Agrégation interne de mathématiques **RK**

Séance n° 1

Thème : Groupes

Un certain nombre de choses dites ici sont valables pour des groupes quelconques, mais on insiste particulièrement sur le cas des groupes abéliens. Le théorème de structure des groupes abéliens finis est démontré en exercice.

Table des matières

1 Notes de cours

1.1 Généralités

Revoir éventuellement la définition d'un groupe, le critère de sous-groupe, la définition d'un morphisme.
L'image par un morphisme d'un sous-groupe est un sous-groupe, l'image réciproque d'un sous-groupe par un morphisme est un sous-groupe. Image et noyau sont des sous-groupes.
Une intersection de sous-groupes est un sous-groupe d'où l'existence, pour une partie donnée A de G, d'un plus petit sous-groupe de G contenant A, appelé sous-groupe engendré $< A >$. On a (on convient que le produit de zéro éléments de G vaut e_G)

$$< A >= \{g \in G;\ \exists p \in \mathbb{N},\ \exists\, x_1, x_2, \ldots, x_p \in A \cup A^{-1},\ g = x_1 x_2 \ldots x_p\}$$

En particulier $< a >= \{a^k, k \in \mathbb{Z}\}$.
Un groupe qui admet une partie génératrice de cardinal 1 est dit monogène. Un groupe monogène fini est dit cyclique.
Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

1.2 Indice d'un sous-groupe, théorème de Lagrange

L'ordre d'un groupe, c'est son cardinal. L'ordre d'un élément, c'est le cardinal du sous-groupe qu'il engendre.
Soit G un groupe et H un sous-groupe de G. Pour tout $x \in G$, on appelle classe à gauche (resp. à droite) modulo H l'ensemble $[x]_H = xH$ (resp. Hx). Les classes à gauche constituent une partition de G, associée à la relation d'équivalente dite de congruence à gauche modulo H :

$$x \equiv y \text{ modulo } H \quad \text{ssi} \quad x^{-1}y \in H.$$

L'ensemble quotient est noté G/H et la surjection canonique est $G \to G/H$, $\pi_H : x \mapsto [x]_H$.
On note que H est une classe particulière (celle de e_G) et que chaque classe peut-être mise en bijection avec H. Si on note $[G : H] = |G/H| \in \mathbb{N} \cap \{+\infty\}$ le nombre de classe à gauche (exercice : vérifier que c'est aussi le nombre de classes à droite), on a (théorème dit de Lagrange)

$$|G| = [G : H]|H|$$

En particulier si G est fini,

$$|H| \text{ divise } |G|$$

et, bien entendu, l'ordre d'un élément divise $|G|$.
Le nombre $[G : H]$ est appelé indice de H dans G.

1.3 Groupe quotient (cas commutatif)

Soit G un groupe *commutatif* et H un sous-groupe de G. Si x, x' sont congrus modulo H et y, y' sont congrus modulo H, on a $(xy)^{-1}x'y' = (x^{-1}x')(y^{-1}y') \in H$ donc xy et $x'y'$ sont congrus modulo H : la classe du produit de deux éléments ne dépend pas du choix de ces éléments dans leur classes respectives. Il donc possible de munir G/H d'une loi de composition interne vérifiant :

$$[x]_H[y]_H = [xy]_H$$

On vérifie facilement que G/H est ainsi muni d'une structure de groupe commutatif. La surjection canonique est un morphisme dont le noyau est H.

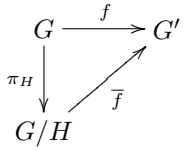
Exemple : $G = \mathbb{Z}$, $H = n\mathbb{Z}$. La classe modulo n de x est notée $[x]_n$ ou $\dot{x}$. La division euclidienne par n permet de voir que $[\mathbb{Z} : n\mathbb{Z}] = n$ et donc $|\mathbb{Z}/n\mathbb{Z}| = n$. Plus précisément,

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

Soient maintenant G, H comme ci-dessus (en particulier G commutatif) et $f : G \to G'$ un morphisme de groupe. Si (et seulement si) f est constante sur chaque classe de G modulo H, on peut définir $\overline{f} : G/H \to G'$ par $\overline{f}([x]_H) = f(x)$. C'est le cas si et seulement si

$$H \subset \mathrm{Ker}(f)$$

On dit que f "passe au quotient" modulo H et on a le diagramme "commutatif" :



$$f = \overline{f} \circ \pi_H$$

$\overline{f}$ est un morphisme de groupe dont l'image est $\mathrm{Im}(f)$ et le noyau $\pi_H(\mathrm{Ker}(f))$.

