Groupes

I Généralités

On note $(G,.)$ un groupe, non nécessairement commutatif
$(G,+)$ sera toujours commutatif

$a.x = e$

$b.x = b$

$x = b$

$x.a = e$

Ex Soit $(G,.)$ un monoïde tq tout élément possède un symétrique à gauche
Mq G est un groupe

S/ Soit $a \in G$, Il existe $a' \in G$ $a'*a = e$ puis $a'' \in G$ tq $a''*a' = e$, On regarde $x = a''*a'*a \longrightarrow x = a'$

donc $a*a' = a'*a = e$

Def : (Sous-groupe) C'est une partie H de G, stable par $.$ telle que $(H,.)$ est un ~~sous~~ groupe

Prop : $e_H = e_G$ et $\forall x \in H$ le symétrique dans H est le même que le symétrique de x dans G

D/ i) Soit $a \in G$ tq $a*a = a$, il vient $(a*a)*a^{-1} = a*a^{-1} = e_G$

donc $a = e_G$

Comme $e_H * e_H = e_H$, il vient $e_H = e_G$

ii) $x*x' = e_H$, $x*x'' = e_G$ } il vient avec i) $x*x' = x*x''$ | $x*(x*x') = x*x*(x*x')$ $\longrightarrow x' = x''$

Def équivalente : $H \neq \emptyset$ et $\forall x,y \in H^2 : x*y^{-1} \in H$

Ex Soit H une partie finie non vide de G, stable par $*$.
Montrer que H est un sous groupe de G.

S/ (I) Soit $a \in H$, on introduit $\varphi_a \left| \begin{array}{ccc} H & \longrightarrow & H \\ x & \longmapsto & ax \end{array} \right.$ idée essentielle ♥

φ_a est correctement définie sur H est stable et injective car G est un groupe. Donc φ_a est bijective

Def: $\exists e' \in H$ tq $ae' = a$. Soit $b \in H$, $\varphi_b \left| \begin{array}{ccc} H & \longrightarrow & H \\ x & \longmapsto & xa \end{array} \right.$

étant bijective $\exists c \in H$, $b = ca$, d'où $be' = (ca)e' = c(ae')$
$= ca = b$

e' est un neutre à droite, il vient $ee' = e'$ donc $e' = e$

Enfin $\exists b \in H$ $\varphi_b^{-1}(b) = e$, i.e. $ab = e$, $b = a^{-1} \in H$

Translations dans un groupe $(G, .)$ est un groupe
Lorsque $a \in G$, on note $\gamma_a \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & ax \end{array} \right.$ $\delta_a \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & xa \end{array} \right.$

⚠ γ_a morphisme de groupe $\Leftrightarrow a = e$ $[\gamma_a(e) = e$ nécessaire$]$

Puissances dans un groupe
On définit pour $n \in \mathbb{N}$ et $x \in G$ $\left| \begin{array}{l} x^0 = e \\ \forall n \in \mathbb{N}, \; x^{n+1} = x * x^n \end{array} \right.$

Enfin, si $n < 0$, $x^n = (x^{-1})^{|n|}$. On vérifie $\forall x \in G \; \forall (m,n) \in \mathbb{Z}^2 \; x^{m+n} = x^m * x^n$

⚠ Si la loi est additive, on note nx au lieu de x^n

Morphisme de groupes: $f \in \mathrm{Hom}((G,*),(G,T)) \Leftrightarrow \forall (x,y) \in G^2 \; f(x*y) = f(x) \, T \, f(y)$
⚠ $* = +$, $T = \cdot$ ——— $f(x+y) = f(x) f(y)$

Ex ① Soit $a \in G$ $j_a \left(\begin{array}{c} (\mathbb{Z},+) \to (G,\cdot) \\ n \mapsto a^n \end{array} \right)$ est un morph de groupes

② Soit $a \in G$ $\sigma_a \left(\begin{array}{c} G \to G \\ x \mapsto axa^{-1} \end{array} \right)$ est un morphisme bijectif

En effet $\forall (x,y) \in G^2$ $axya^{-1} = axa^{-1}aya^{-1} = \sigma_a(x)\sigma_a(y)$

de plus $\forall (a,b) \in G^2$ $\sigma_a \circ \sigma_b = \sigma_{ab}$ $\left((ab)^{-1} = b^{-1}a^{-1} \right)$

et donc $\sigma_a \circ \sigma_{a^{-1}} = \sigma_{a^{-1}} \circ \sigma_a = \sigma_e = Id$

Conjugaison x et y sont conjugués de $G \Leftrightarrow \exists a \in G$, $y = axa^{-1}$ $= \sigma_a(x)$

Cette relation est d'équivalence (exc. pers) : les classes de conjugaison réalise une partition de G

Prop : Soit $f \in \mathrm{Hom}(G,G')$

① $f(e) = e'$: en effet $f(e) = f(e*e) = f(e)Tf(e)$ $f(e)^{-1} = e'$

② Si H est un ssg de G, $f(H)$ est un ssg de G'.
En particulier, $\mathrm{Im}(f) = f(G)$ est un ssg de G', $f(K)$ est un ssg

