103*

NOM : VOGIN Prénom : Lambert Jury :

Algèbre ← Entourez l'épreuve → ~~Analyse~~ 103*

Sujet choisi : Leçon 103 :

Autre sujet : Exemples de sous-groupes distingués et de groupes quotients. Applications.

I) Notions de groupe, sous-groupe distingué et groupe quotient

1) Premières définitions

Déf 1 : Soit G un ensemble, soit une loi de composition interne $\begin{array}{l} G\times G \longrightarrow G \\ (g,g') \longmapsto gg' \end{array}$ associative admettant 1 pour élément neutre.
Si $\forall g\in G, \exists g'\in G$ tq $gg'=1$, on dit que $(G,\cdot)$ est un groupe.

Ex 2 : $(\mathbb{C},+)$, $(\mathbb{R}_+^*,\times)$, $(\mathbb{Z},+)$, $(\mathfrak{S}_n,\circ)$, $(\mathbb{U}_n,\times)$ sont des groupes.

Déf 3 : Soit $H\subset G$, où $(G,\cdot)$ est un groupe, $H\neq\emptyset$.
On dit que H est un sous-groupe de G si $(H,\cdot)$ est un groupe, i.e.
$\begin{cases} \forall h,h'\in H, hh'\in H \\ \forall h\in H, h^{-1}\in H. \end{cases}$

Ex 4 : • $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{R},+)$,
• $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$

Déf 5 : Soit H un sous-groupe de G. Les classes à gauche suivant H sont les gH, où $g\in G$.
On note G/H l'ensemble des classes à gauche.

Théorème 6 : (Lagrange)
Si G est un groupe fini, et H un sous-groupe de G, on a $\mathrm{Card}(H) \mid \mathrm{Card}(G)$.

Ex 7 : $\mathbb{U}_n$ sous-groupe de $\mathbb{U}_m \iff n \mid m$.

Déf 8 : Soient G et G' deux groupes. Soit $\varphi : G\longrightarrow G'$.
On dit que φ est un morphisme (de groupes) si $\forall g,h\in G,\ \varphi(g\cdot h)=\varphi(g)\cdot\varphi(h)$.
Si φ est de plus bijective, on parle d'isomorphisme, et on note $G\simeq G'$.

Ex 9 : $\exp : (\mathbb{R},+)\longrightarrow(\mathbb{R}_+^*,\times)$ est un isomorphisme.

Prop 10 : Soit G un groupe, soient H, H' deux sous-groupes de G.
$H\cap H'$ est encore un sous-groupe de G.

Déf 11 : Soit A une partie de G. On note $\langle A\rangle$ et on appelle sous-groupe engendré par A le plus petit sous-groupe de G contenant A.

Ex 12 : • Si $m,n\in\mathbb{Z}$, $\langle\{m,n\}\rangle = (\mathrm{pgcd}(m,n))\mathbb{Z}$.
• $\forall n\geq 2$, $\mathfrak{S}_n=\langle\{\text{transpositions}\}\rangle=\langle (1\ i), i\in[\![2,n]\!]\rangle$

Déf 13 : On appelle générateur d'un groupe G tout élément $g\in G$ tel que $\langle\{g\}\rangle=G$.

Ex 14 : $(\mathbb{Z},+)=\langle\{1\}\rangle$, $(\mathbb{U}_n,\times)=\langle e^{\frac{2ik\pi}{n}}\rangle$ $\forall k\in[\![0,n-1]\!]$ tel que $k\wedge n=1$.

Déf 15 : Soit G un groupe, soit X un ensemble.
Si $\varphi : G\longrightarrow \mathrm{Bij}\,X$ vérifie $\begin{cases}\forall g,h\in G,\ \varphi(g)\circ\varphi(g')=\varphi(gg') \\ \varphi(1)=\mathrm{id}_X\end{cases}$
on dit que G agit sur X par φ, et on note $G \overset{\varphi}{\curvearrowright} X$.

Ex 16 : $G \overset{\text{conj}}{\curvearrowright} \{\text{sous-groupes de } G\}$ avec $\forall g\in G\ \varphi(g) = H\longmapsto gHg^{-1}$.

