Semaine 10 - Structure de groupe

Valentin De Bortoli
email : valentin.debortoli@gmail.com

A moins que cela ne soit explicitement précisé on adopte la notation multiplicative pour la loi du groupe G.

1 Ordre d'un élément et commutativité

1 Soit $(a,b) \in G^2$. $(ab)^{-1} = b^{-1}a^{-1} = ba$ mais $(ab)^{-1} = ab$ donc $ba = ab$. Donc G est abélien.

2 Soit G un groupe de cardinal 4. On sait que tous ces éléments ont des ordres qui divisent 4. Supposons qu'il existe un élément d'ordre 4 alors $G = \{1, a, a^2, a^3\}$. Posons $\phi : (G, *) \to (\mathbb{Z}/4\mathbb{Z}, +)$ et tel que $\phi(1) = 0$ et $\phi(a) = 1$ alors ϕ est bien un isomorphisme. Supposons qu'aucun élément n'est d'ordre 4 alors ils sont tous d'ordre deux (sauf le neutre qui est d'ordre un...). Donc G est abélien. Soit a et b deux éléments distincts de G, distincts du neutre. On a $ab \neq a$ et $ab \neq b$ sinon $a = 1$ ou $b = 1$. Donc $G = \{1, a, b, ab\}$. On pose $\phi : \left((\mathbb{Z}/2\mathbb{Z})^2, +\right) \to (G, *)$ tel que $\phi(0,0) = 1$, $\phi(1,0) = a$ et $\phi(0,1) = b$ alors ϕ est un isomorphismede groupe.

Ainsi il n'y a que deux groupes d'ordre quatre à isomorphisme près : $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.

Remarque : la page `https://fr.wikipedia.org/wiki/Liste_des_petits_groupes` recense les groupes à isomorphismes près jusqu'à l'ordre seize. On peut se poser la question : jusqu'à quel ordre connait-on le nombre de groupes à isomorphisme près ? La réponse est $2048 = 2^{11}$. La suite qui pour l'entier n vaut le nombre de groupes à isomorphismes près d'ordre n est appelée *group number*. Elle possède des propriétés très originales. Par exemple pour tous les entiers plus petits que 2048 elle vaut 1024 99% du temps... Elle fait aussi l'objet d'une conjecture : est-ce que cette suite est surjective dans $\mathbb{N}^*$? Autrement dit, est-ce que tout entier naturel non nul correspond à un nombre de groupes à isomorphismes près d'un certain ordre ? Voir `https://www.math.auckland.ac.nz/~obrien/research/gnu.pdf` pour plus d'informations (en anglais).

2 Groupe distingué, groupe quotient

1 $ghg^{-1} = gg^{-1}h = h \in H$.

2 Pour montrer que G/H est un groupe il s'agit de montrer qu'il admet une loi interne, un neutre pour cette loi, que cette loi est associative et que tout élément admet un inverse. Avant de montrer tout cela il faut montrer que la loi est bien définie ce qui n'est pas évident a priori... Soit $(g_1, g_1', g_2, g_2') \in G^4$ tels que $g_1H = g_1'H$ et $g_2H = g_2'H$ alors $g_1g_2H = g_1g_2'H$. Mais comme H est distingué $g_2'Hg_2'^{-1} = H$, c'est-à-dire $g_2'H = Hg_2'$. Donc $g_1g_2'H = g_1(Hg_2') = (Hg_1)g_2' = (g_1H)g_2' = (g_1'H)g_2' = Hg_1'g_2' = g_1'g_2'H$. Ainsi la loi est bien définie. Elle est interne. La preuve de l'associativité est triviale. On montre que H est neutre et que $g^{-1}H$ est l'inverse de gH. En effet, $gHg^{-1}H = Hgg^{-1}H = H$.

Toutes ces propriétés reposent sur le fait **essentiel** que H est distingué.