③ Si K est un ssg de G', $f^{-1}(K)$ est un ssg de G. En particulier $\mathrm{Ker} f = f^{-1}(\{e'\})$ est un ssg de G

④ f est injective $\Leftrightarrow \mathrm{Ker} f = \{e\} \Leftrightarrow \mathrm{Ker} f \subset \{e\}$

($\Rightarrow$) $f(e) = e$ donc $x \in \mathrm{Ker} f$, $f(x) = f(e)$ et par suite $x = e$

($\Leftarrow$) Soit $(x,y) \in G^2$, $f(x) = f(y) \Rightarrow f(x)f(y)^{-1} = e'$ $\Rightarrow xy^{-1} = e$
$\Rightarrow f(xy^{-1}) = e'$ $\Rightarrow x = y$ ✓
Hom

Prop : ① Les homomorphismes se composent
② Les isomorphismes de G forment un groupe
③ Les automorphismes de G forment un groupe

Ex : Soit G un groupe $\left(\begin{array}{c} G \to \mathrm{Aut}(G) \\ a \mapsto \sigma_a \end{array} \right)$ est un morphisme de groupe

$\ker \varphi = Z(G) = \{ a \in G \mid \forall x \in G \; ax = xa \}$

En effet : $a \in \ker\varphi \Leftrightarrow \sigma_a = Id \Leftrightarrow \forall x \in G \; axa^{-1} = x$
$ax = xa$

Sous-groupes distingués (invariants)

Déf : Soit H un sous-groupe de G. On dit que H est distingué lorsque $\forall a \in G \; aHa^{-1} \subset H$
($\sigma_a(H)$)

Dans ce cas : $\forall a \in G \; aHa^{-1} = H$
$aH = Ha$

en effet $aHa^{-1} \subset H$; donc $a^{-1}(aHa^{-1})a \subset a^{-1}Ha \subset H$

puis $\sigma_a(H) = Ha$ mais $\sigma_a(aHa^{-1}) = aH$ ✓
égal

Ex : $\{e\}$, G, $\ker f$ où $f \in \mathrm{Hom}(G,G)$ → Produit

Déf : G est dit simple s'il ne possède pas d'autre s.g distingué que G et $\{e\}$

Ex $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$

Produit de deux groupes

On munit $G_1 \times G_2$ de la loi produit $(x_1, x_2)\cdot(y_1, y_2) = (x_1 y_1, x_2 y_2)$
Les projections $pr_i : G_1 \times G_2 \to G_i$ sont des morphismes
Ob : $G_1 \times \{e\}$ est un s.g distingué de $G_1 \times G_2$
$\{e\} \times G_2$ de $G_1 \times G_2$

X Ex : Soient H et K deux s.g d'un groupe G
1) Si $HK = KH$, montrer que HK est un s.g de G
2) Si H est distingué, HK est un s.g de G
3) Si $H \cap K = \{e\}$, $f : \begin{cases} H \times K \to HK \\ (h,k) \to hk \end{cases}$ est bijective (→ isomorphisme)

4) Si $H \cap K = \{e\}$ et si H et K sont distingués alors f est un isomorphisme.

S/ 1) Soit $x \in HK$ s'écrit $x = hk$ $(h,k) \in H \times K$

$y \in HK$ ——— $y = h'k'$

$xy = hkh'k'$

$\in KH = HK \to h''k''$

$xy = h h'' k'' k' \in HK$

2) $hkh'k' = h(khk^{-1})kk' \in HK$

$h'' \in H$ by n

3) $f(h,k) = f(h',k') \Rightarrow hk = h'k' \to h^{-1}h = kk'^{-1} \in H \cap K$

$\Rightarrow h^{-1}h = e = k'k^{-1} \Rightarrow (h,k) = (h',k')$

4) On va montrer $\forall (h,k) \in H \times K$, $hk = kh$

On examine la commutation $[h,k] = hkh^{-1}k^{-1}$

$[h,k] = e \iff hk = kh$

$[h,k] = (hkh^{-1})k^{-1} = h(khk^{-1})$

$\in H$ distingué

$\hookrightarrow [h,k] \in H \cap K = \{e\}$

donc $hk = kh$ | f est bijective avec 3) f est un morphisme de groupes.

120

II Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$, $n \geq 2$, on note $\sim_{n\mathbb{Z}}$ la relation définie sur $\mathbb{Z}^2$ par

$x \sim y \iff n/y-x \iff y-x \in n\mathbb{Z}$

Prop 1) $\sim$ est une relation d'équivalence

2) On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes selon $\sim$, une telle classe s'écrit $\overline{x} = x + n\mathbb{Z} = \{x + \ell n / \ell \in \mathbb{Z}\}$

Def : Soient X et Y deux classes $\in \mathbb{Z}/n\mathbb{Z}$, $x \in X$, $y \in Y$

alors $\overline{x+y}$ ne dépend que de X et de Y (et donc ne dépend pas des choix de représentants x, y)

D/ Soit $x' \in X$, $y' \in Y$ il vient $\begin{matrix} x - x' \in n\mathbb{Z} \\ y - y' \in n\mathbb{Z} \end{matrix}$ $\Big)$ $x+y - (x'+y') \in n\mathbb{Z}$ $\quad x+y = x'+y'$

