5.1. Sous-groupes normaux. Dans le petit cours d'arithmétique nous avons défini une opération interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$ par la formule

$$\overline{a} + \overline{b} := \overline{a+b}$$

ou la même formule avec une autre notation

$$(a + n\mathbb{Z}) \ + \ (b + n\mathbb{Z}) := (a + b + n\mathbb{Z}).$$

Avec cette opération $\mathbb{Z}/n\mathbb{Z}$ est un groupe et l'application naturelle $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto \overline{a}$ est un homomorphisme de groupes.

Est-ce que nous pouvons généraliser ça ? Pour un sous-groupe $H < G$ nous venons de définir l'ensemble des translatés G/H et l'application naturelle

$$\nu_H : G \longrightarrow G/H : \nu_H(g) := g \circ H.$$

Si on met $\overline{g} := g \circ H$ pour la classe de g, il est naturel de poser la question si la formule

$$\overline{g_1} \bullet \overline{g_2} := \overline{g_1 \circ g_2} \tag{1}$$

définit une opération interne sur l'ensemble G/H, et que G/H devient un groupe avec $\bullet$. Et en plus, si $\nu_H : G \longrightarrow G/H$ est un homomorphisme dans ce cas.

La réponse est oui dans le cas où G est abélien, mais non en général.

Exercice 5.1. Montrer que si G est abélien et $H < G$, alors la formule (1) définit une opération interne *bien définie* sur G/H. Montrer que G/H avec cette opération est un groupe abélien.

Aussi l'exercice suivant donne une réponse partielle.

Exercice 5.2. Soit $f : G \longrightarrow K$ un homomorphisme avec noyau $N < G$ et image $F < K$. Montrer que le translaté $g \circ N$ est exactement le sous-ensemble de G des éléments qui ont la même image que g :

$$g \circ K = \{x \in G; f(x) = f(g)\},$$

et qu'il y a donc une bijection naturelle entre G/N et F. Une conclusion est que dans le cas de l'exercice on peut au moins identifier G/N avec un groupe.

Mais pour un sous-groupe général $H < G$, la formule (1) ne donne pas une opération interne sur l'ensemble G/H. Un translaté $g \circ H$ est déterminé par un $g \in G$, mais le représentant g n'est pas déterminé par le translaté $g \circ H$.

Exercice 5.3. Soit $H < G$ et posons $\overline{g} := g \circ H$ pour le translaté de g. Montrer que $\overline{g_1} = \overline{g_2}$ si et seulement si il existe un $h \in H$ tel que $g_1 = g_2 \circ h$.

Pour un exemple où la formule n'est pas bien définie, considérons $H := \{(1), (1, 2)\} < S_3$. Alors $\overline{(1, 3)} = \overline{(1, 3) \circ (1, 2)} = \overline{(1, 2, 3)}$. Si la formule (1) était bien définie on aurait

$$\overline{(1, 3)} \bullet \overline{(2, 3)} = \overline{(1, 2, 3)} \bullet \overline{(2, 3)},$$

ou $\overline{(1, 3) \circ (2, 3)} = \overline{(1, 2, 3) \circ (2, 3)}$, ou $\overline{(1, 3, 2)} = \overline{(1, 2)}$, ou il existerait un $h \in H$ tel que $(1, 3, 2) \circ h = (1, 2)$. Ce qui n'est pas le cas : une contradiction !

Nous allons approcher la formule d'une autre côté. Pour deux sous-ensembles X et Y d'un groupe $(G, \circ)$ on définit leur produit comme étant

$$X \circ Y := \{x \circ y; x \in X, y \in Y\} \subseteq G.$$

Comme d'habitude si l'opération est $+$ on définit la somme

$$X + Y := \{x + y;\ x \in X, y \in Y\}.$$

Par exemple, la somme de deux translatés $a + n\mathbb{Z}$ et $b + n\mathbb{Z}$ dans $\mathbb{Z}$ est un seul translaté $a + b + n\mathbb{Z}$. Le produit dans un groupe G de deux translatés à gauche (vus comme sous-ensembles de G) est la réunion de plusieurs translatés à gauches, mais en général plus que seulement un (montrer ça). On a évidemment l'inclusion