Cas particulier important : si f est un morphisme de G dans G', alors f passe au quotient modulo $\mathrm{Ker}(f)$. L'application quotient induit un isomorphisme de $G/\mathrm{Ker}(f)$ dans $\mathrm{Im}(f)$:

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$$

1.4 Groupes monogènes

Tout groupe monogène est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$. En effet, soit G un groupe monogène et a un générateur de G. L'application

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \to & G \\ & & k & \mapsto & a^k \end{array}$$

est un morphisme surjectif. Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$.
Si $n = 0$, φ est un isomorphisme.
Sinon, φ induit un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans G. Dans ce cas, a (et G) est d'ordre n et

$$G = \{a^k,\ k = 0, 1, \ldots, n-1\}$$

En corollaires :
• Deux groupes monogènes de même ordre sont isomorphes.
• Si G est un groupe quelconque et $a \in G$, $< a > \simeq \mathbb{Z}$ si a est d'ordre infini, $< a > \simeq \mathbb{Z}/n\mathbb{Z}$ si a est d'ordre n (et $< a >= \{e_G, a, a^2, \ldots, a^{n-1}\}$).
• Si G est un groupe quelconque et $a \in G$, on détermine l'ordre de a en résolvant l'équation $a^k = e_G$, $k \in \mathbb{Z}$. Si l'ensemble des solutions est $\{0\}$, a est d'ordre infini. Sinon il vaut $n\mathbb{Z}$, où n est l'ordre de a.
• Si G est un groupe fini d'ordre n, on sait que l'ordre d d'un élément quelconque $a \in G$ divise n. Donc $a^n = (a^d)^{n/d} = e_G$.

L'application φ ci-dessus permet de voir que tout sous-groupe d'un groupe cyclique est cyclique. En effet si H est un sous-groupe de G, $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, donc est monogène. H est ainsi l'image par φ d'un groupe monogène donc est monogène.

Le groupe $\mathrm{U}_n = \{z \in \mathbb{C};\ z^n = 1\}$ des racines $n^{\text{ièmes}}$ de l'unité est cyclique d'ordre n (ses générateurs sont qualifiés de racines primitives de l'unité). Le fait que U_n soit un sous-groupe du groupe des inversibles d'un corps (à savoir $\mathbb{C}$) est pratique pour établir certains résultats. Par exemple :

Si G est cyclique d'ordre n et d est un diviseur de n, G possède un unique sous-groupe d'ordre d. En outre (comme on vient de le voir), les sous-groupes de G sont cycliques. Il suffit en effet d'établir ce fait pour $G = \mathrm{U}_n$. Or si H est un sous-groupe d'ordre d de U_n, on a, pour tout $z \in H$, $z^d = 1$. Donc $H \subset \mathrm{U}_d$ et, par égalité des cardinaux, $H = \mathrm{U}_d$.

Si a est un élément d'ordre n du groupe G, alors, pour tout $p \in \mathbb{Z}$, a^p est d'ordre $\dfrac{n}{\mathrm{pgcd}(n,p)}$ (calcul simple).
En conséquence, si G est cyclique d'ordre n et a est un générateur de G, les autres générateurs sont les a^p où $\mathrm{pgcd}(n,p) = 1$.

1.5 Théorème chinois

Soient $n, m \in \mathbb{N}^*$. L'application

$$\begin{array}{rccc} \psi & : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & x & \mapsto & ([x]_n, [x]_m) \end{array}$$

est un morphisme de groupes. Son noyau vaut $\mathrm{ppcm}(n,m)\mathbb{Z}$. On ne peut donc généralement pas "passer au quotient" modulo nm. Mais dans le cas particulier où $\mathrm{pgcd}(n,m)=1$, le noyau est $nm\mathbb{Z}$ et ψ induit une application injective qui, pour des raisons de cardinal, est aussi surjective, de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$:

$$\mathrm{pgcd}(n,m)=1 \implies \mathbb{Z}/nm\mathbb{Z}\simeq\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$$

