Structures algébriques, arithmétique

Monoïde $(M, \cdot)$, $\cdot$ associative, admet un neutre

▶ Préciser les lois utilisées : S_n groupe pour $\circ$, ...
Caractérisation des sous-groupes : le sur-groupe doit utiliser la même loi

Ex Démonstrations classiques :
- intégrité d'un corps
- $a \cdot 0_E = 0_E$ dans un anneau
- détermination des sous-groupes de $\mathbb{R}$ pour $+$
- f morphisme de groupes, $[f \text{ injective}] \iff [\ker f = \{e\}]$

Théorème de Lagrange

| $(G, \cdot)$ groupe de cardinal fini n, H sous-groupe de G.
| Alors H de cardinal fini p, et p divise n.

↳ $H \subset G$, d'où H de cardinal fini p. Montrons que p divise n.
Partitionnons G en formant des classes d'équivalence de même cardinal p. Soit $\mathcal{R}$ la relation telle que pour $(x,y) \in G$:
$[x \mathcal{R} y] \iff [x y^{-1} \in H]$. Montrons que :

1. $\mathcal{R}$ est une relation d'équivalence
2. $H = Cl(e)$ est une classe
3. Toute classe $Cl(a)$ avec $a \notin H$ est en bijection avec H.
   Montrer que $\varphi : Cl(a) \to Cl(e)$, $x \mapsto a x^{-1}$ définie, injective, surjective.

Sous-groupe engendré $Gr(A)$ par une partie A

| plus petit sous-groupe contenant A.

▶ A est génératrice de $Gr(A)$

▶ $\langle a \rangle := Gr(\{a\})$ est commutatif

Ordre de a s'il existe, $\# \langle a \rangle$

Groupe monogène G, s'il existe $a \in G$ tel que $G = \langle a \rangle$

Groupe cyclique / monogène d'ordre n

| groupe monogène de cardinal fini n.

▶ Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{U}_n$

Résultats classiques de $\mathbb{Z}/n\mathbb{Z}$

| [intègre] $\Longleftrightarrow$ $[n \in \mathcal{P}]$

| $[p \wedge n = 1]$ $\Longleftrightarrow$ [$\bar{p}$ générateur] $\Longleftrightarrow$ [$\bar{p}$ inversible]

| [corps] $\Longleftrightarrow$ $[n \in \mathcal{P}]$

| $G = \langle a \rangle$ ou, bien : • infini : isomorphe à $\mathbb{Z}$
• fini d'ordre n : isomorphe à $\mathbb{Z}/n\mathbb{Z}$
[a^p générateur] $\Longleftrightarrow$ $[p \wedge n = 1]$
tout sous groupe est cyclique

↳ L'image réciproque d'un sous groupe (éventuellement G) par $f : k \in \mathbb{Z} \to a^k$ est sous-groupe de $\mathbb{Z}$, donc est égale à $q\mathbb{Z}$ avec $q \in \mathbb{N}$.

| $p \wedge n = 1$: $\mathbb{Z}/np\mathbb{Z}$ isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

↳ Utiliser $f : \bar{x} \mapsto (\dot{x}, \tilde{x})$ où $\bar{x}$ (resp. $\dot{x}, \tilde{x}$) classe de x dans $\mathbb{Z}/np\mathbb{Z}$ (resp $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$). Définition non triviale : montrer que deux représentants donne la même image.

Théorème des restes chinois

| $p \wedge n = 1$, il existe c tel que $\begin{cases} x \equiv a \ [n] \\ x \equiv b \ [p] \end{cases}$ a pour solution $c + np\mathbb{Z}$.

Indicatrice d'Euler

$\varphi : n \in \mathbb{N}^* \mapsto \begin{cases} \# \{p \in [\![1;n]\!],\ p \wedge n = 1\} & \text{si } n \geq 2 \\ 1 & \text{si } n = 1. \end{cases}$

| $\varphi(n) = \# (\mathbb{Z}/n\mathbb{Z})^*$ pour $n \geq 2$

| $\varphi(np) = \varphi(n)\varphi(p)$ pour $n \wedge p = 1$

↳ isomorphisme entre $(\mathbb{Z}/np\mathbb{Z})^*$ et $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$, s'appuyer sur f.

| $\varphi(p) = p - 1$ pour $p \in \mathcal{P}$

| $\varphi(p^q) = p^{q-1}(p-1)$ pour $p \in \mathcal{P}$, $q \in \mathbb{N}^*$

| $\varphi\left(\prod p_i^{\alpha_i}\right) = \prod_{i=1}^{n} p_i^{\alpha_i - 1}(p_i - 1)$

Théorème d'Euler

$k \wedge n = 1$, $\quad k^{\varphi(n)} \equiv 1 \ [n]$

↳ $G = (\mathbb{Z}/n\mathbb{Z})^*$ fini, de cardinal $\varphi(n)$. Soit p l'ordre de k dans G ($k \in G$ car $k \wedge n = 1$). Alors $p \mid \varphi(n)$ (Lagrange), donc $\bar{k}^{\varphi(n)} = (\bar{k}^p)^s = \bar{1}^s = \bar{1}$.

