Groupes
(version chantier)

Marc SAGE

<2017

Table des matières

groupe quotient (et sg normal) introduit par Hölder pour préciser le théorème de Jordan(-Holder), mais déjà en vue chez Galois

–> consulter *The development and understanding of the concept of quotient group* de Julia Nicholson

Le terme « groupe » est apparemment apparu pour la première fois sous la plume de Galois, en 1830, pour désigner en gros un sous-groupe dece qu'on appelle maintenant le groupe de Galois d'un polynôme (maisGalois ne concevait peut-être pas aussi directement l'opération decomposition). C'est Cayley qui, en 1854 (*On the Theory ofGroups...*, Philosophical Magazine 7 (40-47)), utilise le premier lemot dans son sens vraiment moderne et abstrait.

Xavier 19 06 05, 21h53

Je recopie le livre de Bertrand Hauchecorne, *Les mots et les maths* (c'est peut-être un peu long et répétitif, et tout n'est pas intéressant, mais j'ai vraiment la flemme de faire un résumé).

Le mot groupe vient de l'italien gruppo, noeud, assemblage, lui-même issu de la racine germanique kruppa (l'anglais crop, récolte, est de la même racine). Il apparaît en français au XVIIème siècle et donne bientôt denombreux dérivés.

Évariste Galois utilise le mot groupe pour désigner les permutations qui agissent sur les racines d'une équation. Il s'intéresse surtout à la structure obtenue en composant ces permutations. À partir des années 1850, des mathématiens utilisent de manière d'abord informelle l'expression groupe de permutations pour désigner les actions des transformations sur des ensembles. Le besoin d'une formalisation plus d'une axiomatisation de cette notion se fait sentir tout au long du XIXème siècle. Les premières définitions sont dues à Arthur Cayley,Camille Jordan, Leopold Kronecker, Walter Dyck. La définition actuelle est donnée par Heinrich Weber en 1893.

On peut affaiblir les axiomes en mettant :
assoc, neutre à gauche, tout élémen inversibles à gauche
(cf exos)

Les groupes de Facebook ne sont pas des groupes car ses éléments n'ont pas d'inverses.

Introduction comme groupe d'isométrie des polygone et polyèdres réguliers. Eventuellement introduire le groupe symétrique, puis théorie général des groupes, puis th Cayley pour l'universalité de S_n !

La conjugaison : juste un changement de point de vue.

Les génération : très important, ils codent tout ! Autant en prendre des simples ($1 \in Z$, transvection/dilatations dans GL, transpositions dans $\mathfrak{S}$...)

exemple d'iso : $R/Z \simeq S_1 \simeq Rot$

Toutes les orbites ont une base de lancement commune : le neutre

Les classes de G/H sont toutes équipotentes par $H \longrightarrow gH$.

L'équation $ax = b$ a toujours une unique solution $a^{-1}b$ car les transliation sont bijectives

un carré latin n'est pas toujours un goupe !

automorphismes intérieur

$\langle a \rangle = \{a^n\}$

sous groupes de $Z, +$

groupes de card $1, 2, 3, 4, 5, 6$; intéret de 6 : faire apparaitre S_3 et donc le premier groupes symétrique

groupes monogène : les classifier en Z ou cclque. Ex ; Z/nZ, racine nième de l'unité, rotation stabilisant un n-gone réglier. ils sont toujours abéléiens !

eg : groupe d'ordre premier sont cycliques

G cyclique d'ordre n, d divise n, alors il y a un unique sg d'ordre n

quotients : si H sg de G, les classes aH sont d'intersection triviale, donc partitionnent, d'où une rel eq.

EXO : *si $A \subset G$, mq $\{gA\}$ partionne G ssi A est le translaté d'un sg*

composé direct : soit A et B parties de G ableín. Tout élément de $A+B$ s'écrit $a+b$. Si cette décompotision est toujours unique, A et B sont dit en somme directe et on note $A \oplus B$

lemme :A et B en $\oplus$ ssi $A \cap B = \{0\}$.

(en mulitplicatif, on écrirait $A \odot B$ si la loi est $\cdot$, $A \circledast B$ si la loi est $*$...)

Une classe de conjugaison stalbe par carré est constituée de commutateurs. En effet, $a^2 = x^{-1}ax$, donc $a = a^{-1}x^{-1}ax$! Eg : les transvections, les 3-cycles.

Commuter se récrit en terme de conjugaison.

EXO : montrer qu'un élément commute toujours *en moyenne* avec un groupe fini, au sens où un a cmmute à G ssi $a = \frac{1}{|G|}\sum gag^{-1}$. (interperétation : on moyenne les égalités $a = gag^{-1}$)

Un sg d'un gpe dtf n'est pas forcément dtf.

