{Z}$.

1.2 Sous-groupes et divisibilité

Le point essentiel, qui fait que les sous-groupes ont un rôle à jouer par rapport à la divisibilité vient du fait que (a) est l'ensemble des multiples de a, précisément :

1.3 Proposition. *Soient* $a, b \in \mathbf{Z}$. *On a l'équivalence* $a|b \iff (b) \subset (a)$.

Démonstration. Si a divise b on a $b = ac$ et tout multiple de b est multiple de a, de sorte qu'on a $(b) \subset (a)$. Réciproquement, si on a $(b) \subset (a)$, b est dans (a), donc multiple de a.

1.4 *Remarque.* La relation $(a) = (b)$, qui équivaut à $a|b$ et $b|a$, est encore équivalente à $b = \pm a$. En effet, si on a $a = bc$ et $b = ad$, on a $a = acd$, soit $a(1 - cd) = 0$ et cela entraîne soit $a = 0$ (donc $b = 0$), soit $c = d = \pm 1$. Un sous-groupe non nul admet donc exactement deux générateurs opposés.

2 PGCD et PPCM

2.1 La problématique

La proposition précédente montre que la relation de divisibilité[2] est essentiellement équivalente à l'inclusion sur les sous-groupes (changée de sens). En particulier les questions naturelles qui concernent cette relation (exis-

[2]Cette relation est un préordre : réflexive, transitive, mais pas tout à fait antisymétrique puisque $a|b$ et $b|a$ signifie $a = \pm b$.

tence d'un inf et d'un sup[3] par exemple) vont se résoudre en passant aux sous-groupes.

Les définitions suivantes sont les plus naturelles avec l'entrée choisie ici :

2.1 Définition. *Soient $a, b \in \mathbf{Z}$.*

1) Un élément $d \in \mathbf{Z}$ est appelé un PGCD *de a et b (et on note $d =$ PGCD (a, b) ou $d = a \wedge b$) si c'est une borne inférieure[4] de a et b au sens de la relation de divisibilité, c'est-à-dire s'il vérifie les deux propriétés suivantes :*

- *d divise a et b,*
- *si c divise a et b, c divise d (autrement dit, les diviseurs communs à a et b sont exactement les diviseurs de d).*

2) Un élément $m \in \mathbf{Z}$ est appelé un PPCM *de a et b si c'est une borne supérieure de a et b au sens de la relation de divisibilité, c'est-à-dire s'il vérifie les deux propriétés suivantes :*

- *a et b divisent m,*
- *si a et b divisent c, m divise c.*

On note $m = PPCM(a, b)$ ou $m = a \vee b$.

2.2 *Remarques.*

1) On prendra garde de respecter (au moins provisoirement) la notation PGCD , PPCM avec des majuscules, car il va y avoir plus loin des pgcd et ppcm.

2) On notera que si d est un PGCD (resp. si m est un PPCM) il en est de même de $-d$ (resp. $-m$). Réciproquement, si d, d' sont deux PGCD , ils se divisent mutuellement, donc sont opposés et de même pour les PPCM .

2.2 Existence

La proposition 1.3 montre qu'un PGCD (resp. un PPCM) correspond sur les sous-groupes à un sup (resp. un inf). Elle permet de montrer le théorème suivant :

2.3 Théorème. *Soient $a, b \in \mathbf{Z}$.*

1) Si d est un générateur du sous-groupe :

$$(a, b) := (a) + (b) = \{\lambda a + \mu b \ \mid \ \lambda, \mu \in \mathbf{Z}\},$$

[3]Dans une version antérieure, je parlais de minimum et de maximum au lieu d'inf et de sup. Cela a provoqué un vif débat sur le forum http ://www.les-mathematiques.net/phorum. Je remercie Michel Coste de m'avoir signalé le problème, et j'ai pris la précaution ici de donner des définitions plus conforme aux usages. En tous cas, cet épisode m'a permis de constater avec plaisir que j'ai des lecteurs.

[4]C'est le mot utilisé par Bourbaki, mais je l'éviterai pour sa connotation trop marquée avec l'ordre des nombres réels. Je dirai simplement *inf* et *sup*.

c'est un PGCD *de a et b et il existe des entiers $\lambda, \mu \in \mathbf{Z}$ qui vérifient $\lambda a + \mu b = d$ (relation de Bézout).*
2) Si m est un générateur du sous-groupe $(a) \cap (b)$, c'est un PPCM *de a et b.*

Démonstration. 1) Le sous-groupe $(a) + (b)$ est le plus petit sous-groupe contenant à la fois (a) et (b). C'est donc le *sup* de ces sous-groupes et ses générateurs sont des PGCD de a et b en vertu de 1.3. Comme d est dans $(a) + (b)$ on a bien une relation de Bézout.

(Précisons la preuve : on pose $(d) = (a) + (b)$. Comme on a $(a) \subset (d)$ et $(b) \subset (d)$, on a, par 1.3, $d|a$ et $d|b$. Si c est un diviseur de a et de b, on a $(a) \subset (c)$ et $(b) \subset (c)$, donc $(a) + (b) \subset (c)$, soit encore $(d) \subset (c)$ et donc $d|c$, toujours en vertu de 1.3).

2) Le raisonnement est identique pour le PPCM .

2.3 Nombres premiers entre eux

2.3.1 Définition

2.4 Définition. *Deux nombres a et b sont dits premiers entre eux s'ils n'ont pas de diviseurs communs autres que ± 1.*

2.5 Proposition.
1) Deux nombres a et b sont premiers entre eux si et seulement si le sous-groupe (a, b) est égal à $\mathbf{Z}$, ou encore si le PGCD de a est b est ± 1.
2) Les nombres a et b sont premiers entre eux si et seulement si il existe $\lambda, \mu \in \mathbf{Z}$ avec $\lambda a + \mu b = 1$.