2) Sous-groupe distingué, groupe quotient

Déf 17 : Soient G un groupe, H un sous-groupe de G.
H est dit distingué dans G si $\forall g\in G, gHg^{-1}=H$.
On note $H \triangleleft G$.

Remarque 18 : Si on considère $G \overset{conj}{\curvearrowright} \{\text{sous-groupes de } G\}$, on a $Stab_G(H) := \{g \in G,\ gHg^{-1} = H\} = G$ si et seulement si $H \lhd G$

Ex 19 : • $\{1\}$ et G sont toujours distingués dans G
• $\{1, (1\ 2)\}$ n'est pas distingué dans $\mathfrak{S}_3$, mais $\mathfrak{A}_3 \lhd \mathfrak{S}_3$!

Prop 20 : Soient G et G' deux groupes, et $f : G \to G'$ morphisme. $\operatorname{Ker} f \lhd G$.

Prop 21 : Si G est un groupe abélien, et H un sous-groupe de G, alors $H \lhd G$.

Prop 22 : Si $H \lhd G$, $(G/_H, \cdot)$ est un groupe, appelé groupe quotient, où $gH \cdot g'H = (gg')H$.

Appl 23 : $n\mathbb{Z}$ étant un sous-groupe de $\mathbb{Z}$ abélien, $n\mathbb{Z} \lhd \mathbb{Z}$ donc $\mathbb{Z}/_{n\mathbb{Z}}$ est un groupe.

Prop 24 : Si G, G' sont des groupes, et $f : G \to G'$ un morphisme, alors :
$$\operatorname{Im} f \simeq G/_{\operatorname{Ker} f}$$

Appl 25 : $\mathfrak{A}_n \lhd \mathfrak{S}_n$
Appl 26 : Nombre de carrés dans $\mathbb{F}_q^{\times}$

manque d'appli.

II) Dévissage des groupes

1) Deux théorèmes d'isomorphisme

Prop 27 : Si G est un groupe et H, K sont des sous-groupes de G, on a :
• $H \lhd G \Rightarrow H \cap K \lhd K$
• $H \lhd G \Rightarrow HK$ sous-groupe de G, $H \lhd HK$

Prop 28 : Soit G groupe, $H \lhd G$. Soit $\pi : G \twoheadrightarrow G/_H$ la projection canonique.
• Tout sous-groupe de $G/_H$ est l'image par π d'un unique sous-groupe de G contenant H.
• Si K est un sous-groupe de G tel que $H \not\subset K$, alors HK est un sous-groupe de G contenant H, et $\pi(K) = HK/_H$.

Prop 29 : Soit G groupe, soient $H \lhd G$, K, K' deux sous-groupes de G contenant H.
• K sous-groupe de $K' \Rightarrow K/_H$ sous-groupe de $K'/_H$
• $K \lhd G \Leftrightarrow K/_H \lhd G/_H$

Théorème 30 : Soit G groupe, soit $H \lhd G$, soit K sous-groupe de G.
$$K/_{H \cap K} \simeq HK/_H$$

Théorème 31 : Soit G groupe, soient $H \lhd G$, $K \lhd G$, avec $H \subseteq K$.
$$G/_K \simeq (G/_H)/_{(K/_H)}$$

2) Centre et groupe dérivé

Déf 32 : Soit G un groupe, on note $Z(G)$ son centre :
$$Z(G) := \{a \in G,\ \forall g \in G,\ ag = ga\}$$

Ex 33 : • $Z(\mathbb{H}_8) = \{1, -1\}$
• $Z(GL_n(K)) = \{\lambda I_n,\ \lambda \in K^*\}$
• $Z(G) = G \Leftrightarrow G$ commutatif

Prop 34 : $Z(G) \lhd G$

Déf 35 : Soit G un groupe, on note $D(G)$ son sous-groupe dérivé :
$$D(G) = \langle \{xyx^{-1}y^{-1},\ x, y \in G\} \rangle.$$

Théorème 36 : • $D(G) \lhd G$
• Si $N \lhd G$, $(G/_N \text{ abélien}) \Leftrightarrow (D(G) \subseteq N)$.