3 Soit $g \in G$ et $g_0 \in \ker(\phi)$. $\phi(gg_0g^{-1}) = \phi(g)\phi(g_0)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1$ donc $gg_0g^{-1} \in \ker(\phi)$. Donc le noyau d'un morphisme de groupe est distingué.

4 Il faut d'abord montrer que $\overline{\phi}$ est bien défini. Soit $(g, g') \in G$ tels que $g\ker(\phi) = g'\ker(\phi)$, alors il existe $g_0 \in \ker(\phi)$ tel que $g = g'g_0$ et donc $\phi(g) = \phi(g')$. Ainsi $\phi(g\ker(\phi))$ ne dépend pas du représentant g et vaut $\phi(g)$. Le fait que $\overline{\phi}$ est un morphisme de groupe est trivial. La surjectivité est immédiate également. Soit g tel que $\overline{\phi}(g\ker(\phi)) = 1$. Cela signifie que $\phi(g) = 1$ et donc $g \in \ker(\phi)$ et alors $g\ker(\phi) = \ker(\phi)$ qui est le neutre du groupe quotient. Ainsi on a bien un isomorphisme.

3 Somme des images et morphisme

1 On note S cette somme. Soit g' tel que $\phi(g') \neq 1$. $S\phi(g') = \sum_{g \in G} \phi(gg') = S$. Donc $S = 0$.

4 Un isomorphisme ?

1 Trivial

2 Trivial

3 Non car il y a un élément d'ordre deux dans $(\mathbb{Q}^*, \times)$, -1. Si on avait un isomorphisme on devrait avoir un élément d'ordre deux dans les rationnels munis de l'addition, i.e $q \in \mathbb{Q}^*,\ 2q = 0$. C'est absurde.

5 Un sous groupe d'un groupe abélien

1 On va montrer que H est sous groupe de G. Soit $(g, h) \in H^2$, $(gh^{-1})^n = gh^{-1} \dots gh^{-1} = g^n(h^{-1})^n = 1$.

6 Le théorème de Lagrange

1 Soit $\phi : H \to aH$ tel que $\phi(h) = ah$. Cette fonction est surjective. $\phi(h_1) = \phi(h_2)$ implique que $ah_1 = ah_2$ donc $h_1 = h_2$. Elle est donc injective, donc bijective. On a donc les mêmes cardinaux.

2 Soit $c \in aH$ et dans bH. Alors $c = ah_a = bh_b$. Donc $b^{-1}a \in H$. Donc $b^{-1}aH = H$ et donc $bH = bb^{-1}aH = aH$.

3 $e \in H$ donc $g \in gH$ et donc $G \subset \bigcup_{g \in G} gH$.

4 Donc en termes de cardinaux $|G| = n|H|$ avec n le nombre d'éléments distincts dans $\{gH, g \in G\}$. Donc l'ordre d'un sous-groupe divise celui du groupe.

5 H_x est un sous-groupe. Donc son cardinal divise celui de G. Mais son cardinal est l'ordre de x. Donc l'ordre de x divise celui de G.

7 Le théorème de Cayley

1 $\tau_x(x^{-1}g) = xx^{-1}g = g$ donc elle est surjective. $\tau_x(g_1) = \tau_x(g_2)$ implique que $xg_1 = xg_2$ donc $g_1 = g_2$. C'est donc une bijection.

2 Un groupe oui mais pour quelle loi ? La loi considérée ici est la composition. Elle est interne car la composée de deux bijections est une bijection. L'associativité vient de l'associativité de la composition sur les fonctions quelconques. Le neutre est l'identité. Le symétrique d'une bijection est son inverse.

3 $\tau_{xy} = \tau_x\tau_y$ donc on a bien $\phi(xy) = \phi(x) \circ \phi(y)$. De plus $\phi(1) = \mathrm{Id}$. De plus $\tau_x = \tau_y$ implique que $x1 = y1$ donc $x = y$.