$$(g_1 \circ g_2) \circ H \subseteq g_1 \circ H \circ g_2 \circ H \tag{2}$$

mais l'inclusion peut être stricte. Pour un exemple, considérons $G := S_3$, $H := \{(1), (1, 2)\}$, $g_1 := (1, 3)$ et $g_2 := (2, 3)$. Alors

$$(g_1 \circ g_2) \circ H = \{(1, 3, 2), (2, 3)\}$$

et

$$g_1 \circ H \circ g_2 \circ H = \{(1), (1, 2), (2, 3), (1, 3, 2)\} = H \ \cup \ (g_1 \circ g_2 \circ H)$$

sont strictement différents.

Exercice 5.4. Montrer que la formule (1) donne une opération bien-définie sur G/H si et seulement si on a toujours l'égalité dans l'équation (2).

Quand pour un sous-groupe $H < G$ le produit de deux translatés (comme sous-ensembles de G) est toujours un seul translaté, alors l'opération (1) est bien définie dans G/H. On montrera facilement que G/H avec cette opération forme un groupe et la règle des homomorphismes serait satisfaite

$$\nu_H(g) \bullet \nu_H(k) = \nu_H(g \circ k).$$

Abstraitement, soient x et y deux éléments de G/H et $X \subset G$ et $Y \subset G$ les deux translatés de H correspondants. On multiplie X et Y comme sous-ensembles de G et par l'hypothèse $X \circ Y$ est un translaté Z qui correspond à un élément $z \in G/H$. Alors par définition $x \bullet y := z$. Nous n'avons pas choisi des représentants des translatés, donc la définition est bien cette fois.

On verra dans le théorème suivant que le sous-groupe H a cette propriété agréable *si et seulement si* H est le noyau d'un certain homomorphisme *si et seulement si* $ghg^{-1} \in H$ pour chaque $g \in G$ et $h \in H$ *si et seulement si* chaque translaté à gauche est simultanément un translaté à droite.

Théorème 5.1. *Soit $H < G$ un sous-groupe d'un groupe $(G, \circ)$. Alors les cinq prépositions suivantes sont équivalentes.*

(i) Pour chaque g et $k \in G$ le sous-ensemble $g \circ H \circ k \circ H$ de G est un seul translaté à gauche de H par un élément de G, ça veut dire $g \circ H \circ k \circ H = (g \circ k) \circ H$ pour chaque $g, k \in G$.

(ii) Il existe une opération interne $*$ sur l'ensemble G/H, pour laquelle $(G/H, *)$ est un groupe et pour laquelle l'application naturelle $\nu_H : G \longrightarrow G/H$ est un épimorphisme.

(iii) Il existe un groupe K et un homomorphisme $\phi : G \longrightarrow K$ tel que $H = \mathrm{Ker}(\phi)$.

(iv) On a $g \circ h \circ g^{-1} \in H$ pour chaque $g \in G$ et pour chaque $h \in H$.

(v) Chaque translaté à gauche de H par un élément de G est égal comme sous-ensemble de G à un translaté à droite de H par un élément de G, ça veut dire pour chaque $g \in G$ on a

$$g \circ H = H \circ g$$

comme sous-ensembles de G.

Preuve. Supposons (i) est vrai. Plus haut nous avons défini une opération interne bien-définie (par l'hypothèse) $\bullet$ sur l'ensemble de translatés à gauche G/H. On montre maintenant que $(G/H, \bullet)$ est un groupe.

