TD n°2 : Quotients et groupes abéliens
1 et 4/10/2024

Exercice 1. Sous-groupes d'un quotient

Soit G un groupe, soit $H \triangleleft G$ l'un de ses sous-groupes distingués et $\pi : G \to {}^{G}/_{H}$ la projection associée.

1. Soit K un sous-groupe de G. Démontrer que $K \cap H \triangleleft K$ puis que π induit un isomorphisme

$$K/_{K \cap H} \cong \pi(K).$$

Nous voulons à présent décrire les sous-groupes de ${}^{G}/_{H}$ en fonction de ceux de G, puis les quotients correspondant à ceux des sous-groupes qui sont distingués.

2. Démontrer que l'application suivante est une bijection :

$$\{K \leq G \mid H \subseteq K\} \to \left\{\Delta \leq G/_{H}\right\}, \quad K \mapsto \pi(K).$$

3. Démontrer que cette bijection est croissante pour l'inclusion et qu'elle envoie les sous-groupes distingués de G contenant H exactement sur les sous-groupes distingués de ${}^{G}/_{H}$.
4. Soit K un sous-groupe distingué de G contenant H. Construire un isomorphisme

$$G/_{K} \cong {}^{({}^{G}/_{H})}/_{({}^{K}/_{H})}.$$

Correction de l'exercice 1

1. La conjugaison par un élément de K laisse stable H puisqu'il est distingué et K puisque c'est un sous-groupe. La conjugaison par un élément de K laisse donc stable $K \cap H$. Cela implique que $K \cap H \triangleleft K$. Considérons ensuite le morphisme de groupes $\pi_{|K}$. Son noyau vaut $K \cap \mathrm{Ker}(\pi) = K \cap H$. Le premier théorème d'isomorphisme conclut alors que π induit par passage au quotient un isomorphisme

$$K/_{K \cap H} = K/_{\mathrm{Ker}(\pi_{|K})} \cong \mathrm{Im}(\pi_{|K}) = \pi(K).$$

2. Pour se faire la main, nous redémontrons à partir de zéro cet énoncé, qui est conséquence de la proposition 2.9 de votre cours établissant une correspondance entre sous-groupes de l'image d'un morphisme et sous-groupes de la source contenant le noyau. Pour tout sous-groupe Δ de ${}^{G}/_{H}$, le sous-ensemble $\pi^{-1}(\Delta)$ de G est un sous-groupe puisqu'il s'agit de l'image inverse d'un sous-groupe par un morphisme de groupes, et il contient $\pi^{-1}(\{H\}) = H$. Nous démontrons que cela fournit un inverse à $K \mapsto \pi(K)$. En effet, pour tout sous-groupe Δ de ${}^{G}/_{H}$, nous avons

$$\pi(\pi^{-1}(\Delta)) = \Delta.$$

Ce n'est en revanche pas vrai pour un sous-groupe K quelconque de G que $\pi^{-1}(\pi(K)) = K$; nous avons seulement l'inclusion $K \subseteq \pi^{-1}(\pi(K))$. Pour tout élément de $g \in \pi^{-1}(\pi(K))$, il existe un $k \in K$ tel que $\pi(g) = \pi(k)$. Ainsi, nous pouvons écrire $g = kh$ avec $h \in \mathrm{Ker}(\pi) = H$. Lorsque $H = K$, nous avons en particulier démontré que $g \in K$, et donc que $\pi^{-1}(\pi(K)) = K$. Ceci parachève la démonstration du caractère bijectif.

3. La prise d'image par π est une application croissante pour l'inclusion. Puisqu'elle est injective lorsqu'on la restreint aux sous-groupes de G contenant H, elle est strictement croissante.

Lorsque K est distingué, pour tout élément $\pi(g)$ de ${}^{G}/_{H}$ nous avons

$$\pi(g)\pi(K)\pi(g)^{-1} = \pi(gKg^{-1}) \subseteq \pi(K)$$

grâce au caractère distingué de K. Ceci démontre que $\pi(K)$ est distingué. Réciproquement, si Δ est distingué, nous avons pour tout $g \in G$ que

$$\pi(g\pi^{-1}(\Delta)g^{-1}) \subseteq \pi(\Delta)$$

ce qui implique que

$$g\pi^{-1}(\Delta)g^{-1} \subseteq \pi^{-1}(\Delta)H.$$

Nous concluons que $\pi^{-1}(\Delta)$ est distingué en nous souvenant qu'il contient H donc que $\pi^{-1}(\Delta)H = \pi^{-1}(\Delta)$.