Th $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe commutatif $\left(\begin{matrix} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ x \mapsto \overline{x} \end{matrix}\right)$

est pour morphisme $n\mathbb{Z}$ ~~$\mathbb{Z}$~~

2) $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$ $\mathbb{Z}$ infini $\to$

3) Si $n \in \mathbb{Z}$ $\left(\begin{matrix} \{n, \dots, n+n-1\} \to \mathbb{Z}/n\mathbb{Z} \\ k \mapsto \overline{k} \end{matrix}\right)$

D/ 1) $\overline{0} + \overline{x} = \overline{0+x} = \overline{x}$ et $\overline{x} + \overline{-x} = \overline{0}$

Noyau $\{x \in \mathbb{Z} / \overline{x} = \overline{0}\} = n\mathbb{Z}$

2) Soit $n \in \mathbb{Z}$ $x = nq + r$, $\overline{x} = \overline{nq+r} = \overline{n}\,\overline{q} + \overline{r} = \overline{0} + \overline{r} = \overline{r}$

Si $0 \leq r < s \leq n-1$, n ne divise pas $s-r$ et donc $\overline{r} \neq \overline{s}$

3) j est injective, Si $0 < r < s \leq n-1$, $\overline{m+r} \neq \overline{m+s}$ $\left(\text{car } \overline{s-r} \neq \overline{0}\right)$

Prop $\varphi\left(\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & U_n \\ \overline{k} & \longrightarrow & e^{\frac{2ik\pi}{n}} \end{array}\right)$ est correctement défini c'est un isomorphisme

D/ Si $\overline{k} = \overline{\ell}$, il vient $\ell = k + qn$, déjà $e^{\frac{2i\pi\ell}{n}} = e^{2i\pi q} e^{\frac{2ik\pi}{n}}$

de plus pour $(k,\ell) \in \mathbb{Z}^2$ $\varphi(k+\ell) = \varphi(k)\varphi(\ell)$, c'est surjective donc bijective par cardinalité

II Ordre d'un élément:

Soit $a \in G$: on note $j\left(\begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (G,\cdot) \\ m & \longmapsto & a^m \end{array}\right)$ c'est un morphisme de groupes surjectif sur $\{a^m\}_{m\in\mathbb{Z}}$, SG de G

On regarde $\ker j$

1er cas: $\ker j = \{0\}$, j est un isomorphisme, $\forall m, m'$ $a^m \neq a^{m'}$ $|\langle a \rangle| = |\mathbb{Z}| = +\infty$

2e cas: $\ker j \neq \{0\}$ on sait alors $\exists m \in \mathbb{N}^*$, $\ker j = n\mathbb{Z}$

on note $\omega(a) = n$

Prop: $(\ker j \neq \{0\}) \Rightarrow n = \min\{k \in \mathbb{N}^*, a^k = e\}$

1) $\forall m \in \mathbb{Z}$ $\exists! k \in \{0,\dots,n-1\}$ $a^m = a^k$

D/ $m = qn + k$, $k \in \{0,\dots,n-1\}$ $a^m = a^{qn+k} = a^k$ d'où l'existence

Unicité si $0 \leq k < \ell \leq n-1$, $a^k = a^\ell \Rightarrow a^{\ell-k} = e$

$\Rightarrow n \mid \ell - k$ absurde

3) (I) Soit $k \in \mathbb{Z}$, alors $\omega(a^k) = \frac{n}{n \wedge k}$

* $(a^k)^{\frac{n}{n\wedge k}} \Rightarrow a^{\frac{kn}{n\wedge k}} = a^{dn}$ où $d = \frac{k}{n\wedge k} = p$

** Soit $m \in \mathbb{N}$ $(a^k)^m = e \Rightarrow n \mid km$ | $k = k' k\wedge m$, $n = n' k\wedge m$, $k' \wedge n' = 1$

$\Rightarrow n \mid k'nm$ avec $(n \mid k'n) = 1$

$\Rightarrow n \mid m$ et $\frac{n}{n\wedge k} \mid m$.

donc

Conséquence si $q \mid n$, $\omega(a^q) = \frac{n}{q}$

Exemple: $a = \exp\left(\frac{2ik\pi}{n}\right) = \exp\left(\frac{2i\pi}{n}\right)^k$, $\omega(a) = \frac{n}{n\wedge k}$

4) Actions de Morphismes: $f \in \mathrm{Hom}(G, G')$

i) $\omega(f(a)) \mid \omega(a)$

ii) Si f est un isomorphisme $\omega(f(a)) = \omega(a)$

iii) Si a et b sont conjugués $\omega(a) = \omega(b)$

D/ i) $n = \omega(a)$ $f(a)^n = f(a^n) = f(e)$, $f(a)^n = e'$ par déf $\omega(f(a)) \mid n$

ii) avec f et f^{-1} iii) $b = \sigma_c(a)$, σ_c automorphisme, on applique ii)