L'associativité : soient $g_1 \circ H$, $g_2 \circ H$ et $g_3 \circ H$ trois translatés à gauche. Alors dans G/H on a

$$(g_1 \circ H \bullet g_2 \circ H) \bullet g_3 \circ H = (g_1 \circ g_2) \circ H \bullet g_3 \circ H = ((g_1 \circ g_2) \circ g_3) \circ H =$$

$$= (g_1 \circ (g_2) \circ g_3)) \circ H = g_1 \circ H \bullet (g_2 \circ H \bullet g_3 \circ H).$$

L'existence du neutre : $\mathbf{1}_G \circ H = H$ est un neutre pour $\bullet$, parce que

$$\mathbf{1}_G \circ H \bullet g \circ H = (\mathbf{1}_G \circ g) \circ H = g \circ H = (g \circ \mathbf{1}_G) \circ H = g \circ H \bullet \mathbf{1}_H \circ H$$

pour chaque $g \circ H \in G/H$.

L'existence des inverses : l'inverse $(g \circ H)^{-1}$ de $g \circ H \in G/H$ est $g^{-1} \circ H$, parce que

$$g \circ H \bullet g^{-1} \circ H = (g \circ g^{-1}) \circ H = \mathbf{1}_G \circ H = (g^{-1} \circ g) \circ H = g^{-1} \circ H \bullet g \circ H.$$

Donc $(G/H, \bullet)$ est un groupe. On a déjà vu que ν_H est surjective et que $\nu_H(g) \bullet \nu_H(k) = \nu_H(g \circ k)$, alors l'application naturelle est un épimorphisme. Alors (i) implique (ii).

Supposons (ii) est vrai. Le noyau de ν_H est

$$\{g \in G | \ \nu_H(g) = \mathbf{1}_{G/H} = \nu_H(\mathbf{1})\} = \{g \in G | \ g \circ H = H\} = H.$$

On peut prendre $(G/H, *)$ pour le groupe K et ν_H pour l'homomorphisme ϕ. Alors (ii) implique (iii).

Supposons (iii) est vrai, et que H est le noyau de ϕ, où $\phi : G \longrightarrow K$ est un homomorphisme entre les groupes $(G, \circ)$ et $(K, *)$. Pour $h \in H$ et $g \in G$ on a

$$\phi(g \circ h \circ g^{-1}) = \phi(g) * \phi(h) * \phi(g^{-1}) = \phi(g) * \mathbf{1}_K * \phi(g^{-1}) = \phi(g) * \phi(g^{-1}) = \mathbf{1}_H.$$

Donc $g \circ h \circ g^{-1} \in \operatorname{Ker} \phi = H$. Alors (iii) implique (iv).

Supposons que (iv) est vrai. Soit $g \in G$. Pour chaque $h \in H$ on a $g \circ h = (g \circ h \circ g^{-1}) \circ g \in H \circ g$. Donc $g \circ H \subseteq H \circ g$ et de façon analogue $H \circ g \subseteq g \circ H$. Alors (iv) implique (v).

Supposons que (v) est vrai. On calcule

$$g \circ H \circ k \circ H = g \circ k \circ H \circ H = (g \circ k) \circ H,$$

parce que $H \circ k = k \circ H$, par hypothèse et $H \circ H = H$, parce que $H < G$. Alors (v) implique (i). $\square$

On dit que $H < G$ est un *sous-groupe normal* de G ou *sous-groupe distingué*, si une des prépositions dans le théorème est vraie pour H (donc si toutes les prépositions sont vraies). On écrit $H \lhd G$. Par abus de notation on prend le même symbole pour les opérations internes de G et G/H. Dans la théorie des nombres, c'est la théorie de $\mathbb{Z}$, il est absolument nécessaire d'aussi considérer les groupes quotients $\mathbb{Z}/n\mathbb{Z}$. Dans la théore des groupes il est absolument nécessaire d'aussi considérer les groupes quotients par des sous-groupes normaux. Abstrait, oui, mais cela donne exactement la force de l'algèbre : une grande flexibilité !