4. Puisque $H \subseteq K$, la propriété universelle du quotient[1] nous affirme que la projection canonique $\pi_K : G \to {}^{G}/_{K}$ se factorise par π_H en

$$\overline{\pi_K} : {}^{G}/_{H} \to {}^{G}/_{K}, \ \ gH \mapsto gK.$$

Le noyau de cette factorisation est $\pi_H(\mathrm{Ker}(\pi_K)) = \pi_H(K)$. La première question nous fournit une identification de ce noyau avec ${}^{K}/_{H}$ (nous rappelons qu'ici $H \subseteq K$). Enfin, le premier théorème d'isomorphisme appliqué au morphisme surjectif $\overline{\pi_K}$ fournit un isomorphisme

$$({}^{G}/_{H})/({}^{K}/_{H}) \xrightarrow{\sim} {}^{G}/_{K}.$$

Exercice 2. Quotient par le centre

1. Soit G un groupe tel que ${}^{G}/_{\mathrm{Z}(G)}$ est monogène. Démontrer que G est abélien.

Nous définissons[2] le *groupe des quaternions*

$$\mathbb{H}_8 = \left\{\pm\mathrm{Id}, \pm I = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}, \pm J = \pm\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}, \pm K = \pm\begin{pmatrix} 0 & -i \\ -i & 0\end{pmatrix}\right\} < \mathrm{GL}_2(\mathbb{C}).$$

2. Vérifier que I, J et K sont d'ordre 4 puis que $IJ = K$ et $JI = -K$.
3. Que dire sur le quotient de $\mathbb{H}_8$ par son centre ?

Correction de l'exercice 2

1. Soit $g \in G$ tel que $g\mathrm{Z}(G)$ engendre ${}^{G}/_{\mathrm{Z}(G)}$. Soient à présent g_1 et g_2 deux éléments de G. Par construction de g, il existe deux entiers $(k_1, k_2) \in \mathbb{Z}^2$ et deux élément $(z_1, z_2) \in \mathrm{Z}(G)^2$ tels que

$$g_i = g^{k_i} z_i \ \text{ pour } \ i = 1, 2.$$

Avec ces notations, il est possible d'écrire

$$\begin{aligned} g_1 g_2 &= g^{k_1} z_1 g^{k_2} z_2 \\ &= g^{k_1} g^{k_2} z_2 z_1 \\ &= g^{k_1+k_2} z_2 z_1 \\ &= g^{k_2} g^{k_1} z_2 z_1 \\ &= g^{k_2} z_2 g^{k_1} z_1 \\ &= g_2 g_1 \end{aligned}$$

où l'on a utilisé que z_2 est dans le centre pour passer au deuxième et quatrième lignes. Ceci démontre que G est abélien.

1. N'hésitez pas à relire l'exercice 6 du TD 1 pour vous remémorer pourquoi la rédaction qui suit n'omet aucun détail, en bref pourquoi la propriété universelle est une grande machinerie qui nous fournit des morphismes de groupes et nous donne même leur expression sans plus se soucier de savoir s'ils sont définis de manière non ambigüe.
2. Vous pouvez vérifier qu'il s'agit d'un sous-groupe.

2. Ce sont des calculs matriciels. Vous devez tomber sur $I^2 = J^2 = K^2 = -\mathrm{Id}$.
3. On vérifie également que $JK = -KJ$. Ainsi, ni I, ni J, ni K ne commutent à tous les éléments. Dans $\mathbf{H}_8$, le centre vaut $\{\pm\mathrm{Id}\}$. Le quotient de $\mathbf{H}_8$ par son centre est donc un groupe d'ordre 4, qui ne peut être cyclique sans quoi $\mathbf{H}_8$ serait abélien. Nous obtenons ainsi que
$$\mathbf{H}_8/\mathrm{Z}(\mathbf{H}_8) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^2.$$

Exercice 3. Produits semi-directs isomorphes

Soient N et K deux groupes. Soient φ et ψ des morphismes de K dans $\mathrm{Aut}(N)$.

1. Supposons qu'il existe $\alpha \in \mathrm{Aut}(K)$ tel que $\psi = \varphi \circ \alpha$. Démontrer que $N \rtimes_\varphi K$ et $N \rtimes_\psi K$ sont isomorphes.
2. Supposons qu'il existe $u \in \mathrm{Aut}(N)$ tel que
$$\forall k \in K,\ \ \psi(k) = u \circ \varphi(k) \circ u^{-1}.$$
Démontrer que $N \rtimes_\varphi K$ et $N \rtimes_\psi K$ sont isomorphes.

Soit p un nombre premier. On définit le groupe des transformations affines [3] de $\mathbb{Z}/p\mathbb{Z}$ comme
$$\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z}) := \{(x \mapsto ax+b) \in \mathrm{Bij}(\mathbb{Z}/p\mathbb{Z}) \,\big|\, a, b \in Z/p\mathbb{Z},\ \ a \neq 0\}.$$

3. Démontrer que l'ensemble des translations (i.e. pour $a = 1$) est distingué. En déduire que
$$\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/p\mathbb{Z})^\times$$
pour un certain φ que l'on explicitera.
4. Nous pouvons obtenir un isomorphisme pour d'autres φ en utilisant les questions 1 et 2. À quoi correspond le fait de changer ainsi de φ du point de vue des transformations affines ?