Petit théorème de Fermat

$p \in \mathcal{P}$, $k \wedge p = 1$: $\quad k^{p-1} \equiv 1 \ [p]$

▶ Extension : $p \in \mathcal{P}$, $\quad k^p \equiv k \ [p]$

Groupe des inversibles de G G^*

Soit $(A,+,\times)$ un anneau <u>intègre</u> donc commutatif.

Divisibilité dans A $[a \mid b] \Longleftrightarrow [\exists c \in A,\ b = a \times c]$

Éléments a et b associés $[a \mid b \text{ et } b \mid a] \Longleftrightarrow [\exists c \in A^*,\ b = a \times c]$

↳ $\Leftarrow$: Ok. $\Rightarrow$: $b = ac = bc'c$ donc $b(1_A - cc') = 0_A$ donc $cc' = 1_A$: $c \in A^*$

Idéal I de A
- I sous-groupe de A pour +
- I stable pour $\times$ par A

Ex • $\mathbb{Z}$: • $\mathbb{Z}^* = \{-1;1\}$
- $[a$ et b associés$] \Longleftrightarrow [a = \pm b]$
- sous groupes de $\mathbb{Z}$: $p\mathbb{Z}$, $p \in \mathbb{N}$ (idéaux)

• $\mathbb{K}[X]$, • $\mathbb{K}[X]^* = \mathbb{K}_0[X] \setminus \{0\}$
- $[P$ et Q associés$] \Longleftrightarrow [\exists \lambda \in \mathbb{K}^*,\ P = \lambda Q]$
- sous-groupes de $\mathbb{K}[X]$: $P_0\,\mathbb{K}[X]$, $P_0 \in \mathbb{K}[X]$ (idéaux)

| $f : A \to B$ morphisme de groupes : • $\mathrm{Ker} f$ idéal de A
• $f(J)$ idéal de $\mathrm{Im} f$ si J idéal

Idéal principal aA

▶ La somme d'idéaux principaux est idéale

| $[aA = bA] \Longleftrightarrow [a$ et b associés$]$

Anneau principal tout idéal de A est principal

Ex $\mathbb{Z}$, $\mathbb{K}[X]$

PGCD de $a_0, \dots a_n \in A$ principal d tel que $dA = \sum_{i=0}^{n} a_i A$

▶ Existence : $\sum_{i=0}^{n} a_i A$ est idéal, donc idéal principal car A principal.
Non unicité : $[d'$ PGCD$] \Longleftrightarrow [dA = d'A] \Longleftrightarrow [d'$ et d associés$]$.
On peut fixer un critère pour obtenir l'unicité :
- $\mathbb{Z}$: positif
- $\mathbb{K}[X]$: unitaire

| $[d$ PGCD$] \Longleftrightarrow \begin{cases} \forall i \in [\![0;n]\!],\ d \mid a_i \\ \forall \delta \in A,\ [\forall i \in [\![0,n]\!],\ \delta \mid a_i] \Rightarrow [\delta \mid d] \end{cases}$

Théorème d'Euclide $a \wedge b = (a + bk) \wedge b$ $k \in \mathbb{Z}$

▶ Algorithme d'Euclide

Éléments premiers entre eux 1_A PGCD

Résultats classiques

- $[a\wedge b = 1_A] \iff [\exists u,v \in A,\ ua+vb = 1_A]$ (égalité de Bézout)
- $a = da',\ b = db' \neq 0_A$: $[d = a\wedge b] \iff [a'\wedge b' = 1_A]$
- $[a\wedge b = 1_A,\ a\wedge c = 1_A] \Rightarrow [a\wedge bc = 1_A]$
- $[a\wedge b = 1_A,\ a \mid bc] \Rightarrow [a \mid c]$ (thm. de Gauss)
- $[p \in \mathcal{P},\ p \mid \prod x_i] \Rightarrow [\exists i_0,\ p \mid x_{i_0}]$
- $[a\wedge b = 1_A,\ a\mid c,\ b \mid c] \Rightarrow [ab \mid c]$
- $[p \in \mathcal{P}] \Rightarrow [p \mid k$ ou $p\wedge k = 1_A]$

▶ A connaître et à pouvoir démontrer, avec l'égalité de Bézout et la caractérisation des PGCD.

PPCM de $a_0, \dots, a_n \in A$ principal : m tel que $mA = \bigcap_{i=0}^{n} a_i A$

▶ Existence et non unicité comme pour le PGCD

$$[m \text{ PPCM}] \iff \begin{cases} \forall i \in [\![0,n]\!],\ a_i \mid m \\ \forall s \in A,\ [\forall i \in [\![0,n]\!],\ a_i \mid s] \Rightarrow [m \mid s] \end{cases}$$

ab et $(a\wedge b)(a\vee b)$ associés

↳ Soit d un PGCD de a et b, a', b' tels que $a = da'$, $b = db'$, m un PPCM de a et b, q, q' tels que $m = qa = q'b$.

$da'b' = ab' = a'b$ multiple de a et b donc de m, donc il existe $v \in A$ tel que $mv = da'b'$

$m = qda' = q'db'$, donc $b' \mid qa'$, donc $b' \mid q$ (Gauss), donc il existe $v' \in A$ tel que $q = v'b'$, donc $m = qa = v'b'da'$

Donc $da'b' = mv = v'v\,da'b'$, d'où $vv' = 1_A$.