Exemple 5.1. (i) $\mathrm{Alt}_n \lhd S_n$, parce que Alt_n est le noyau de l'homomorphism sg et le groupe S_n/Alt_n a deux éléments. Par exemple,

$$(1,2,3) \circ \mathrm{Alt}_7 \ \circ (4,5) \circ \mathrm{Alt}_7 = (1,2,3,4,5,6) \circ \mathrm{Alt}_7 \in S_7/\mathrm{Alt}_7 \,.$$

(ii) $\mathrm{SL}(n,K) \lhd \ \mathrm{GL}(n,K)$, parce que $\mathrm{SL}(n,K)$ est le noyau du déterminant. Nous écrivons

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mathrm{SL}(2,\mathbb{R})$$

pour le translaté à gauche dans le groupe quotient $K := \mathrm{GL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{R})$. Alors le neutre de K est

$$\overline{\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}}$$

et

$$\overline{\begin{pmatrix} 5 & 10 \\ 13 & 27 \end{pmatrix}}^{-1} = \overline{\begin{pmatrix} \frac{1}{10} & -1 \\ \frac{1}{10} & 1 \end{pmatrix}}.$$

(iii) Soit $H = V_4$ le 4-groupe de Klein vu comme sous-groupe de $G = \mathrm{Alt}_4$. Pour chaque $f \in V_4$, aussi $gfg^{-1} \in V_4$ pour chaque $g \in \mathrm{Alt}_4$ (même pour $f \in S_4$), donc $H \lhd G$. On a $O(G/H) = 3$, donc

$$G/H \simeq C_3.$$

Un générateur est par exemple $\sigma = \overline{(1,2,3)} = (1,2,3) \circ H$, et $G/H = \{\sigma, \sigma^2, \sigma^3 = \mathbf{1}_{G/H}\}$.

Exercice 5.5. Si $H < G$ et $(G : H) = 2$, montrer que $H \lhd G$. Donner un exemple d'un sous-groupe qui n'est pas distingué et d'index 3.

Exercice 5.6. Pour un sous-ensemble $X \subset G$ d'un groupe on définit $X^{-1} = \{x^{-1}; x \in X\}$. Soit $H < G$ un sous-groupe. Alors $H \lhd G$ *si et seulement si* pour chaque translaté à gauche $g \circ H$ on a $(g \circ H)^{-1} = g^{-1} \circ H$.

Exercice 5.7. Montrer que $U(n,K) \lhd B(n,K)$ mais $U(n,K)$ n'est pas normal dans $\mathrm{GL}(n,K)$. Ici $n > 1$ et K un corps. Montrer que $C_n \lhd D_n$. Déterminer les sous-groupes normaux de S_3.

Exercice 5.8. Soit H un sous-groupe du centre de G. (i) Montrer que $H \lhd G$. (ii) Supposons que G/H est cyclique (ça veut dire que G/H est engendré par un seul élément). Montrer que G est abélien.

Exercice 5.9. Soit S un sous-ensemble de G, tel que $gsg^{-1} \in S$ pour chaque $s \in S$ et $g \in G$. Montrer que $< S > \lhd G$. Montrer que $V_4 \lhd S_4$ et $G' \lhd G$.

Exercice 5.10. Montrer que l'intersection d'une famille quelconque de sous-groupes normaux est un sous-groupe normal.

Exercice 5.11. Soit $H < G$ un sous-groupe caractéristique, c-à-d pour chaque automorphisme $\phi \in \mathrm{Aut}(G)$ on a $\phi(H) = H$. Montrer que $H \lhd G$. Montrer que le centre et le sous-groupe dérivé sont des sous-groupes caractéristiques.

5.2. **Le théorème fondamental des homomorphismes.** L'idée de fonction (ou d'application) en mathématiques n'a pas toujours été là : c'est difficile à imaginer maintenant qu'on a dû inventer ce concept à la fin du 17ième siècle. Aussi la réalisation qu'on devrait systématiquement étudier les homomorphismes entres les groupes est d'une date relativement récente, surtout popularisé par Nicolas Bourbaki[12] il y a seulement 50 ans, sous l'influence de Emmy Noether[13]. Dans les sections qui suivent nous allons donner les théorèmes de base sur des homomorphismes. Dans les autres sujets d'algèbre (espaces vectoriels, anneaux, modules, et cetera) on a des théorèmes semblables. Une fois qu'on comprend ces théorèmes pour la théorie des groupes, les théorèmes dans les autres sujets algébriques seront facile à comprendre. Le but est simple: on veut "factoriser" les homomorphismes dans des morceaux plus simples; un peu comme on factorise un entier comme produit de nombres premiers, ou une matrice inversible comme produit de matrices élémentaires.

