NOM : AUFORT **Prénom :** William **Jury :**

Algèbre ← Entourez l'épreuve → **Analyse**

Sujet choisi : 104 : Groupes finis, exemples et applications.

Autre sujet :

I Rappels sur les groupes, exemples fondamentaux

a) Définitions

Déf 1 On appelle <u>groupe</u> un ensemble G muni d'une loi de composition interne $*$ associative, admettant un élément neutre, telle que tout élément de G ait un inverse. Si $xy = yx$ $\forall (x,y) \in G^2$, G est dit <u>commutatif</u> ou <u>abélien</u>. Si $|G|$ est fini, on dit que G est un <u>groupe fini</u>.

Ex 2 : - $(\mathbb{Z},+)$ est un groupe, mais pas un groupe fini
- $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe fini (voir b)).

Déf 3 Si G, G' sont 2 groupes, un <u>morphisme</u> (de groupes) de G dans G' est une application $f : G \to G' / f(xy) = f(x)f(y)$ $\forall x,y \in G^2$.
f est un <u>isomorphisme</u> si $\exists g : G' \to G$ morphisme tel que $g \circ f = Id_G$ et $f \circ g = Id_{G'}$. Un <u>automorphisme</u> est un isomorphisme de G dans G.

Déf 4. $H \subseteq G$ est un <u>sous-groupe</u> de G si $H \neq \emptyset$, $\forall x,y \in H^2$, $xy \in H$ et $x^{-1} \in H$.

Déf/Proposition 5 : Si $A \subseteq G$, $A \neq \emptyset$, il existe un plus petit sous-groupe de G contenant A, appelé <u>sous-groupe engendré</u> par A, noté $\langle A \rangle$

Déf 6 : G est <u>monogène</u> si $\exists a \in G / G = \langle \{a\} \rangle \overset{\text{notation}}{=} \langle a \rangle$. On dit que G est <u>cyclique</u> si G est monogène et fini. On appelle <u>ordre</u> de $a \in G$ le cardinal de $\langle a \rangle$, noté $o(a)$

Prop 7 : Si $f : G \to G'$ est un morphisme, $\mathrm{Im}(f) = f(G)$ et $\ker f = \{x \in G / f(x) = e'\}$ sont des sous-groupes respectifs de G' et G.

Déf 8 : deux groupes sont isomorphes s'il existe $f : G \to G'$ un isomorphisme entre les deux.

b) Exemples fondamentaux

• $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est un groupe (muni de la loi +). (c'est même un anneau commutatif)

Prop 9 : - $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$.
- $\bar{a}$ est générateur de $\mathbb{Z}/n\mathbb{Z} \iff pgcd(a,n) = 1$.
- $\mathbb{Z}/n\mathbb{Z}$ admet donc $\varphi(n)$ générateurs distincts.

Ex 10 : Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\bar{1}, \bar{5}, \bar{7}$ et $\overline{11}$.

Déf 11 : $((\mathbb{Z}/n\mathbb{Z})^{\times}, *)$ est un groupe, c'est l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Ex 12 : Si $n = p$ premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe, mais déterminer ses générateurs est un problème "difficile" !

Ex 13 : $\mathbb{U}_n$ l'ensemble des racines n-ième de l'unité est un groupe engendré par $\zeta = \exp(\frac{2i\pi}{n})$. Il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ via $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$, $\bar{k} \mapsto \zeta^k$.

• **Déf 14 :** S_n est le groupe des permutations de $\{1,\dots,n\}$, muni de la loi de composition. $Card(S_n) = n!$

Déf 15 : Pour $i \neq j$, la <u>transposition</u> si i,j est la permutation τ_{ij} telle que $\tau_{ij}(i) = j$, $\tau_{ij}(j) = i$, $\tau_{ij}(x) = x$ sinon.