On peut aussi voir les choses ainsi : soient G et H deux groupes cycliques d'ordre n et m respectivement. Soient $a\in G$ et $b\in H$ d'ordre p et q respectivement. Alors $(a,b)\in G\times H$ est d'ordre $\mathrm{ppcm}(p,q)$. Donc $G\times H$ admet un élément d'ordre nm, c'est-à-dire est cyclique, si et seulement si on peut choisir $p|n$ et $q|n$ tels que $\mathrm{ppcm}(p,q)=nm$, c'est-à-dire si et seulement si $\mathrm{pgcd}(n,m)=1$ (on a donc la réciproque de l'implication ci-dessus). De plus, lorsque $\mathrm{pgcd}(n,m)=1$, (a,b) est générateur de $G\times H$ si et seulement si $p=n$, $q=m$: les générateur de $G\times H$ sont les couples (a,b), a générateur de G, b générateur de H.

1.6 Indicatrice d'Euler

Soit $n\in\mathbb{N}^*$. On note $\varphi(n)$ le nombre d'entiers dans $[\![0,n-1]\!]$ premiers avec n. C'est donc aussi le nombre de générateurs d'un groupe cyclique d'ordre n. L'application φ est appelée indicatrice d'Euler. Comme un groupe cyclique d'ordre n possède, pour $d|n$, un unique sous-groupe d'ordre d, lequel est cyclique, il comporte exactement $\varphi(d)$ éléments d'ordre d. Donc

$$n=\sum_{d|n}\varphi(d)$$

Le théorème chinois permet de montrer que φ est une application faiblement multiplicative, c'est-à-dire que

$$\text{si } \mathrm{pgcd}(n,m)=1 \text{ alors } \varphi(nm)=\varphi(n)\varphi(m).$$

On en déduit

$$\varphi(n)=n\prod_{p|n,p\text{ premier}}\left(1-\frac{1}{p}\right)$$

2 Exercices

1. Soit G un groupe et H,K des sous-groupes de G. À quelle condition $H\cup K$ est-il un sous-groupe de G ?
2. Donner un exemple de groupe G et d'une partie $A\subset G$ stable pour la loi produit et qui, muni de la loi induite, est un groupe, mais n'est pas un sous-groupe de G.
3. Soient G un groupe et H,K deux sous-groupes de G. On pose $HK=\{hk,\ h\in H,\ k\in K\}$.
   (a) Montrer que HK est un sous-groupe de G si et seulement si $HK=KH$.
   (b) On suppose H et K finis. Prouver $|HK|=\dfrac{|H||K|}{|K\cap H|}$ (on pourra considérer l'application $(h,k)\mapsto hk$ de $H\times K$ dans HK). Que dire si $H\cap K=\{e_G\}$?
4. Soient H' et K' deux groupes et $G=H'\times K'$. Montrer que G contient deux sous-groupes H et K vérifiant :
   i) $H\simeq H'$ et $K\simeq K'$
   ii) $H\cap K=\{e_G\}$
   iii) Si $x\in H$ et $y\in K$ alors $xy=yx$
   iv) $HK=G$

Montrer réciproquement que si H et K sont deux sous-groupes de G vérifiant ii), iii) et iv), alors l'application $(x, y) \mapsto xy$ est un isomorphisme de $H \times K$ dans G.

Remarque : lorsque G est commutatif, que la loi est notée additivement, et que H et K sont comme ci-dessus, on écrit

$$G = H \oplus K$$

Trouver deux sous-groupes non triviaux H et K de $\mathbb{Z}/15\mathbb{Z}$ tels que $\mathbb{Z}/15\mathbb{Z} = H \oplus K$.

5. Soit G un groupe, et $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. Montrer que $\mathrm{Aut}(G)$ est un groupe pour la loi $\circ$. Identifier $\mathrm{Aut}(G)$ lorsque $G = (\mathbb{Z}/2Z)^2$.
6. Donner une nouvelle preuve du théorème chinois en considérant les groupes U_n, U_m, U_{nm} et en utilisant l'exercice 4.
7. Montrer que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$ ne sont pas isomorphes.
8. Soit G un groupe fini d'ordre n. Montrer que G admet une partie génératrice de cardinal au plus $\log_2(n)$.
9. Quels sont les sous-groupes finis de $\mathbb{C}^*$? Les sous-groupes compacts ?
10. Soient G un groupe et K, H deux sous-groupes. Prouver

$$[G : H \cap K] \leqslant [G : K][G : H]$$

(en particulier, si H et K sont d'indice fini, $H \cap K$ aussi).