En composant deux morphismes $f : G \longrightarrow K$ et $g : K \longrightarrow H$ on obtient un autre homomorphisme $h = g \circ f : G \longrightarrow H$:

$$\begin{tikzcd} G \arrow[rr, "\exists\, h"] \arrow[dr, "f"'] & & H \\ & K \arrow[ur, "g"'] & \end{tikzcd}$$

Des informations sur f ou g donnent des informations sur h, et vice versa. Un exemple est donné par l'exercice suivant.

Exercice 5.12. On a

(i) $\mathrm{Im}\, h \subseteq \mathrm{Im}\, g$, donc si h est un épimorphisme, alors g est aussi un épimorphisme.

(ii) $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$, donc si h est un monomorphisme, alors f est aussi un monomorphisme.

Factoriser un homomorphisme $h : G \longrightarrow H$ comme $h = g \circ f$ peut être très utile pour la compréhension de h.

Exercice 5.13. Supposons $O(G) = 60$, $O(H) = 12$. Supposons qu'on peut factoriser l'homomorphisme $h : G \longrightarrow H$ comme $h = g \circ f$, où $f : G \longrightarrow K$ et $g : K \longrightarrow H$ et $O(K) = 35$. Montrer que $h(g) = \mathbf{1}_H$ pour chaque $g \in G$.

Pour factoriser un homomorphisme le théorème suivant est fondamental.

[12] Nicolas Bourbaki, le pseudonyme d'un groupe de mathématiciens, voir en.wikipedia.org/wiki/Bourbaki

[13] Emmy Noether, mathématicienne allemande, 1882 - 1935, "la mère de l'algèbre abstraite", voir en.wikipedia.org/wiki/Noether

Théorème 5.2 (Théorème fondamental des homomorphismes)**.** *Soit $h:\ G \longrightarrow H$ un homomorphisme et soit $f:\ G \longrightarrow K$ un épimorphisme.*

$$\begin{tikzcd} G \arrow[rr, "h"] \arrow[dr, "f"'] & & H \\ & K \arrow[ur, "\exists ? g"'] & \end{tikzcd}$$

(i) Il existe un homomorphisme $g:\ K \longrightarrow H$ tel que $g \circ f = h$ si et seulement si

$$\ker f \subseteq \ker h.$$

(ii) Il existe au maximum un seul tel homomorphisme g.

(iii) On a $\mathrm{Im}(g) = \mathrm{Im}(h)$, donc g est un épimorphisme si et seulement si h est un épimorphisme.

(iv) On a $f(\mathrm{Ker}(h)) = \mathrm{Ker}(g)$, donc g est un monomorphisme si et seulement si

$$\mathrm{Ker}(f) = \mathrm{Ker}(h).$$

Preuve. (i) Si g existe, un exercice plus haut donne que $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$. Supposons maintenant que $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$. Nous définissons une application $g : K \longrightarrow H$. Soit $y \in K$. Il existe un $x \in G$ tel que $y = f(x)$ (parce que f est un épimorphisme). Alors on définit

$$g(y) := h(x).$$

Cette définition semble dépendre du choix de la pré-image x de y, il faut donc qu'on montre que g soit bien-définie. Si x' est une autre pré-image, $x'x^{-1} \in \mathrm{Ker}(f)$, parce que $f(x'x^{-1}) = f(x')f(x)^{-1} = yy^{-1} = \mathbf{1}_K$. Donc il existe un $z \in \mathrm{Ker}(f)$ tel que $x' = xz$. Par hypothèse $z \in \mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$, donc $h(z) = \mathbf{1}_H$ et

$$h(x') = h(xz) = h(x)h(z) = h(x).$$

Il suit que à cause de $\mathrm{Ker}\, f \subseteq \mathrm{Ker}\, h$ l'application g est bien définie.