Ex (Min6) $m \wedge n = 1$: trouver tous les morphismes de groupe $(\mathbb{Z}/m\mathbb{Z}^*, \cdot) \to (\mathbb{Z}/n\mathbb{Z}^*, \cdot)$

S/ On regarde $\omega(\overline{1}_m)$ et $\omega(f(\overline{1}_m))$

$k \cdot \overline{1}_m = \overline{0}_m \Leftrightarrow \overline{k}_m = \overline{0}_m \Leftrightarrow m \mid k$

$\omega(\overline{1}_m) = m$

Soit $a = f(\bar{1}_m)$ il vient $\omega(a) | m$

et aussi avec $a = \bar{k}$ $m \cdot \bar{k} = \bar{k} + \dots + \bar{k}$

donc $\omega(a) | m$, $\omega(a) | m \wedge m = 1$

donc $a = \bar{0}$, f est nul car $f(\bar{e}_m) = f(\ell \cdot \bar{1}_m) = \ell f(\bar{1}_m) = \bar{0}_m$

Ex Soit $(a,b) \in G^2$ avec a et b d'ordres finis m et n

(i) ab d'ordre fini ? Indic : S_a et S_b symétries

(ii) On suppose $ab = ba$ et $\omega(a) \wedge \omega(b) = 1$ Montrer que $\omega(ab) = mn$

(i) $S_{\Delta'} \circ S_{\Delta} = r_{2(\Delta', \Delta)}$ (ordre 2 ordre 2) On choisit Δ', Δ de sorte que $2(\Delta', \Delta) = 2\pi\theta$ avec $\theta \in \mathbb{R} \setminus \mathbb{Q}$

(ii) $[a,b] = e$ (déf) $\Leftrightarrow abab^{-1} = e$, alors $\forall \ell \in \mathbb{Z}$ $(ab)^\ell = a^\ell b^\ell$

$(ab)^\ell = e \Rightarrow a^\ell b^\ell = e \Rightarrow a^{m\ell} b^{m\ell} = e \Rightarrow b^{m\ell} = e$

($m = \omega(a) | \ell$) $\Rightarrow$ ($m = \omega(b) | m\ell$)

On a $n \wedge m = 1$ donc $n | \ell$, de même $m | \ell$ et puis donc $mn | \ell$

Réciproquement $(ab)^{mn} = e$, donc $\omega(ab) = mn$

(c) On suppose $[a,b] = e$, $\omega(a) = m \in \mathbb{N}^*$, $\omega(b) = n \in \mathbb{N}^*$

construire $c \in G$ tq $\omega(c) = ppcm(a,b)$

5/ Décomp en fact premiers

$m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ p_i 2 à 2 $\neq$ $\alpha_i \geq 0$ | $mVn = p_1^{\max(\alpha_1,\beta_1)} \cdots p_n^{\max(\alpha_n,\beta_n)}$

$n = p_1^{\beta_1} \cdots p_n^{\beta_n}$

On suppose que est $\max(\alpha_1,\beta_1) = \alpha_1$, ..., $\max(\alpha_k,\beta_k) = \alpha_k$

$\max(\alpha_{k+1},\beta_{k+1}) = \beta_{k+1}$ ... $\max(\alpha_n,\beta_n) = \beta_n$

On pose $a' = a p_{k+1}^{\alpha_{k+1}} \cdots p_n^{\alpha_n}$, $b' = b p_1^{\beta_1} \cdots p_k^{\beta_k}$

$\omega(b') = p_1^{\beta_{k+1}} \cdots p_n^{\beta_n} = \frac{m}{d}$

$\omega(a') = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \frac{m}{\delta}$

$\omega(a') \wedge \omega(b') = 1$ il vient $\omega(a'b') = \frac{mn}{d\delta} = mVn$

Conséquence: Si $a_1, \dots, a_s$ commutent et sont d'ordre fini, il existe $c \in \langle a_1, \dots, a_s \rangle$ tq $\omega(c) = \prod_{1 \leq i \leq n} \omega(a_i)$

Th (Sylow) Soit G un groupe commutatif fini - Soit $a \in G$
Alors a est d'ordre fini et $\omega(a) \mid |G|$

D/ $\gamma_i \left(\begin{array}{c} G \longrightarrow G \\ x \longrightarrow ax \end{array} \right)$ est bijective ; donc, G étant commutatif
on peut écrire $\prod_{x \in G} x = \prod_{x \in G} ax = a^{|G|} \prod_{x \in G} x$, donc $\omega(a) \mid |G|$

⚠ $\prod_{x \in G} x = e$ en simplifiant avec le raisonnement FAUX
Si $x^2 = e$, x est compté une fois

IV Groupes cycliques:

Déf: Soit G un groupe. On dit que G est monogène s'il existe a tq $G = \{a^k\}_{k \in \mathbb{Z}}$

me gusta las listas

Deux cas : i) a est d'ordre infini, $\varphi \left| \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & a^k \end{array} \right.$ est un isomorphisme

ii) a est d'ordre fini, $G = \{e, a, \dots, a^{n-1}\}$, $n = \omega(a) = |G|$

RM : Si a est d'ordre fini dans un groupe G, $n = \omega(a)$
$\langle a \rangle = \{e, \dots, a^{n-1}\}$ est cyclique

Th G est cyclique de cardinal $n \iff G$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

D/ $\Leftarrow$ $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$

⚠ Rappel : dans $(G, +)$ la puissance k-ième se note $k.a$
$(\mathbb{Z}/n\mathbb{Z}, +) = \langle \bar{1} \rangle$; si φ un isom $(\mathbb{Z}/n\mathbb{Z}, +) \to G$, $a = \varphi(\bar{1})$
convient.