11. Soient p un nombre premier, et G un groupe d'ordre p^n, $n \geqslant 1$. Montrer que G admet un élément d'ordre p.
12. Soit G un groupe abélien, a et b deux éléments d'ordre fini p et q. On suppose $\mathrm{pgcd}(p, q) = 1$. Montrer que l'ordre de ab est pq. Peut-on supprimer l'hypothèse $\mathrm{pgcd}(p, q) = 1$?
13. Soit G un groupe abélien et H un sous-groupe d'indice fini p de G. Montrer

$$\forall x \in G,\ x^p \in H$$

Quels sont les sous-groupes d'indice fini de $\mathbb{C}^*$?

14. Soit G un groupe d'ordre impair. Montrer que l'application $x \mapsto x^2$ est une bijection.
15. Soit G un groupe abélien et K un sous-groupe de G. Soit $\mathcal{S}_K(G)$ l'ensemble des sous-groupes de G contenant K et $\mathcal{S}(G/K)$ l'ensemble des sous-groupes de G/K. Montrer que l'application

$$\begin{array}{ccc} \mathcal{S}_K(G) & \to & \mathcal{S}(G/K) \\ H & \mapsto & H/K \end{array}$$

est une bijection.

Retrouver ainsi l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

16. Soient G cyclique d'ordre n et G' cyclique d'ordre m. Déterminer les morphismes de G dans G'. Combien y en a-t-il ?
17. Soient K un corps et G un sous-groupe fini de $(K^*, \times)$. Prouver que G est cyclique. On pourra considérer l'ordre n de G et, pour $d|n$, le nombre $\psi(d)$ d'éléments d'ordre d de G puis établir $n = \sum_{d|n} \psi(d)$ et $\psi(d) \leqslant \varphi(d)$.

18. Soit G un groupe fini dans lequel tout élément est idempotent : $\forall x \in G,\ x^2 = e$. Montrer que G est abélien, puis que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

19. **Exposant d'un groupe abélien fini** Soit G un groupe abélien fini. On appelle exposant de G, et on note $e(G)$, le ppcm des éléments de G. Montrer qu'il existe $a \in G$ d'ordre $e(G)$.

20. **Caractères d'un groupe fini**

    Soit G un groupe fini. On appelle caractère de G un morphisme à valeurs dans le groupe $\mathbb{C}^*$. Comme le produit de deux caractères est encore un caractère, on vérifie sans mal que leur ensemble est un groupe pour cette loi, qu'on note $\widehat{G}$.

    (a) Montrer que l'image d'un caractère est un U_s.

    (b) Quels sont les caractères d'un groupe cyclique ?

    (c) On suppose ici G abélien. Soit H un sous-groupe strict de G, et $\varphi \in \widehat{H}$. Soit $x \in G \setminus H$. Quel est le plus petit sous-groupe K de G contenant H et x ? Montrer que l'on peut prolonger φ en un caractère de K. En déduire que tout caractère de H peut se prolonger en un caractère de G.

21. **Structure des groupes abéliens finis**

    Dans cet exercice, on utilise les notions d'exposant (exercice 19) et de caractère (exercice 20) pour démontrer qu'un groupe abélien fini est isomorphe à

    $$(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/n_r\mathbb{Z})$$

    où $r \in \mathbb{N}$ et les n_i sont des entiers $\geqslant 2$ vérifiant $n_i | n_{i+1}$. La notation est additive. Soit donc G un groupe abélien fini.

    (a) D'après le premier exercice cité, il existe un élément x de G d'ordre $e(G)$. Soient $\omega = e^{\frac{2i\pi}{e(G)}}$, et φ un prolongement à G (second exercice) du caractère de $\mathrm{gr}(x)$ défini par $\varphi(x^k) = \omega^k$. Montrer que $\mathrm{gr}(x) \cap \mathrm{Ker}(\varphi) = \{0\}$, puis $\mathrm{gr}(x) + \mathrm{Ker}(\varphi) = G$. En déduire l'existence d'un sous-groupe H de G tel que $G \simeq H \times \mathrm{gr}(x)$.