Soient $y_1, y_2 \in K$. Il existent $x_1, x_2 \in G$ tels que $f(x_1) = y_1$, $f(x_2) = y_2$ et $f(x_1x_2) = y_1y_2$. Donc

$$g(y_1y_2) = h(x_1x_2) = h(x_1)h(x_2) = g(y_1)g(y_2).$$

Alors g est un homomorphisme tel que $h = g \circ f$.

(ii) Supposons on a aussi $h = g' \circ f$. Si $f(x) = y$, alors

$$g'(y) = g'(f(x)) = h(x) = g(y).$$

Donc $g' = g$.

(iii) est montré dans l'exercice plus haut.

(iv) Soit $y \in \mathrm{Ker}\, g$ et $x \in G$ tel que $f(x) = y$. Alors par définition de g on a $g(y) = h(x) = \mathbf{1}_H$. Donc $x \in \mathrm{Ker}(h)$ et $\mathrm{Ker}(g) \subseteq f(\mathrm{Ker}(h))$. Si $y = f(x)$ où $x \in \mathrm{Ker}\, h$, alors $g(y) = h(x) = \mathbf{1}_G$ et $x \in \mathrm{Ker}\, h$, donc $y \in \mathrm{Ker}(g)$, ou $\mathrm{Ker}(g) \supseteq f(\mathrm{Ker}(h))$. □

Exercice 5.14. (i) Donner un exemple de deux homomorphismes $h : G \longrightarrow H$ et $f : G \longrightarrow K$ tels qu'il y a au moins deux homomorphismes différents $g_i : K \longrightarrow H$ tels que $h = g_i \circ f$ $(i = 1, 2)$.

(ii) Donner un exemple de deux homomorphismes $h : G \longrightarrow H$ et $f : G \longrightarrow K$ tels que $\ker f \subseteq \ker h$ mais qu'il n'y a pas d'homomorphismes $g : K \longrightarrow H$ tel que $h = g \circ f$.

Supposons on a un théorème sur une certaine classe d'homomorphismes, comme le théorème fondamental. Si on change les directions des flèches, monomorphismes par épimorphismes, Ker par Im, on trouve parfois un autre théorème. Mais la preuve peut être beaucoup plus facile (ou plus dure).

Exercice 5.15. Soit $h: \ H \longrightarrow G$ un homomorphisme et soit $f: \ K \longrightarrow G$ un monomorphisme.

$$\begin{tikzcd} G & & H \arrow[ll, "h"'] \arrow[dl, "\exists ?\ g"] \\ & K \arrow[ul, "f"] & \end{tikzcd}$$

(i) Il existe un homomorphisme $g: \ H \longrightarrow K$ tel que $f \circ g = h$ *si et seulement si*

$$\operatorname{Im} f \supset \operatorname{Im} h.$$

(ii) Il existe au maximum un seul tel homomorphisme g.

(iii) On a $\operatorname{Ker}(g) = \operatorname{Ker}(h)$, donc g est un monomorphisme si et seulement si h est un monomorphisme.

(iv) On a $f^{-1}(\operatorname{Im}(h)) = \operatorname{Im}(g)$, donc g est un épimorphisme si et seulement si

$$\operatorname{Im}(f) = \operatorname{Im}(h).$$

5.3. **Le premier théorème d'isomorphisme.** Chaque homomorphisme h factorise comme

$$h = \iota \circ \overline{h} \circ \nu_N$$

où ι est une inclusion, $\overline{h}$ un isomorphisme et ν_N l'homomorphisme naturel associé à un sous-groupe normale. Donc pour comprendre tous les homomorphismes il suffit de comprendre les inclusions, les isomorphismes et les homomorphismes naturels.

Théorème 5.3 (Premier théorème d'isomorphisme)**.** *Soit $h: \ G \longrightarrow H$ un homomorphisme. L'inclusion* $\operatorname{Im}(h) \subseteq H$ *induit un monomorphisme*

$$\iota: \ \operatorname{Im}(h) \longrightarrow H$$

défini par $\iota(x) := x$ pour $x \in \operatorname{Im}(h)$.