Corollaire 37 : $G/_{D(G)}$ abélien

Ex 38 : • $D(G) = \{1\} \Leftrightarrow G$ abélien
• $D(\mathfrak{S}_3) = \{id, (1\ 2\ 3), (1\ 3\ 2)\} = \mathfrak{A}_3$
• $D(\mathbb{H}_8) = \{1, -1\}$

3) Produits directs et semi direct

Prop 39 : Soient N, H groupes. Posons $G = N \times H$, et $\forall (n, h), (n', h') \in G$, $(n, h) \cdot (n', h') := (nn', hh')$. $(G, \cdot)$ est un groupe, appelé produit direct de N et H.
Avec $\tilde{N} = \{(n, 1_H),\ n \in N\}$, $\tilde{H} = \{(1_N, h),\ h \in H\}$, $\tilde{N} \lhd G$, $\tilde{H} \lhd G$ et $N \simeq G/_{\tilde{H}}$, $H \simeq G/_{\tilde{N}}$.

Appl 40 : Théorème chinois
Si p, q premiers entre eux ($p, q \in \mathbb{N}^*$), on a
$$\left(\mathbb{Z}/_{pq\mathbb{Z}}\right) \simeq \left(\mathbb{Z}/_{p\mathbb{Z}}\right) \times \left(\mathbb{Z}/_{q\mathbb{Z}}\right).$$

Contre-exemple 41 : $\mathbb{Z}/_{4\mathbb{Z}} \not\simeq \left(\mathbb{Z}/_{2\mathbb{Z}}\right)^2$

Déf 42 : Soient N, G, H des groupes. On dit que
$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$
est exacte si $\begin{cases} i \text{ injective} \\ p \text{ surjective} \\ \operatorname{Im} i = \operatorname{Ker} p \end{cases}$

Ex 43 : Si $N \lhd G$, $1 \longrightarrow N \xrightarrow{\text{inclusion}} G \xrightarrow{\text{proj. can.}} G/_N \longrightarrow 1$ exacte.

Prop 44. Soit G groupe. Soit $N \lhd G$. Soit H sous-groupe de G tel que $\exists\, \varphi : H \to \mathrm{Aut}\,N$ morphisme.
Posons $\forall (n,h),(n',h') \in N \times H$,
$(n,h) \cdot_\varphi (n',h') = (n\varphi(h)(n'), hh')$.
Ona $(N \times H, \cdot_\varphi)$ groupe, appelé produit semi-direct de N et H, noté $N \rtimes_\varphi H$.

Prop 45: $1 \to N \xrightarrow{i} N \rtimes_\varphi H \xrightarrow{p} H \to 1$ est exacte, où $i(n) = (n, 1_H)$ et $p(n,h) = h$ $\forall n \in N, h \in H$.

Prop 46: • Si $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ est exacte,
$G \simeq N \rtimes H \iff \exists\, s : H \to G$ morphisme tel que $p \circ s = id_H$.
• Si G admet deux sous-groupes N, H tels que $N \lhd G$, $N \cap H = \{1\}$, $G = NH$
alors $G \simeq N \rtimes H$.

Appl 47: • $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \{-1,1\} \simeq \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.
• $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ où D_n est le groupe diédral

Remarque 48: • Si φ trivial, $N \rtimes_\varphi H = N \times H$.
• Sinon, $N \rtimes_\varphi H$ n'est pas abélien.

Appl 49: $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{H}_8$ ne sont pas des produits semi-directs

III) Groupes simples

1) Définition, premiers exemples

Déf 50: On dit d'un groupe qu'il est simple si ses seuls sous-groupes distingués sont $\{1\}$ et lui même.

Théorème 51: Un groupe est abélien et simple si, et seulement si, il est cyclique d'ordre premier.
Ainsi, les $(\mathbb{Z}/p\mathbb{Z})$, p premier, sont les seuls groupes abéliens simples à isomorphisme près.