    (b) Conclure.

22. On montre ici que l'entier r et la suite $(n_i)_{1 \leqslant i \leqslant r}$ mis en évidence dans l'exercice précédents sont uniques. On forme l'hypothèse de récurrence sur $n \in \mathbb{N}$: si G est un groupe abélien de cardinal n, que

    $$G \simeq (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/n_r\mathbb{Z}) \simeq (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_s\mathbb{Z})$$

    où $r, s \in \mathbb{N}$, $n_i, m_i \geqslant 2$, $n_i | n_{i+1}$ et $m_i | m_{i+1}$ alors $r = s$ et $n_i = m_i$. On considère un groupe abélien G de cardinal n et on suppose l'hypothèse de récurrence vérifiée pour tout groupe d'ordre strictement inférieur à n.

    (a) Soient $a, b \in \mathbb{N}^*$. Prouver $a\dfrac{\mathbb{Z}}{b\mathbb{Z}} \simeq \dfrac{\mathbb{Z}}{\frac{b}{\mathrm{pgcd}(a,b)}\mathbb{Z}}$.

    (b) Prouver $n_1 n_2 \ldots n_r = n_1 n_2 \ldots m_s$ et $\displaystyle\prod_{i=1}^{r} \frac{n_i}{n_1} = \prod_{i=1}^{s} \frac{m_i}{\mathrm{pgcd}(n_1, m_i)}$.

    (c) Prouver $r = s$ puis $n_1 | m_1$ et conclure.

3 Annexes

3.1 Relations d'équivalence

Soit $\mathcal{R}$ une relation binaire sur un ensemble E. $\mathcal{R}$ est dite d'équivalence si elle est réflexive, symétrique et transitive. Une relation d'équivalence permet, comme on va le voir, de répartir les éléments de E en différentes "classes" (dites classes d'équivalence).
Si l'on veut répartir les éléments d'un ensemble E en différentes "classes", il y a plusieurs moyens de procéder, qui s'avèrent équivalents :

- La méthode "brute", qui consiste à considérer une partition de E (rappelons qu'une partition de E est un ensemble de parties non vides de E, deux à deux disjointes et de réunion égale à E).
- La méthode "chromatique" (identification par la "couleur") : on considère une application surjective de $\chi : E \to C$ de E dans un ensemble (de couleurs par exemple...) C. On lui associe la partition de E dont les parties sont les $\chi^{-1}(\{y\})$, où $y \in C$. Deux éléments x et x' sont donc dans la même classe lorsque $\chi(x) = \chi(x')$ (ils ont même "couleur").
- La méthode par équivalence, qui consiste donc à considérer une relation d'équivalence $\mathcal{R}$ sur E. Dans ce cas on appelle, pour chaque $x \in E$, classe d'équivalence de x modulo $\mathcal{R}$ l'ensemble $[x]_{\mathcal{R}} = \{x' \in E;\ x\mathcal{R}x'\}$. Alors $x \in [x]_R$ pour tout $x \in E$ et deux classes sont soit disjointes soit égales. Par conséquent, l'ensemble des classes d'équivalence est une partition de E notée $E/\mathcal{R}$ et appelé ensemble quotient.

Les trois points de vue sont bien équivalents :
Si X est une partition de E, on peut lui associer l'application $\chi : E \to X$ qui à $x \in E$ associe la partie de X à laquelle x appartient. On peut aussi lui associer la relation $\mathcal{R}$ définie par $x\mathcal{R}y$ lorsque x et y appartiennent à la même partie de X. On voit que la partition associée à χ comme à $\mathcal{R}$ n'est autre que X.
Si $\chi : E \to C$ est une application surjective, on peut lui associer, comme indiqué, la partition des $\chi^{-1}(\{y\})$, $y \in C$. On peut lui associer aussi la relation d'équivalence définie par $x\mathcal{R}x' \iff \chi(x) = \chi(x')$.
Enfin, étant donnée une relation d'équivalence $\mathcal{R}$ sur E, on appelle surjection canonique l'application

$$\begin{array}{rccc} \pi\ : & E & \to & E/\mathcal{R} \\ & x & \mapsto & [x]_{\mathcal{R}} \end{array}$$

L'application π joue le rôle de l'application χ ci-dessus.