Alors il existe un unique isomorphisme $\overline{h}$ entre le groupe quotient $G/\operatorname{Ker}(h)$ et l'image $\operatorname{Im}(h)$ tel que

$$h = \iota \circ \overline{h} \circ \nu_{\operatorname{Ker}(h)} \ :$$

$$\begin{tikzcd} G \arrow[r, "h"] \arrow[d, "\nu_{\operatorname{Ker}(h)}"'] & H \\ G/\operatorname{Ker}(h) \arrow[r, "\exists \simeq \overline{h}"'] & \operatorname{Im}(h) \arrow[u, "\iota"'] \end{tikzcd}$$

Preuve. Les noyaux de h et $\nu_{\ker(h)}$ sont égaux, donc par le théorème fondamental des homomorphismes il existe un monomorphisme $g: G/\operatorname{Ker}(h) \longrightarrow H$ tel que $h = g \circ \nu_{\operatorname{Ker}(h)}$ et $\operatorname{Im}(h) = \operatorname{Im}(g)$. Puis, on peut appliquer l'exercice avant avec l'homomorphisme g et le monomorphisme ι. Ça donne un morphisme $\overline{h}: G/\operatorname{Ker}(h) \longrightarrow \operatorname{Im}(g)$ tel que $\iota \circ \overline{h} = g$. Cet homomorphisme est un épimorphisme (parce que $\operatorname{Im}(h) = \operatorname{Im}(\iota) = \operatorname{Im}(g)$) et un monomorphisme (parce que g est un monomorphisme). Donc $\overline{h}$ est un isomorphisme et

$$\iota \circ \overline{h} \circ \nu_{\operatorname{Ker}(h)} = h.$$

□

Corollaire 5.1. *Soit $h: G \longrightarrow H$ un homomorphisme. Alors l'index $(G : \operatorname{Ker}(h))$ divise le plus grand commun diviseur de $O(G)$ et de $O(H)$. Si $x \in G$, alors $O(h(x))$ divise le plus grand commun diviseur de $O(x)$ et de $O(H)$.*

Preuve. On a $G/\operatorname{Ker}(h) \simeq \operatorname{Im}(h)$ par le théorème, donc $(G : \operatorname{Ker}(h)) = \operatorname{Im}(h)$. Les divisibilités suivent du théorème de Lagrange. Soit $k : < x > \longrightarrow H$ la restriction de h au sous-groupe $< x >$. L'image de k est $< h(x) >$, et le noyau de k est $< x > \cap \operatorname{Ker}(h)$. Donc le premier théorème donne l'existence d'un isomorphisme

$$< x > /(< x > \cap \operatorname{Ker}(h)) \simeq < h(x) > .$$

Puis on applique le théorème de Lagrange. □

Exercice 5.16. Soit $h: G \longrightarrow H$ un épimorphisme. Si $N \lhd H$, montrer que

$$G/h^{-1}(N) \simeq H/N.$$

5.4. **Le deuxième théorème d'isomorphisme.** Si H et K sont deux sous-groupes normaux de G, alors $(H \cap K) \lhd K$ et $H \lhd HK$, où $HK = \{hk;\ h \in H, k \in K\}$ est un sous-groupe de G. Le deuxième théorème d'isomorphisme suivant dit que les deux groupes quotients $K/(H \cap K)$ et HK/H sont isomorphes.

Soit $H < G$. On pose

$$N_G(H) := \{g \in G;\ \forall h \in H:\ ghg^{-1} \in H\}.$$

On l'appelle le *normalisateur* de H dans G. Évidemment on a

$$H \lhd N_G(H) < G$$

et le normalisateur est le plus grand sous-groupe de G qui contient H comme sous-groupe normale.

Exercice 5.17. Soient H, K et L trois sous-groupes de G, tels que $H \lhd K$ et $H \lhd L$. Montrer que le sous-groupe M de G engendré par K et L est contenu dans le normalisateur $N_G(H)$.