$\Rightarrow$ On suppose $G = \langle a \rangle$, $n = \omega(a)$; Soit $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$
posons $\varphi(\bar{k}) = a^k$ a^k ne dépend pas du choix du représentant de la classe : si $\bar{k'} = \bar{k}$, il vient $k' = k + nq$, $a^{k'} = a^{k+nq}$

$= a^k (a^n)^q = a^k$ ($a^n = e$)

c'est clair que φ est un morphisme bijectif

Exo Soit $G = \langle a \rangle$ un groupe cyclique. Mq

Soit H un sg de G. Mq $\exists d/n$: $H = \langle a^{n(a)} \rangle$; H est d'ordre d

D/ Soit $\varphi \left| \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & a^k \end{array} \right.$ est surjective (épimorphisme), $\ker \varphi = n\mathbb{Z}$

On a donc $H = \varphi(\varphi^{-1}(H))$ où $\varphi^{-1}(H)$ est un sg de $\mathbb{Z}$

~~avec $n\mathbb{Z}$~~ ainsi $\varphi^{-1}(H) = d\mathbb{Z}$, avec $n\mathbb{Z} \subset d\mathbb{Z}$

donc $d|n$

$H = \{a^k / k \in \mathbb{Z}\} = \langle a^{kd'} / k \in \mathbb{Z}\rangle = \langle a^{nd} \rangle$ où $d = \frac{n}{d'}$

Flèche help for some moments après

RM. D_n = les diviseurs de n $\quad R = \{d \in D_n / d < \sqrt{n}\}$

$Q = \{d \in D_n / d > \sqrt{n}\}$ $\quad \mu \left(\begin{array}{ccc} P & \to & Q \\ d & \to & \frac{n}{d} \end{array} \right)$ est une bijection donc $|D_n| \leq 2\sqrt{n}+1$

Ex générateurs : Si G est cyclique $= \langle a \rangle$ de cardinal n

$g(G) = \{b \in G / \langle b \rangle = G\} = \{a^k / k \wedge n = 1\}$ et de cardinal $\varphi(n)$

S/ Soit $b \in G$, si $b = a^k$, $\omega(b) = \frac{n}{k \wedge n}$ (HP), donc $\langle b \rangle = G$

$\Leftrightarrow k \wedge n = 1$, avec $k \in \{1, \dots, n-1\}$ on a le 2ème résultat

particulier très important

Rem **CPI:** $G = U_n$ ($\mathbb{U}_n$) avec $k \wedge n = 1$, s'appelle une racine primitive n-ième.

Ex : Soit $n \in \mathbb{N}^*$: $\sum_{\substack{d|n \\ d \geq 1}} \varphi(d) = n$

S/ On note $g_d = \{b \in G / \omega(b) = d\}$ $\quad d | n = \langle G \rangle$ (Lagrange)

On sait que, pour tout $d \in D_n$ il existe un sg de G, de cardinal

d. $H_d = \langle a^{n/d} \rangle$, $b \in g_d \Leftrightarrow |\langle b \rangle| = d \Leftrightarrow \langle b \rangle = H_d$

$\Leftrightarrow b \in g(H_d)$

Ainsi $|g_d| = \varphi(d)$

$G = \bigsqcup_{\text{disj}} g_d$ donc $|G| = \sum_{d|n} |g_d| = \sum_{d|n} \varphi(d)$

12

Ex Produit de deux groupes cycliques

On suppose $G_1 = \langle a_1 \rangle$ et $G_2 = \langle a_2 \rangle$ sont cycliques

CNS pour que $G_1 \times G_2$ le soit

S/IFEIS que $|G_1| \wedge |G_2| = 1$

CS $a = (a_1, a_2)$: $a^m = e = (e_1, e_2) \iff a_1^m = e_1$ et $a_2^m = e_2$

$\omega(a_1) \mid m$ et $\omega(a_2) \mid m$

$\iff$ ~~$m \mid \omega(a_1)$~~ et ~~$m \mid \omega(a_2)$~~

$\iff$ ~~$m \mid \omega(a_1) \omega(a_2)$~~

lyon $\omega(a_1) \mid \omega(a_2) \mid m$

$\omega(a_1, a_2) = \omega(a_1) \vee \omega(a_2) = |G_1 \times G_2| \ni K$

CN On suppose $d = m_1 \wedge m_2 > 1$. Soit $a = (a_1^k, a_2^\ell) \in G_1 \times G_2$