Ex 52: $\forall n \geq 5$, $\mathfrak{A}_n$ est simple

Ex 53: $SO_3(\mathbb{R})$ est simple.

Prop 54: Si G simple, et $f : G \to G'$ morphisme, on a f injectif ou trivial.

2) Théorèmes de Sylow

Déf 55: Soit p un nombre premier, G un groupe de cardinal $p^\alpha m$, où $\alpha \geq 1$, $p \nmid m$.
Un p-Sylow de G est un sous-groupe de G de cardinal p^α.

Théorème 56 (Sylow):
Soit G comme précédemment.
• G admet un p-Sylow
• Les p-Sylow de G sont conjugués
• Si n_p désigne le nombre de p-Sylow de G,
$\begin{cases} n_p \equiv 1 [p] \\ n_p \mid m \end{cases}$

Corollaire 57: Si $n_p = 1$, G n'est pas simple.

Appl 58: Il n'y a pas de groupe simple de cardinal 15.

Théorème 59: $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.

Développements:
• 52 : $\forall n \geq 5$ $\mathfrak{A}_n$ est simple
• 59 : $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60

Refs : Perrin - Calais.

Exples de ss-gpes distingués et de gpes quotients. Appli.

I Questions dvt 2

- Pourquoi A_n seul sous-gpe d'indice 2 de $\mathfrak{S}_n$?
↳ construire un morφ non trivial de $\mathfrak{S}_n \to \{-1, 1\}$ dt $\ker = H$ (le ss-gpe d'indice 2) alors $H = A_n$ car seul morφ non trivial de $\mathfrak{S}_n \to \{-1, 1\} = \varepsilon$ (transpo conjuguées + engendrent $\mathfrak{S}_n$ ⇒ l'im d'une transpo détermine le morφ).

- Quels sont les ss-gpes distingués de $\mathfrak{S}_n$?

II Questions plan.

- Déf 5. Justifier l'appelation classe à G. ↳ Classes d'équiv.

- Prop 21. Est-ce que caractérise les gpes abéliens ?

- Prop 22. Qu'est-ce qu'elle dit en terme de gpe. ? ↳ morφ $\begin{cases} G \to G/H \\ g \mapsto gH \end{cases}$

- Thm 36. Pourquoi $D(G) \lhd G$?

- Appl 47. Quels sont les morφ ?
↳ • $\begin{cases} \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(A_n) \\ 0 \mapsto (\sigma \mapsto \sigma) \\ 1 \mapsto (\sigma \mapsto (12)\sigma(12)) \end{cases}$
• $\begin{cases} \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\,\{1, r, \dots r^{n-1}\} \\ 0 \mapsto id \\ 1 \mapsto (r^i \mapsto sr^i) \end{cases}$
une symétrie

Canoniques ?
↳ non car dépendent des élts choisis ns déf. les ss-mult à la fi.
↳ savoir pq.

on peut en trouver des ss-gpes distingués de n'importe quel ordre ds un p-gpes

- Thms de Sylow (III-2). Que peut-on dire si on part de p-gpe ?
Quand a-t-on un p-gpe simple ?
↳ que lorsque $G = \mathbb{Z}/p\mathbb{Z}$
$Z(G)$ est un p-gpe non trivial si G non abélien et est distingué
Si G est abélien alors $\simeq \mathbb{Z}/p^\alpha\mathbb{Z}$. $\alpha = 1$: corps, simple. Si $\alpha > 1$, un ss-gpe par diviseur de p^α et distingué car abélien (de manière gnale, un ss-gpe par div. de n ds $\mathbb{Z}/n\mathbb{Z}$)

III. Rqs

- Savoir immédiatement pourquoi A_4 pas simple
↳ Gpe des dbles transpositions est distingué

- On peut mettre le lien entre simplicité et table de caract. (bon dev.)

- Représentations : moins risqué que pdt semi-direct.

- On peut parler du normalisateur $\bigcap_{g \in G} gHg^{-1}$

- Présentations : un peu casse-gueule ms pq pas à l'oral