4 Donc G est isomorphe à son image par ϕ qui est un sous-groupe de $\mathfrak{S}_G$.

8 Nombres réels et sous groupes

1 La borne inférieure d'une parite non vide minorée de $\mathbb{R}$ est bien définie...

2 Soit $\epsilon > 0$. Il existe $g \in G$ tel que $0 < g < \epsilon$. $g\mathbb{Z} \subset G$. Soit $x \in \mathbb{R}$, il existe $n_0 \in \mathbb{Z}$ tel que $ng \leq x \leq (n+1)g$ donc x est au plus à une distance ϵ de G. Cela vaut pour tout ϵ et donc G dense dans $\mathbb{R}$.

3 Soit une suite $(z_n)_{n\in\mathbb{N}}$ qui tend vers la borne inférieure de G_+. A partir d'un certain rang tous ses éléments sont à distance $\frac{x_0}{2}$. Si elle est stationnaire alors $x_0 \in G_+$. Sinon il existe deux éléments distincts z_{n_1} et z_{n_2} tels que $z_{n_1} \neq z_{n_2}$. Mais $|z_{n_1} - x_0| < \frac{x_0}{2}$ et donc $|z_{n_1} - z_{n_2}| < x_0$. Supposons que $z_{n_1} > z_{n_2}$ alors $z = z_{n_1} - z_{n_2} \in G_+$ et $z < x_0$. C'est absurde. Donc la suite est stationnaire et $x_0 \in G_+$.

4 Soit $x_1 \in G$. Il existe $n \in \mathbb{Z}$ tel que $nx_0 \leq x_1 \leq (n+1)x_0$. Si les inégalités sont strictes alors $x_1 - nx_0 \in G_+$ et est plus petit que x_0. C'est absurde donc $x_1 \in x_0\mathbb{Z}$.

5 On a ainsi deux situations pour les groupes additifs réels. Soit on est dense, soit on est un groupe discret.

9 Le groupe symétrique

Soit $\mathfrak{S}_n$ l'ensemble des bijections de $[\![1, n]\!]$.

1 Voir l'exercice 7 question 2.

2 On montre que tout permutation multipliée à gauche par un produit de transpositons est égale à l'identité. On raisonne par récurrence. L'initialisation est triviale sur $\mathfrak{S}_1$. Supposons que $\phi(n) = n$ alors ϕ restreinte à $[\![1, n-1]\!]$ est encore une bijection. On conclut grâce à l'hypothèse de récurrence. Sinon on définit $\tilde{\phi} = (n\phi(n))\phi$ alors $\tilde{\phi}(n) = n$ et on applique l'hypothèse de récurrence à cette permutation. On trouve que $\tilde{\phi}$ multipliée par un produit de transpositions p est égale à l'identité. Mais $p(n\phi(n))$ est encore un produit de transpositions. On peut donc conclure en remarquant que l'inverse d'un produit de transpositions est un produit de transpositions.

10 Loi de groupe et géométrie

1 On donne le procédé de construction suivant. Dans le plan on place $A(1, 0)$ et $B(0, 1)$. On considère également les points $M_0(x_0, y_0)$ et $M_1(x_1, y_1)$. On place P_0 de la manière suivante :

- $P_0 \in (AB)$.
- (P_0M_0) parallèle à (Ox).

On place Q_0 de la manière suivante :

- (P_0Q_0) et (M_1B) parallèles.
- $Q_0 \in (AM_1)$

On place M_2 de manière à ce que $M_0P_0Q_0M_2$ forme un parallélogramme.

1 Montrer que les coordonnées de Q_0 sont $(1 + x_0y_1, y_0y_1)$.

2 En déduire que M_2 a pour coordonnées $(x_0 + x_1y_0, y_0y_1)$.

3 Montrer que $\mathcal{P}' = \{M(x, y),\ y \neq 0\}$ est un groupe pour la loi $*$ définie par $M_0 * M_1 = M_2$.