$a^{\frac{m_1 m_2}{d}} = \left((a_1^k)^{\frac{m_1 \times m_2}{k d}}, (a_2^\ell)^{\frac{m_2 \times m_1}{\ell d}} \right) = (e_1, e_2)$

e_1

$\omega(a) < |G_1 \times G_2|$ pas de générateur

Ex 1) Soit A un ~~anneau~~ anneau commutatif unitaire

i) Soient $P, Q \in A[X]$, avec $\deg(Q) = 1$

Mq l'on peut effectuer la division euclidienne de P par Q

ii) On suppose A intègre et $\deg P = n \geq 0$ Mq P possède au plus n racines distinctes

2) Soit $\mathbb{K}$ un CC, et G un sg fini de $\mathbb{K}^*$
montrer que G est cyclique

S/ 1)

a) Par récurrence sur le deg de P

posons $\deg Q = m$ ie:

ie $Q = X^m + \dots$, $n < m$ $P = 0 \cdot Q + P$

Si $n \geq m$ $P(X) - a_n X^{n-m} Q(X) = \underbrace{a_{n-1} X^{n-1} + \dots}_{\text{Récurrence}}$

ii) Récurrence sur n. Soit a un zéro de P dans A.

$P = \underbrace{(X-a)U}_{\text{Coef} = 1} + V$

où $\deg V \leq 0$, $V \in A$, il vient $0 = P(a) = V$

Ainsi $P(X) = (X-a)U(X)$ soit b racine de P, $b \neq a$

On a $0 = P(b) = \underbrace{(b-a)}_{\neq 0} U(b)$, A est intègre $U(b) = 0$

Les racines de $P \neq a$ les racines de U; comme $\deg U = n-1$
il y a moins de $n-1$ dans le résultat

2) Soit $a \in G$, $\omega(a) = \operatorname{PPCM}_{x \in G}(\omega(x)) = N$

* $\langle a \rangle \subset G$ et $|\langle a \rangle| = N$ ** $\forall x \in G$, $x^N - 1 = 0$ | x de ω divise N

notons alors R l'ensemble des racines de $X^N - 1$

On a $\underbrace{\langle a \rangle}_{|\cdot| = N} \subset G \subset R$ et $|R| \leq N$ | $\langle a \rangle = G = R$

KJ

V Groupe engendré par une partie

G est un groupe, $A \subset G$

Th-déf Il existe un plus petit sous groupe de G contenant A
On le note $\langle A \rangle$ et on l'appelle groupe engendré par A.

Description externe : $\langle A \rangle = \bigcap_{\substack{H \text{ sg de } G \\ H \supset A}} H$

Prop (description interne) $\langle A \rangle$ est l'ensemble des mots

$$M = a_1^{\alpha_1} \cdots a_n^{\alpha_n} \quad \left| \begin{array}{l} n \in \mathbb{N} \\ a_i \in A \\ \alpha_i \in \mathbb{Z} \end{array} \right. \quad \left(n = 0 \longrightarrow e \right) \quad i = 1, \dots, n$$

D/ $\langle A \rangle$ est un sg de G, donc contient tous les mots construits sur A.

$\mathcal{M}_G$ = ens des mots sur A et un sg de G

$M = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ $\quad M^{-1} = a_n^{-\alpha_n} \cdots a_1^{-\alpha_1}$

$M' = a_1^{\beta_1} \cdots a_n^{\beta_n}$, $MM' = a_1^{\alpha_1} \cdots a_n^{\alpha_n} \underbrace{a_{n-1}^{\beta_1}}_{a_1'} \cdots a_{\lambda-n}^{\beta_n} \in \mathcal{M}$

CC $\mathcal{M}_G = \langle A \rangle$

Ex $A = \{a, b\}$ $M = a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_n} b^{\beta_n}$, en regroupant $\alpha_i \in \mathbb{Z}$ $\beta_i \in \mathbb{Z}$

$$M = a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_n} b^{\beta_n}$$
$$\text{ou} = b^{\beta_1} \cdots a^{\alpha_n}$$

(commence avec a ou b fini avec b ou a)

On dit que a et b engendrent un groupe libre lorsque les mots réduits sont 2 à 2 $\neq$

Voc A générateur $\Leftrightarrow \langle A \rangle = G$

Ex ① $G = G_n$: transpositions et cycles

Théorème de Cauchy

Exo Soit $(G,\cdot)$ un groupe de cardinal fini, p un nombre premier. On suppose $\forall x \in G,\ o(x) \mid p$. Montrer $\exists n \in \mathbb{N}^*$ $\exists a_1, \dots, a_n \in G$ tq $G = \langle a_1, \dots, a_n \rangle$ et $|G| = p^n$

S/ G est un $\mathbb{Z}/p\mathbb{Z}$-ev

par hyp $\forall x \in G : px = 0$

Soit $\lambda \in \mathbb{Z}/p\mathbb{Z}$: $\lambda = \bar{k} = \tilde{\ell}$ il vient $\exists m \in \mathbb{Z}$ $\ell = k + mp$

$x\ell = kx + mpx = kx$: on peut donc bien définir $\lambda x = kx$

Cette opération fait de $(G,+)$ un $\mathbb{Z}/p\mathbb{Z}$ ev

$\bar{1} \cdot x = x$
$\bar{0} \cdot x = 0$
$\lambda(x+y) = \lambda x + \lambda y$

$\mathbb{Z}/p\mathbb{Z}$ f.