Démonstration. Le point 1) vient du fait que les diviseurs communs à a et b sont les diviseurs de leur PGCD (cf. 2.1). Il en résulte, avec 2.3, que si a, b sont premiers entre eux ils vérifient une relation de Bézout. Réciproquement, si on a $1 = \lambda a + \mu b$, il est clair que tout diviseur commun à a et b divise 1, donc vaut ± 1.

2.3.2 La comptine du PGCD

2.6 Proposition. *Soient $a, b \in \mathbf{Z}$. Le nombre d est un* PGCD *de a et b s'il vérifie la "comptine du PGCD" : on peut écrire $a = da'$, $b = db'$ avec a' et b' premiers entre eux.*

Démonstration. Si d est un PGCD , il divise a et b et on a donc $a = da'$, $b = db'$. De plus, si c divise a' et b', dc divise a et b, donc il divise d et on a

$c = \pm 1$. Réciproquement, si on a $a = da'$, $b = db'$ on a $(a, b) \subset (d)$. Si, de plus, a' et b' sont premiers entre eux, on a une relation de Bézout $\lambda a' + \mu b' = 1$, donc $\lambda a + \mu b = d$ et $(d) \subset (a, b)$. En définitive, on a $(d) = (a, b)$, donc d est un PGCD de a et b.

2.3.3 Lien entre PPCM et PGCD

2.7 Proposition. *Soient $a, b \in \mathbf{Z}$. On a* $\mathrm{PGCD}\,(a, b) \times \mathrm{PPCM}\,(a, b) = \pm ab$.

Démonstration. Soit d un PGCD de a, b. On écrit la comptine : $a = da'$, $b = db'$, avec a', b' premiers entre eux et il suffit de montrer que $m = da'b'$ est un PPCM de a et b (car on a $md = ab$). C'est clairement un multiple commun. Pour voir que c'est le PPCM, on prend un multiple quelconque n de a, b et il s'agit de voir qu'il est multiple de m. Pour cela on écrit une relation de Bézout : $d = \lambda a + \mu b$ et on multiplie par n : $nd = \lambda an + \mu bn$. Comme an et bn sont multiples de ab, on voit que nd est multiple de $ab = md$, donc que n est multiple de m.

2.4 Les pgcd et ppcm ordinaires

Cette fois on travaille dans $\mathbf{N}$ et on fait le lien avec les notions plus élémentaires de pgcd et ppcm. On renvoie à [Perrin1] pour des détails. Rappelons les définitions suivantes :

2.8 Définition.
1) Soient $a, b \in \mathbf{N}$, non tous deux nuls. On appelle $\mathrm{pgcd}\,(a, b)$ *un nombre $d \in \mathbf{N}$ qui divise a et b et qui est le plus grand (au sens de la relation d'ordre ordinaire) pour cette propriété.*
2) Soient $a, b \in \mathbf{N}$, tous deux non nuls. On appelle $\mathrm{ppcm}\,(a, b)$ *un nombre m qui est un multiple commun de a et b et qui est le plus petit pour cette propriété.*

2.9 *Remarque.* L'existence et l'unicité du pgcd et du ppcm viennent des propriétés de $\mathbf{N}$ (existence de plus petit ou plus grand élément). On prendra garde aux hypothèses de non nullité ; on peut poser, si l'on veut, $\mathrm{pgcd}\,(0, 0) = 0$ et $\mathrm{ppcm}\,(a, 0) = 0$.

2.10 Proposition. *Soient $a, b \in \mathbf{N}$ non tous deux nuls (resp. tous deux non nuls) et soit $d \in \mathbf{N}$ (resp $m \in \mathbf{N}$). Alors d est le* pgcd *(resp. le* ppcm*) de a et b si et seulement si c'en est un* PGCD *(resp. un* PPCM*).*

Démonstration. Il est clair que si $d > 0$ est un PGCD de a et b c'est aussi un pgcd car $c|d$ implique $c \leq d$ dans $\mathbf{N}$. Réciproquement, si d est le pgcd, soit δ le PGCD positif de a et b. Comme d est un diviseur commun, il divise δ, donc est $\leq \delta$, comme δ est un diviseur commun il est $\leq d$. Ils sont donc égaux.

2.5 Compléments

2.5.1 L'algorithme d'Euclide

Voir [Perrin1] chapitre 1 paragraphe 3.b. Voir [Perrin2] pour un programme.

2.5.2 Exercices

Voir [Perrin1] et tous les exercices du genre : trouver a et b connaissant leur somme et leur pgcd, etc. Noter aussi les exercices du genre : pour quels n les nombres $2n + 1$ et $9n + 4$ sont-ils premiers entre eux ?

3 Équations diophantiennes de degré 1

On renvoie à [Perrin1] Chapitre 1, paragraphe 3.g où c'est vachement bien et aux exercices et problèmes sur ce sujet.

Voir aussi tous les exercices sur les équations diophantiennes. En voici un autre qui n'est pas dedans : l'auberge d'Euler.

Un soir, dans une auberge, plusieurs diligences font halte pour manger. Il y a des hommes et des femmes (mais moins de femmes que d'hommes, c'est l'époque qui veut ça). Les hommes paient 19 sous, les femmes 13, l'aubergiste récolte 1000 sous. Combien y a-t-il d'hommes et de femmes ?

4 Références

[Perrin1] Daniel Perrin, Mathématiques d'école, Cassini, 2005.

[Perrin2] Daniel Perrin, Bézout par les matrices (sur ma page web).