Exposé 13 :

L'anneau $\mathbb{Z}$, sous groupes additifs de $\mathbb{Z}$. Les idéaux de $\mathbb{Z}$ sont principaux. Egalité de Bezout. Résolution dans $\mathbb{Z}$ d'une équation de la forme $ax+by=c$

0_ Pré-Requis :

- def anneaux, groupe, idéal, sous groupe.
- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

I. Entiers Relatifs :

1) Anneau $(\mathbb{Z},+,\times)$

• $(\mathbb{Z},+,\times)$ est un anneau non vide, commutatif et intègre.

[$0\in\mathbb{Z}$, $ab=ba$ et $\forall a,b\in\mathbb{Z}$ $ab=0 \Rightarrow a=0$ ou $b=0$

• La relation d'ordre usuelle sur $\mathbb{Z}$ est compatible avec l'addition et la multiplication : $\forall a,b,c\in\mathbb{Z}$ $a\leq b \Rightarrow a+c\leq b+c$

$\forall a,b,c\in\mathbb{Z}$ et $c>0$ $a\leq b \Rightarrow ac\leq bc$

• $(\mathbb{Z},+,\cdot,\geqslant)$ est un anneau totalement ordonné

$\Rightarrow (\mathbb{Z},+,\cdot\geqslant)$ est anneau, non vide, intègre, commutatif et totalement ordonné.

Rq : $\mathbb{Z}$ est aussi archimédien ie $\forall a\in\mathbb{Z}$ et $b\in\mathbb{N}^*$ $\exists q\in\mathbb{Z}$ tq $a<mq$

• Valeur absolue sur $\mathbb{Z}$:

propriétés : $\forall z\in\mathbb{Z}$, $|z|\geqslant 0$ et $|z|=0 \Rightarrow z=0$

$$\forall z,z'\in\mathbb{Z},\ ||z|-|z'||\leqslant|z+z'|$$

• Division euclidienne dans $\mathbb{Z}$:

propriété : $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$, il existe un unique couple $(q,r)\in\mathbb{Z}\times\mathbb{N}$ tq $a=bq+r$, $0\leq r<|b|$

[$\{k\in\mathbb{Z} \mid bk\leq a\}$ est une partie non vide de $\mathbb{Z}$ et majorée donc admet un plus grand élément. (Existence)

Unicité par l'absurde]

2) Sous groupes additifs de $\mathbb{Z}$:

Thm : Les sous-groupes de $(\mathbb{Z},+)$ sont les ensembles $m\mathbb{Z}=\{mk \mid k\in\mathbb{Z}\}$, $m\in\mathbb{N}$

[Tout d'abord $m\mathbb{Z}$ est bien un sous groupe de $(\mathbb{Z},+)$ (facile à vérifier)

. Soit G un sous groupe de $\mathbb{Z}$

- Si $G=\{0\}$ alors $G=0.\mathbb{Z}$
- Si $G\neq\{0\}$, alors il existe $g\in G$, $g\neq 0$. G est un sous groupe donc $-g\in G$

$\Rightarrow G$ contient un élément strictement positif.

Soit $m=\min\{g\in G \mid g>0\}$ ← (partie non vide $\mathbb{N}$ ce qui prouve l'existence de m)

- $m\mathbb{Z}\subset G$ (car $m+m+\dots+m\in G$)
- Mq $G\subset m\mathbb{Z}$. Soit $a\in G$ et effectuons la division euclidienne de a par m alors $\exists(q,r)\in\mathbb{Z}\times\mathbb{N}$ tq $a=mq+r$ $0\leq r<m$

Comme $m\in G$, $mq\in G$ d'où $r=a-mq\in G$

or $r\in[\![0,m-1]\!]$ ie $0\leq r<m$ et $r\in G$ absurde $r=0$.

et $\underline{a=mq}$

]

Corollaire : Tout sous groupe de $(\mathbb{Z},+)$ est l'ensemble des multiples de son plus petit élément strictement positif.