G est finie donc possède une base finie $(a_1, \dots, a_n)$

$\forall x \in G\ \exists!\ (\lambda_1, \dots, \lambda_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ $x = \lambda_1 a_1 + \dots + \lambda_n a_n$

et de ce fait $|G| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$

⚠ Un p-groupe n'est pas forcément commutatif.

$$G = \left\{ \begin{pmatrix} \bar{1} & \bar{a} & \bar{b} \\ \bar{0} & \bar{1} & \bar{c} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in SL_3(\mathbb{Z}/p\mathbb{Z}) \right\} \quad |G| = p^3$$

Mais c'est Ainsi pour $|G| = p$

ou $|G| = p^2$ (plus compliqué)

Compléments :

I Classes latérales

Soit G un groupe, H un ssg de G

Prop : La relation $\sim$ définie sur G^2 par $x \sim y \Leftrightarrow x^{-1}y \in H$ est d'équivalence. Pour tout $a \in G$, la classe de a pour $\sim$ est aH

D/ Comme $e \in H$, on a $\forall x \in G \; x \sim x$

soit $(x,y,z) \in G^3$. Si $x \sim y$ il vient $x^{-1}y \in H$ donc $(x^{-1}y)^{-1} = y^{-1}x \in H$ et $x \sim y$

Si de plus $y \sim z$ on a $y^{-1}z \in H$ donc $x^{-1}z = x^{-1}y(y^{-1}z) \in H$

enfin $x^{-1}y \in H \Leftrightarrow y \in xH$

Ainsi G est réunion disjointe de classes

$\exists I, \exists (a_i)_{i \in I} \in G^I$ tq $G = \bigsqcup_{i \in I} a_i H$. Noter que $\bar{e} = eH = H$

Th on suppose G est fini et H un ssg de G

1) Toute classe à gauche selon H est en bijection avec H

Lagrange 2) $|H| \mid |G|$ ($[G:H] = \frac{|G|}{|H|}$ = nbre de classes à gauche)

D/ 1) $G = \bigsqcup_{i \in I} a_i H$ donne $|G| = |I| \times |H|$

RM Si $a \in G$, $\forall \in |\langle a \rangle|$, G donc $a^{\text{Card } G} = e$

$a^p = \cdot$

$b_1 a^p \cdots b_q a^p$

Ex Soient p et q deux nombres premiers, et $(G,+)$ un groupe abélien avec $|G| = pq$. Alors $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

5/ Soit $a \in G$ on a $\omega(a) \mid pq$ donc $\omega(a) \mid p$ ~~$\omega(a) = p$~~

$\omega(a) = \{p, q, pq\}$

si $\forall a \in G, \omega(a) \mid p$ G est un $\mathbb{Z}/p\mathbb{Z}$ ev, $|G| = p^\alpha$ abs

donc $\exists a \in G$ $\omega(a) \in \{p, pq\}$, $\omega(a) = pq \Rightarrow G = \langle a \rangle$

Sinon $\exists b \in G$, $\omega(b) = q$ et alors $\omega(ab) = pq$

(CC) G est cyclique et d'ordre pq, donc $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ~~car~~

et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est d'ordre pq aussi donc $\simeq \mathbb{Z}/pq\mathbb{Z}$

Groupe quotient: — Soit H un sg distingué de G

1) Le produit de deux classes à gauche est encore à gauche

2) Pour ce produit, les classes à gauche selon H forment un groupe

3) $\left(\begin{array}{l} G \to G/H \\ a \to \overline{a} = aH\end{array}\right)$ est un morphisme de groupes de noyau H

4) Soit $f \in \mathrm{Hom}(G, G')$. Alors f se factorise sous la forme $f = \tilde{f} \circ \pi$: $G \xrightarrow{f} G'$ où $\tilde{f} \in \mathrm{Hom}(G/H, \mathrm{Im} f)$

$G \xrightarrow{\pi} G/H \xrightarrow{\tilde{f}}$ et $H = \mathrm{Ker} f$

1/ RMI H distingué donc $\forall a \in G$ $aH = Ha$

1) $aH \times bH = a(Hb)H = a(bH)H = abHH = abH$

2) Unité : $(aH)^{-1} = a^{-1}H$ — —

3) Par construction, $\pi \in \mathrm{Hom}(G/G/H)$ et $\pi(a) = \bar{e} = H$
$\Leftrightarrow aH = eH \Leftrightarrow e^{-1}a \in H \Leftrightarrow a \in H$

4) Soit $A \in G/H$, $A = aH = bH$, il vient $f(a)^{-1} f(b) = f(\underbrace{a^{-1}b}_{\in H = \ker f}) = e'$
donc $f(a) = f(b)$. On pose correctement $\tilde{f}(aH) = f(a)$
(indép des représentants). On a bien $\tilde{f} \in (\mathrm{Hom}(G/H), G)$ car
$\tilde{f}(aH) = e' \Leftrightarrow f(a) = e' \Leftrightarrow a \in H = \ker f \Leftrightarrow aH = H$ $\ker \tilde{f} = \{\bar{e}\}$
et donc $\tilde{f}$ est injective, car $\mathrm{Im}\, \tilde{f} = \mathrm{Im}\, f$.