Déf 16 : On appelle <u>orbite</u> de a suivant σ l'ensemble des $\sigma^k(a)$, $k \in \mathbb{Z}$. $\sigma \in S_n$ est un <u>cycle</u> s'il ne contient qu'une seule orbite non réduite à un élément, le support est cette orbite.

Théorème 17 : Toute permutation $\sigma \neq id$ se décompose de manière unique (à l'ordre près) en un produit de cycles à supports 2 à 2 disjoints.

Déf 18 On appelle signature de $\sigma \in S_n$ $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$.

Prop 19 : $\varepsilon : S_n \to \{-1,1\}$ est un morphisme de groupes

Déf/Prop 20 $\ker \varepsilon$ est donc un sous groupe de S_n, appelé groupe alterné d'indice n, noté A_n.

II] Outils de théorie des groupes et applications aux groupes finis

a) Indice, Quotient :

Dans cette sous-partie, G est un groupe et H un sous-groupe de G.

Déf 21 : $xH = \{xy ; y \in H\}$ est la classe à gauche de x modulo H.

L'ensemble des classes à gauche modulo H est noté G/H.

L'indice de H dans G est $|G/H|$, noté aussi $[G:H]$

Théorème 22 (Lagrange) : $|G| = [G:H] \times |H|$, en particulier $|H|$ divise $|G|$.

Corollaire 23 : $\forall a \in G$, $o(a) \mid |G|$.

Déf 24 : On dit que H est distingué dans G si $\forall x \in G$, $xHx^{-1} = H$, on le note $H \triangleleft G$.

Prop 25 : La relation $x R_H y \Leftrightarrow xy^{-1} \in H$ est compatible avec G (i.e $xR_Hy, x'R_Hy' \Rightarrow (xx')R(yy')$) si et seulement si $H \triangleleft G$. G/H muni de la loi quotient $(xH).(yH) = xyH$ est alors un groupe, appelé groupe quotient.

Prop 26 : Si $[G:H] = 2$, alors $H \triangleleft G$.

Ex 27 : $\mathbb{Z}/n\mathbb{Z}$ peut être vu comme le groupe quotient des groupes $\mathbb{Z}$ et $n\mathbb{Z}$.

! $Z(G) = \{g \in G / \forall x \in G, gx = xg\}$ est un sous-gr distingué de G, appelé centre de G.

- Si $f : G \to G'$ est un morphisme, $\ker f \triangleleft G$.

Théorème 28 (d'isomorphisme) $G/\ker f \simeq \mathrm{Im} f$.

Théorème 29 : Si H et K sont deux sous groupes de G, avec $H \triangleleft G$, alors $HK \triangleleft G$ et $HK/H \simeq K/H\cap K$. (second théorème d'isomorphisme)

Déf 30 : G est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et G.

b) Actions de groupes

Déf 31 : Si X est un ensemble, on dit que G agit sur X si on s'est donné une application $\begin{array}{ccc} G\times X & \to & X \\ (g,x) & \mapsto & g.x \end{array}$ telle que
- $\forall g, g', x$, $g.(g'.x) = (gg').x$
- $\forall x$, $e.x = x$.

Déf 32 :
- L'orbite de $x \in X$ est $\omega(x) = \{y \in X / \exists g \in G / y = g.x\}$
- Le stabilisateur de $x \in X$ est $H_x = \{g \in G / g.x = x\}$. C'est un sous-groupe de G.

Prop 33 : $\varphi : \begin{array}{ccc} G/H_x & \to & \omega(x) \\ \overline{g} & \mapsto & g.x \end{array}$ est bien déf et est une bijection. En particulier, on en déduit que $|\omega(x)|$ divise $|G|$.

Ex 34 : S_n agit sur $X = \{1,\dots,n\}$ par $\sigma.i = \sigma(i)$, tout comme $\langle\sigma\rangle$. On peut retrouver la décomposition du thm 17 à partir des orbites de X sous $\langle\sigma\rangle$.