3) Les idéaux de $\mathbb{Z}$

Thm : Les idéaux de $(\mathbb{Z},+,\times)$ sont de la forme $a\mathbb{Z}$.

[Même demonstration que sous groupe de la forme $n\mathbb{Z}$ ...]

Rq : Dans l'anneau $(\mathbb{Z},+,\cdot)$ les notions d'idéaux et de sous groupes sont confondues.

Corollaire : L'anneau $(\mathbb{Z},+,\times)$ est principal.

[un anneau est principal s'il est commutatif, unitaire, intègre, et si tous ses idéaux sont principaux. On a vu debut dans la partie I et idéaux principaux vient du thm précédent.]

II Arithmétique

1) Egalité de Bezout :

Prop : Soit $a\in\mathbb{Z}$, $b\in\mathbb{Z}$. Alors $a\mathbb{Z}+b\mathbb{Z}=\{x\in\mathbb{Z} \mid \exists (u,v)\in\mathbb{Z}\times\mathbb{Z} \text{ tq } x=au+bv\}$ est un sous-groupe de $\mathbb{Z}$.

Def : Soit $a\in\mathbb{Z}$, $b\in\mathbb{Z}$. On appelle pgcd de a et b l'unique entier $d\geq 0$ tq $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$, d est noté $a\wedge b$

Def : Soit $a\in\mathbb{Z}$ et $b\in\mathbb{Z}$. On dit que a divise b si $\exists k\in\mathbb{Z}$ tq $b=ak$, on note $a|b$.

Prop : $a|b \iff b\mathbb{Z}\subset a\mathbb{Z}$

Def : Soit $a,b\in\mathbb{Z}$. On dit que a et b sont premiers entre eux si $a\wedge b=1$

Prop : Soit $a,b\in\mathbb{Z}$. $a\wedge b=d \iff \begin{cases} d|a \text{ et } d|b,\ d\geq 0 \\ \forall d' \text{ tq } d'|a \text{ et } d'|b \text{ alors } d'|d. \end{cases}$

Prop : Soit $a,b\in\mathbb{Z}$. $a\wedge b=d$ ie $a=da'$ et $b=db'$ alors $a'\wedge b'=1$

Thm : $a\wedge b=1 \iff \exists u,v \in\mathbb{Z}^{*}$ tq $au+bv=1$ (Egalité de Bezout)

Thm : (Gauss) : $a,b\in\mathbb{Z}$ tq $a\wedge b=1$, $a|bc$ alors $a|c$

2) Résoudre dans $\mathbb{Z}$ des équations du type $ax+by=c$ (E) $a,b,c\in\mathbb{Z}$

Existence de solution

Thm : $ax+by=c$ admet une solution ssi $(a\wedge b)|c$.

[$\Leftarrow$ où $d=a\wedge b$ $a=da'$ $b=db'$ On suppose que $a\wedge b|c$ ie $c=dc'$ $c'\in\mathbb{Z}$

$a'\wedge b'=1$ ie $\exists u,v\in\mathbb{Z}$ tq $a'u+b'v=1$

ie $da'u+db'v=d$

ie $au+bv=d$

donc $(c'u,c'v)$ solution de (E) ie $ac'u+bc'v=dc'=c$

$\Rightarrow$ Réciproquement supposons qu'il existe x, y solutions de (E)

ie $ax+by=c$ $c\in a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}$ $c\in(a\wedge b)\mathbb{Z}$

$\Rightarrow (a\wedge b)|c$]

Recherche de solutions :

Donc ~~on suppose que~~ $d | c$, (il y a bien existence de solutions).