Correction de l'exercice 5

1. Considérons l'application
$$\iota\ :\ N \rtimes_\psi K \to N \rtimes_\varphi K,\ \ (n,k) \mapsto (n, \alpha(k)).$$
Puisque α est bijective, elle est bijective et il suffit donc de prouver qu'il s'agit d'un morphisme de groupes. Soient donc $(n_1, n_2, k_1, k_2) \in N^2 \times K^2$. Nous calculons
$$\begin{aligned}\iota((n_1,k_1) \cdot_\psi (n_2,k_2)) &= \iota((n_1\psi(k_1)(n_2), k_1k_2)) \\ &= (n_1\psi(k_1)(n_2), \alpha(k_1k_2)\end{aligned}$$
$$\begin{aligned}\iota((n_1,k_1)) \cdot_\varphi \iota((n_2,k_2) &= (n_1, \alpha(k_1)) \cdot_\varphi (n_2, \alpha(k_2)) \\ &= (n_1(\varphi\circ\alpha)(k_1)(n_2), \alpha(k_1)\alpha(k_2)\end{aligned}$$
qui sont égaux puisque $\psi = \varphi \circ \alpha$ et α est un morphisme de groupes.
2. Démontrez de même que l'application
$$j\ :\ N \rtimes_\varphi K \to N \rtimes_\psi K,\ \ (n,k) \mapsto (u(n), k)$$
est un isomorphisme. On utilisera crucialement que $\forall k \in K,\ \ \psi(k) \circ u = u \circ \psi(k)$.

3. On peut également le définir comme l'ensemble des bijections telles que $\forall x, y, \lambda,\ \ f(\lambda x + (1-\lambda)y) = \lambda f(x) + (1-\lambda) f(y)$.

3. On vérifie que l'application "coefficient directeur" est un morphisme de $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ vers $(\mathbb{Z}/p\mathbb{Z})^\times$. Son noyau, les translations, est donc un sous-groupe distingué.

   À la main : soit $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$. On démontre que

   $$(x \mapsto ax+b)^{-1} = (x \mapsto a^{-1}x - a^{-1}b)$$

   puis que

   $$\forall c \in \mathbb{Z}/p\mathbb{Z},\ \ (x \mapsto ax+b) \circ (x \mapsto x+c) \circ (x \mapsto ax+b)^{-1} = (x \mapsto x+ac).$$

   Cela prouve à la main que les translations forment un sous-groupe distingué.

   Le sous-groupes des transformations linéaires $(x \mapsto ax)$ formant un complémentaire des translations, on en déduit que $\mathbb{A}\mathfrak{U}\mathfrak{U}(\mathbb{Z}/p\mathbb{Z})$ est le produit semi-direct interne des transformations linéaires par les translations. Le premier est isomorphe par l'application "coefficient directeur" à $(\mathbb{Z}/p\mathbb{Z})^\times$, le deuxième à $\mathbb{Z}/p\mathbb{Z}$ par $f \mapsto f(0)$ ce qui conclut. Pour expliciter le morphisme, on utilise les calculs ci-dessus et on trouve que $\varphi(a)(c) = ac$.

4. Si l'on tord par un automorphisme de $(\mathbb{Z}/p\mathbb{Z})^\times$ comme à la première question, cela revient à identifier $\{(x \mapsto ax) \in \mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})\}$ à $(\mathbb{Z}/p\mathbb{Z})^\times$ non pas par $(x \mapsto ax) \mapsto a$ mais $(x \mapsto ax) \mapsto a^i$ pour un certain [4] i premier à $p-1$. Au fond, cette identification revient à choisir un générateur des translations linéaires $(x \mapsto a_0)$, et tordre par un tel automorphisme à en changer. Remarquons que changer de complémentaire ne produit par d'autres φ puisqu'il consiste à toucher au terme constant en remplaçant $(x \mapsto a_0 x)$ par un certain $(x \mapsto a_0 x + b)$, ce qui ne change pas la relation de conjugaison.

   Si l'on tord par un automorphisme de $(\mathbb{Z}/p\mathbb{Z})$, rien ne change puisque l'image de φ commute à tous lesdits automorphismes.

Exercice 5. Échauffement ?

Quelques questions avec des nombres précis pour pratiquer la structure des groupes abéliens de type fini. Trouver tous les groupes abéliens d'ordre 8 à isomorphisme près, puis d'ordre 500.

Correction de l'exercice 5

Cela correspond aux suites d'entiers se divisant mutuellement, de produit 8 (resp. 500). Nous listons en commençant par le plus grand facteur invariant possible. La liste des groupes abéliens d'ordre 8 à isomorphisme près est donc

$$\mathbb{Z}/8\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$(\mathbb{Z}/2\mathbb{Z})^3$$

De même, la liste des groupes abéliens d'ordre 500 à isomorphisme près est

$$\mathbb{Z}/500\mathbb{Z}$$
$$\mathbb{Z}/250\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$\mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$
$$\mathbb{Z}/20\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$$
$$(\mathbb{Z}/10\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z}$$

4. Se souvenir que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$ et qu'un automorphisme d'écrit donc $a \mapsto a^i$ pour un certain i premier à $p-1$.