Ex 35 : G agit sur G par translation à gauche : $g.a = ga$

Corollaire 36 (Cayley) : Si $|G| = n$, G est isomorphe à un sous-groupe de S_n.

Ex 36 G agit sur G par automorphisme intérieur $g.a = gag^{-1}$.

Prop 37 : Si G fini agit sur X fini, soient $\omega_1 \dots \omega_k$ les orbites (distinctes) de cette action, alors :
- $\mathrm{Card}(E) = \sum_{i=1}^{k} \mathrm{Card}(\omega_i)$ (Formule des classes)
- Le nombre d'orbites est $k = \frac{1}{|G|}\sum_{g\in G} \mathrm{Card}(\mathrm{fix}(g))$ où $\mathrm{fix}(g) = \{x \in X / g.x = x\}$ (Formule de Burnside)

Déf 38 L'ensemble des points fixes de X sous G est $X^G = \{x \in X / \forall g \in G, g.x = x\}$

Déf 39 : On dit que G est un p-groupe si $|G| = p^\alpha$, où p est premier.

Prop 40 : Si G est un p-groupe $|X^G| \equiv |X| \bmod p$

Corollaire 41 : Le centre d'un p-groupe n'est pas trivial.

Prop 42 : Si p est le plus petit facteur premier de $|G|$, et H est un sous-groupe d'indice p alors $H \triangleleft G$.

c) Théorème de Sylow :

Remarque 43 : Par Lagrange, si H est un sous-groupe de G alors $|H| \mid |G|$. Réciproquement, a-t-on un sous-groupe de cardinal d pour tout $d \mid |G|$?

Ex 44 : $|A_4| = 12$, mais A_4 n'a pas de sous-groupe de cardinal 6.

Déf 45 : Si $|G| = n$ et p divise premier de n ($n = p^\alpha m$, $p \nmid m$), un pSylow de G est un sous-groupe de cardinal p^α, ou autrement dit un p-Sous-groupe d'indice premier avec p.

Théorème 47 (Sylow) Avec les notations et conditions précédentes, G contient un pSylow.

Lemme 46 (Stabilité par sous-groupe) Si H est un sous-groupe de G et P un pSylow de G, il existe $a \in G$ / $aPa^{-1} \cap H$ soit un pSylow de H.

Théorème 48 (Sylow) :
- Si H est un p-sous groupe de G, il est inclus dans un pSylow de G.
- Les pSylow sont tous conjugués.
- Si n_p est le nombre de pSylow, alors $n_p \equiv 1 \ (p)$ et $n_p \mid m$.

Corollaire 49 : S est l'unique pSylow de $G \trianglelefteq S_4 G$.

Application 50 : Un groupe d'ordre 63 n'est pas simple.

III] Construction de groupes

Idée 51 : A partir des groupes rencontrables connus ($\mathbb{Z}/n\mathbb{Z}$, S_n ...), comment construire d'autres groupes ?

a) Produit direct

Déf 52 : Soient N, H deux groupes. Le produit direct $G = N \times H$ est le produit cartésien de N et H muni de la loi produit $(n,h)\cdot(n',h') = (nn', hh')$.

Prop 53 (Cas de 2 groupes cycliques) : $N \times H$ est cyclique si et seulement si : N et H sont cycliques d'ordres premiers entre eux.

Prop 54 : (Théorème chinois) : Si $p \wedge q = 1$, alors $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Ex 55 : $|\mathfrak{S}_3| = 6$, non cyclique, donc ne peut s'écrire comme un produit direct.

b) Produit semi-direct

Prop-Déf 56 : Si N, H sont deux groupes, $\mathrm{Aut}N$ l'ens. des automorphismes de N, $\varphi : H \to \mathrm{Aut}N$ un morphisme, on définit le produit semi-direct $N \times_\varphi H$ comme le produit cartésien de N et H muni de la loi $(n,h)\cdot(n',h') = (n\varphi(h)(n'), hh')$. C'est un groupe.