$c = dc'$

On est donc amené à résoudre $a'x + b'y = c'$ $(x,y) \in \mathbb{Z}^2$ et $a' \wedge b' = 1$

de plus $a' \wedge b' = 1$ donc (Bezout) $\exists u, v \in \mathbb{Z}$ tq $a'u + b'v = 1$

$$a'c'u + b'c'v = c'$$

donc $\begin{cases} a'x + b'y = c' \\ a'c'u + b'c'v = c' \end{cases} \Leftrightarrow a'(x - c'u) = b'(c'v - y)$

Donc on applique Gauss :

$a' | b'(c'v - y)$ or $a' \wedge b' = 1$

donc $a' | c'v - y$ ie $c'v - y = a'k$ $k \in \mathbb{Z}$.

ie $\boxed{y = c'v - a'k,\ k \in \mathbb{Z}}$

$a'(x - c'u) = b'(c'v - y)$

ie $a'(x - c'u) = b'(\cancel{c'v} - \cancel{c'v} + a'k)$ $k \in \mathbb{Z}$

$\cancel{a'}(x - c'u) = b'\cancel{a'}k$ | $k \in \mathbb{Z}$

$\boxed{\text{ie } x = c'u + b'k}$

$S = \{ x = c'u + b'k \text{ et } y = c'v - a'k \mid k \in \mathbb{Z} \}$

Exposé 13 : Démonstration :

L'anneau $\mathbb{Z}$, sous groupes additifs de $\mathbb{Z}$. Les idéaux de $\mathbb{Z}$ st principaux. Egalité de Bezout. Résolution dans $\mathbb{Z}$ d'une équation de la forme $ax+by=c$.

Thm : Soit $a, b \in \mathbb{N}^*$, $a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}^2$ tq $au+bv=1$

[* On suppose que $a \wedge b = 1$ c'est dire que $a\mathbb{Z}+b\mathbb{Z} = 1\mathbb{Z}$

$1 \in \mathbb{Z}$ donc $\exists u, v \in \mathbb{Z}$ tq $au+bv=1$

* On suppose qu'il existe $u, v \in \mathbb{Z}^2$ tq $au+bv=1$

On raisonne par l'absurde et on suppose que $a \wedge b = d$ avec $d \in \mathbb{N}$, $d > 1$

$a \wedge b = d$ ie $a = da'$ avec $a' \wedge b' = 1$
$b = db'$

ie $au+bv=1$

ie $da'u+db'v=1$

$d(a'u+b'v)=1$ ie $d \mid 1$ ie $d = \pm 1$ Jc $a \wedge b = 1$]

Thm de Gauss :

$a \wedge b = 1$ et $a \mid bc \Rightarrow a \mid c$

[$a \wedge b = 1 \Rightarrow$ Thm de Bezout, $\exists u, v \in \mathbb{Z}$ tq $au+bv=1$

$acu+bcv=c$

or $a \mid bc$ ie $bc = ak$ $k \in \mathbb{Z}$

$acu+akv=c$

$a(cu+kv)=c$ ie $a \mid c$

II Arithmétique Prop 3

[Le fait que $a\mathbb{Z}+b\mathbb{Z}$ est un sous groupe est trivial]

[$\Rightarrow$ donc $\exists d \in \mathbb{Z}$ tq $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$]

[$a \mid b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$, $a \mid b$ ie $b = ak$, $k \in \mathbb{Z}$ $b\mathbb{Z} = ak\mathbb{Z} \subset a\mathbb{Z}$

si $b\mathbb{Z} \subset a\mathbb{Z}$

ie $b \subset a\mathbb{Z}$ ie $a \mid b$

ie $\exists q \in \mathbb{Z}$ tq $b = aq$]

[$a \wedge b = d \Leftrightarrow d \mid a$ et $d \mid b$. vient de $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$ ie $a\mathbb{Z} \subset d\mathbb{Z}$ ie $d \mid a$

$b\mathbb{Z} \subset d\mathbb{Z}$ ie $d \mid b$

soit $d' \in \mathbb{Z}$ tq $d' \mid a$ et $d' \mid b$ ie $d \in d\mathbb{Z}$, ie $\exists u, v \in \mathbb{Z}$ tq

$d = au+bv$

$d = d'(da'+db')$ ie $d' \mid d$]