Ex Soit H un sg de G (fini) tq $[G : H] = 2$: Mq H contient tous les carrés
(nbre de classes à gauche, égal)

S/ Soit $a \in G \setminus H$ donc $a \neq e$ et $G = H \cup aH$ (2 choses)
de même $G = H \cup Ha$
de là $Ha = aH$ distingué $|G/H| = 2$ Pour tout $a \in G$
$\bar{a}^2 = \bar{e}$, ie $a^2 \in H$

I Opérations de groupes

A Opération par conjugaison

Soit G un groupe fini. Lorsque $a \in G$, on note

$$C(a) = \{x \in G \mid ax = xa\} = \{x \in G : xax^{-1} = a\}$$

$$\mathcal{O}(a) = \{xax^{-1} \mid x \in G\}$$

RMI $a \in Z(G) \iff C(a) = G \iff O(a) = \{a\}$

1) $C(a)$ est un ssg de G et $G/C(a) \cong O(a)$

2) Soit $gC(a)$ une classe ; on pose $\varphi(gC(a)) = gag^{-1}$

Si $gC(a) = zC(a)$ il vient $z^{-1}g \in C(a)$ (DÉF)

donc $z^{-1}g \, a \, (z^{-1}g)^{-1} = a$

$z^{-1}g a g^{-1} z = a$ et donc $gag^{-1} = zaz^{-1}$ } φ est bien définie

* φ est surjective par définition [si $a' = yay^{-1}$, $a' = \varphi(yC(a))$

** Si $\varphi(yC(a)) = \varphi(zC(a))$ il vient $yay^{-1} = zaz^{-1}$

donc $z^{-1}y \, a \, (z^{-1}y)^{-1} = a$ et

$z^{-1}y \in C(a)$

$zC(a) = yC(a)$

φ est donc injective

2) $|G| = |O(a)||C(a)|$

3) Formule des classes Soit R un ens de représentants des classes de conjugaison non réduites à un point

si $a \in R$ $|O(a)| \geq 2$

si $b \notin Z(G)$ $\exists ! \, a \in R$ $O(b) = O(a)$

$$|G| = \sum |\text{classes de conjugaison}| = \sum_{\text{classe 1 ép}} 1 + \sum_{\substack{\text{classe} \\ \text{de card} \geq 2}} |\text{classe}|$$

donc $|G| = |Z(G)| + \sum_{a \in R} |O(a)| = |Z(G)| + \sum_{a \in R} \frac{|G|}{|C(a)|}$

$G/Z(G)$ cyclique $\Rightarrow G$ commutatif ($\forall q\ p^2 = |G| \Rightarrow G$ commutatif)

Appl: Soit G un p-groupe, $G = p^n$

$$|G| = |Z(G)| + \sum_{\sigma \in R} p^{k_\sigma}$$

Modulo p : $p \mid |Z(G)|$

B) Th de Cauchy

Soit G un groupe fini, et p un nombre premier tq $p \mid |G|$

Alors $\exists \sigma \in G$, $\omega(\sigma) = p$

S/ On introduit $E = \{(x_1, \dots x_p) \in G^p,\ x_1 \dots x_p = e\}$

$|E| = |G|^{p-1}$ si l'on se donne $x_1, \dots, x_{p-1} \in G$ de façon qqe

$$x_p = (x_1 \dots x_{p-1})^{-1}$$

On note $\sigma = (1 \dots p)$ soit α la relation définie sur E par :

$x \sim y \Leftrightarrow \exists k \in \mathbb{Z}\ (y_1, \dots, y_p) = (x_{\sigma^k(1)}, \dots, x_{\sigma^k(p)})$ σ permute

Elle est d'équivalence, de plus, comme $\sigma^p = Id$, par DE par p

$$\overline{x} = \{\sigma^k x \mid k = 0, \dots, p-1\}$$

i) $\sigma \cdot x = x \Rightarrow (x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1}) \Rightarrow \forall i \neq j\ x_i = x_j$

ii) $\exists k \in \{1, \dots, p-1\}$ $\sigma^k(x) = x$, Bézout $k \wedge p = 1 \Rightarrow \exists (u, v) \in \mathbb{Z}^2$ $uk + vp = 1$

de là $\sigma^{uk} \sigma^{vp} = \sigma$ et de ce fait $x = \sigma^k x = (\sigma^k)^u x = \sigma x$

donc $x_1 = \dots = x_p$

(CCP) $\bar{x}$ possède p éléments différents entre $x_1, \dots, x_p$

Donc $|E| = \sum_{\text{classes}} 1$

$$|G|^{p-1} = \sum_{\text{classes 1 élém}} 1 + \sum_{\text{p élém}} 1 \quad (\text{classes})$$

$$= (\text{nbre de classe à 1 él}) + pm$$

Modulo p comme $p/6$, le nbre de classes à 1 él est de la forme $kp + 1$

Soit $(a, \dots, a)$ une classe à un él avec $a \neq e$

il vient $a^p = e$