Si A et B sont deux sg, alors AB sg ssi $AB = BA$

Attention : si HK est un sg, alors H et K ne commutent pas forcément (couple par couple).

morphisme : préserve la strucutre de groupe -> neutre, produit, inverse. Produit suffit, mais pas les deux autrse (même si bij) : CEG dans $\mathbb{Z}$, les endos sont les homothties, préserver inverser veut dire "fonction impaire", donc on choisit n'importe quoi de non linéaie sur $\mathbb{N}$ et on complète par symétrie.

1 Exo sur les actions

Lemme.

Deux éléments $a, b \in E$ sont dans une même orbite pour $\langle G_i \rangle$ si et seulement s'il y a une suite finie Ω_0, Ω_1, ..., Ω_n de parties de E telle que :

1. *chaque Ω_i est une orbite d'un certain groupe G_j ;*
2. *les points a et b appartiennent respectivement à Ω_0 et Ω_n ;*
3. *les orbites Ω_{i-1} et Ω_i se rencontrent pour tout $i = 1, ..., n$.*

Démonstration.

On

$\boxed{\Longrightarrow}$ On écrit $b = g(a)$ pour un certain $g \in \langle G_i \rangle$. Il y a donc des groupes $G_{i_1}, ..., G_{i_n}$ et des éléments $g_k \in G_{i_k}$ pour tout $k = 0, ..., n$ tel que $g = g_n \cdots g_0$. Notons Ω_k (pour tout $k = 0, ..., n$) l'orbite du groupe G_{i_k} qui contient l'élément $a_k := g_{k-1} \cdots g_0(a)$:

$$a = a_0 \overset{g_0}{\longmapsto} a_1 \overset{g_1}{\longmapsto} a_2 \longmapsto \cdots \overset{g_{n-1}}{\longmapsto} a_n \overset{g_n}{\longmapsto} b.$$

Chaque orbite Ω_k est stable par G_{i_k}, donc contient, outre a_k, son image $g_k(a_k) = a_{k+1}$. Par conséquent, la suite $\Omega_0, \Omega_1, ..., \Omega_n$ convient.

$\boxed{\Longleftarrow}$ Notons a_k un point de $\Omega_{k-1} \cap \Omega_k$ pour tout $k = 1, ..., n$ et posons $(a_0, a_{n+1}) := (a, b)$. Puisque a_k et a_{k+1} sont dans une même orbite Ω_k, il y a un élément g_k du groupe engendré $\langle G_i \rangle$ tel que $a_{k+1} = g_k(a_k)$, ce qui montre que

$$b = a_{n+1} = g_n(a_n) = g_n g_{n-1}(a_{n-1}) = \cdots = g_n \cdots g_0(a_0) = \underbrace{g_n \cdots g_0}_{\in \langle G_i \rangle}(a), \text{ c. q. f. d..}$$

2 exo dur

soit G un groupe vérifiant :

(1') $\{1\}$ est le seul sous-groupe d'indice infini de G

Alors G est isomorphe à$\mathbb{Z}$.

Esquisse de preuve :

Clairement, un tel groupe n'a pas de sous-groupe fini non trivial, donc est sans torsion. Donc il possède un élément d'ordre infini, ce qui prouve qu'il possède un sous-groupe d'indice fini isomorphe à $\mathbb{Z}$.

Or, on montre qu'un groupe sans torsion, possédant un sous groupe cylique infini d'indice fini doit lui-même être cyclique. Je poste la preuve sur demande ; en attendant, c'est un exo sympa.

Soit G un groupe abelien fini projectif dans cette categorie. Soit M l'exposant de G, i.e. M est le ppcm des ordres des elements de G.

Soit H la somme directe de copies de $\mathbb{Z}/\left(M^2\mathbb{Z}\right)$, une copie pour chaque element de G, i.e. $H=\bigoplus_{g\in G}\mathbb{Z}/\left(M^2\mathbb{Z}\right)e_g$ où e_g est un symbole abstrait pour g parcourant G. Soit p la surjection de H sur G definie par $p\left(e_g\right)=g$. Soit s une section de p.

Soit x un element de G. Alors $Mx=0$ donc si $s\left(x\right)=\sum y_g e_g$, on doit avoir pour tout g : $My_g=0$ dans $\mathbb{Z}/\left(M^2\mathbb{Z}\right)$. Mais cela implique alors que y_g s'ecrit $y_g=Mz_g$ pour un certain z_g dans $\mathbb{Z}/\left(M^2\mathbb{Z}\right)$. On a alors $x=ps\left(x\right)=p\left(\sum Mz_g e_g\right)=Mp\left(\sum z_g e_g\right)=0$.

Ainsi tout element x de G est nul, il en est de meme de G.

Pour le thm de structure, on peut faire prouver l'existence assez rapidement pour $\mathbb{Z}$ (ou un anneau euclidien) en prouvant que toute matrice carrée sur $\mathbb{Z}$ est equivalente (au sens $=P\cdot Q$, avec P,Q dans $GL\left(\mathbb{Z}\right)$) a une matrice diagonale.

Une preuve par récurrence sur le coeff de valeur absolue minimale et divisions euclidiennes successives est assez taupinale par exemple.

DrG.