Remarque 57 : Si $\varphi : h \mapsto id_N$, on retrouve le produit direct $N \times H$.

Remarque 58 : On peut voir φ comme une action par automorphisme de H sur N.

Déf 59 : Une suite exacte $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ est telle que i injectif, p surjectif, $\mathrm{Im}\, i = \ker p$.

Prop 60 : Si on a une suite exacte comme avant, et si p possède une section (ie un morphisme $s : H \to G$ tel que $p \circ s = id_H$), alors G est isomorphe à un produit semi direct $N \times H$.

Ex 61 : $1 \to A_n \xrightarrow{i} S_n \xrightarrow{\varepsilon} \{-1;1\} \to 1$, $s : \begin{cases} 1 \mapsto id \\ -1 \mapsto \tau \end{cases}$ section

alors $S_n \simeq A_n \times \{-1;1\}$
$\simeq A_n \times \mathbb{Z}/2\mathbb{Z}$

Ex 62 : D_n le groupe diédral des isométries du plan euclidien conservant un n-gone est tq

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

(en particulier $D_3 \simeq S_3$).

Prop 63 : Si $\varphi, \psi : H \to \mathrm{Aut}(N)$ sont tels qu'il existe $\alpha \in \mathrm{Aut}(H) / \psi = \varphi \circ \alpha$, alors $N \times_\varphi H \simeq N \times_\psi H$.

c) Automorphismes remarquables

Rem 64 : Chercher tous les produits semi-direct revient à déterminer $\mathrm{Aut}(N)$, d'où l'intérêt de connaître $\mathrm{Aut}(G)$ pour les groupes "fondamentaux". En effet, le problème général n'est pas simple.

Prop 65 : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Corollaire 66 : Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

Remarque 67 : Si p premier, $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

IV] Etude de groupes, classification

Idée 68 : A l'inverse de III, on souhaite, à partir de G, trouver un isomorphisme avec les groupes et constructions connus.

a) Cas des groupes abéliens

Théorème 69 (de structure des groupes abéliens finis) : Si G abélien de cardinal n, alors il existe $q_1 \geq 2$, q_2 multiple de q_1, ..., q_k multiple de q_{k-1} uniques, tels que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$.

Exemple 70 : Structure possible pour G abélien de cardinal 600 ?

b) Groupes d'ordre pq

Prop 71 : Soit G un groupe de cardinal pq, $p<q$ premiers. Alors : (DEV1)
- si $q \not\equiv 1 [p]$, $G \simeq \mathbb{Z}/pq\mathbb{Z}$
- si $q \equiv 1 [p]$, $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \times_\theta \mathbb{Z}/p\mathbb{Z}$ avec : $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ tel que $\theta(\bar{1}) = \tau$ d'ordre p dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

c) Groupes de petit cardinal

Ex 72 : Si $|G| = 6$, $G \simeq \mathbb{Z}/6\mathbb{Z}$ ou $G \simeq S_3$. ← il n'y a pas de $\mathfrak{S}_3$ (cf leçon 2)

Ex 73 : $|H_8| = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions n'est pas un produit semi direct.

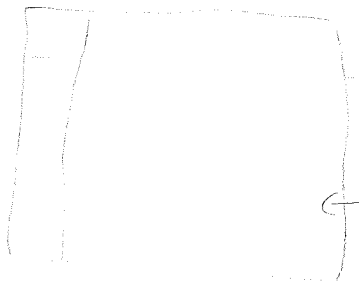
Ex 74 : Les groupes de cardinal 8 sont, à isomorphisme près, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4 et H_8. (DEV2)

Références : Combes, Rouvière, FGN Algèbre 1, (Gourdon) Hauchecorne (Contre-exs et culture).

3/3

(I) Devoir de plan

- Introduc° : histoire de l'étude des gpes.
  Act n° d'avoir la notion → arithmétique $\mathbb{Z}/n\mathbb{Z}$ } être ≠ts ms struct commun
  → permutation $\mathfrak{S}_n$ }
  Il faut attendre milieu du XIX & Cayley pour la n° de gpe et l'étude systématique
- Notations.
  $G, *$



  ↳ G fini : $* \simeq$ table
- Pdt semi-direct. Que se passe-t-il si G abélien ?

(II) Questions plan

- Exple 12. Que veut dire déterminer un gén. ?
  Quand on sait qu'il est cyclique ? ↳ gpe mult de $\mathbb{F}_p$
- Thm 24 (1ème thm d'isomor φ). Dém ?
  ↳ Erreur $H \cap K \lhd K$. Cex où $H \cap K \not\lhd G$: en prenant $H = G$ alors on aurait H ss-gpe est distingué.
  Cex de ss-gpes distingués : G, $Z(G)$)
  Pourquoi HK est un gpe ?
  ↳ $H \lhd G$. $hk(h'k') \in HK$
  $hk(h'k') = \underbrace{hkh'k^{-1}}_{\in H \lhd G} \underbrace{kk'}_{\in K}$
- Ex 62. C'est quoi l'automor φ ssc- jacent de $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$?
  ↳ La ssc° c'est $-1 \mapsto$ sym $\in$ On. cg. $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$
  $\bar{0} \mapsto \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$
  $\bar{1} \mapsto -\mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$
- Prop 64. On peut dire + préc. la forme de $(\mathbb{Z}/p\mathbb{Z})^\times$? ↳ Oui cyclique. Il y a une bse explicite

III Exos

- ‖ $H \lhd G$. S p-sylow de H $S \lhd H$. Mq $S \lhd G$.
  ↳ On veut mq $xSx^{-1} = S$ pr H $x \in G$.
  xSx^{-1} est un p-sylow de H. En effet $\forall K < H$ avec $H \lhd G$ alors $\forall x \in G$, $xKx^{-1} < H$ car H distingué. Ici on a en plus un p-sylow et on voudrait mq ça reste un p-sylow. xSx^{-1} est de m cardl que S de c'est un p-sylow.
  De + on sait que ts les p-sylow sont conjugués donc comme $S \lhd H$ alors S est le seul p-sylow de H donc $\forall x \in G$, $xSx^{-1} = S$. □

- ‖ Donner ts les gpes abéliens de card 120
  ↳ Décomposons 120 : $120 = 2 \times 5 \times 2^2 \times 3 = 2^3 \times 3 \times 5$.
  $\rightsquigarrow (120) \simeq \mathbb{Z}/120\mathbb{Z}$
  $(2, 60) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$
  $(2, 2, \frac{2\times3\times5}{30}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/30\mathbb{Z}$

IV Bqs

- Dvt : bien. Suggestion pr gagner du tps : il y a un seul élt d'ordre 2, on l'appelle -1 et $i^2 = j^2 = k^2 = -1$ et $-1 \in Z(G)$.

- Défense de plein : bien de présenter $\mathbb{Z}/n\mathbb{Z}$, S_n et struct commune. On pourrait parler de Gaffas et des act° de gpes.

- Plan. Bien. Bcp de contenu. Ok manque un peu d'appli.
  Ce qu'on pourrait enlever (s'il n'y a pas d'appli) :
  * isomorph (ou bien)
  * Burnside
  (* Sylow) ← il faut bien maîtriser ce qu'il y a autour
  (* petit semi-direct) ← c'est bien, ou il faut aussi bien maîtriser ici on a l'impression que $D_n \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ pas canonique alors que si.

(V) Autres possibilités

- Dénombrement
- Ironor & remarquables/exceptionnels
- Représentation

- Cas discret.

(VI) Questions à se poser.

- Gpes classiques $\mathbb{Z}/n\mathbb{Z}$, D_n, S_n, $Gl_n(K)$
  Se demander pq ils sont $\neq$?