Théorème 5.4 (Deuxième théorème d'isomorphisme)**.** *Soient H et K deux sous-groupes de G tels que*

$$K < N_G(H).$$

Alors on a
(i) $KH = HK < G$;
(ii) $H \lhd HK$ et $H \cap K \lhd K$;

(iii) et

$$K/(H \cap K) \simeq HK/H.$$

Preuve. Soit $h: \ K \longrightarrow N_G(H)/H$ la restriction à $K \subseteq N_G(H)$ de l'homomorphisme naturel

$$\nu_H: \ N_G(H) \longrightarrow N_G(H)/H.$$

Le noyau de h est $H \cap K$, donc $(H \cap K) \lhd K$. L'image de h est

$$\mathrm{Im}(h) = \{kH; \ k \in K\}.$$

C'est un sous-groupe de $N_G(H)/H$. Par le premier théorème d'isomorphisme on obtient un isomorphisme

$$K/(H \cap K) \simeq \{kH; \ k \in K\}.$$

Le pré-image $\nu_H^{-1}(\mathrm{Im}(h)) = \{kh; k \in K, h \in H\} = KH$ est un sous-groupe de $N_G(H)$, et donc de G. On a

$$kh = (khk^{-1})k \in HK$$

donc $HK = KH < N_G(H)$. Soit maintenant $k: \ HK \longrightarrow N_G(H)/H$ la restriction de ν_H à $HK \subseteq N_G(H)$. Alors l'image de k est $\mathrm{Im}(h)$, et son noyau est $HK \cap H = H$. Par le premier théorème d'isomorphisme on obtient un isomorphisme

$$HK/H \simeq \{kH; \ k \in K\}.$$

En utilisant les deux isomorphismes on obtient un isomorphisme

$$HK/H \simeq K/(H \cap K).$$

□

Exercice 5.18. Soit $G = \mathrm{Alt}_5$ et $H =< (1,2,3,4,5) >$. (i) Soit $g \in N_G H$ un élément d'ordre 5. Calculer l'ordre de $H < g >$ et conclure que $g \in H$ et $N_G H \neq G$.

(ii) Montrer que $(2,5)(3,4) \in N_G H$, et utiliser Lagrange pour montrer que $N_G H$ ne contient aucun élément d'ordre 3, i.e., aucun 3-cycle.

(iii) Montrer que Alt_5 contient 15 éléments d'ordre 2, et que ces éléments engendrent Alt_5. Conclure que $N_G H$ contient moins que 15 éléments d'ordre 2, et contient moins que 20 éléments en total.

(iv) Montrer que $N_G H =< (2,5)(3,4) > H$, d'ordre 10.

Exercice 5.19. Soit U un sous-espace vectoriel V sur un corps fixé. Définir sur V/U un structure d'espace vectoriel (appelé l'espace quotient). Formuler et montrer les versions des deux premiers théorèmes d'isomorphisme pour les espaces vectoriels.

5.5. **Le troisième théorème d'isomorphisme.** Si $N \subseteq M$ sont deux sous-groupes normaux, on peut "simplifier la fraction" $(G/N)/(M/N) \simeq G/M$.

Théorème 5.5 (Troisième théorème d'isomorphisme)**.** *Soient N et M deux sous-groupes normaux de G tels que*

$$N \subseteq M \subseteq G.$$

Alors
(i) $N \lhd M$;
(ii) On peut identifier M/N avec un sous-groupe normal de G/N;
(iii) et

$$(G/N)/(M/N) \simeq G/M.$$

Preuve. On a $N = \mathrm{Ker}(\nu_N) \subseteq \mathrm{Ker}(\nu_M) = M$, donc par le théorème fondamental des homomorphismes il existe un épimorphisme $g : \ G/N \longrightarrow G/M$ tel que $\nu_M = g \circ \nu_N$ avec noyau

$$\mathrm{Ker}(g) = \nu_N(M) = \{mN; \ m \in M\}.$$

Et comme $N \subseteq M$ l'ensemble de translatés $\{mN; \ m \in M\} \subseteq G/N$ s'identifie avec l'ensemble de translatés M/N. Donc par le premier théorème d'isomorphisme on obtient :

$$(G/N)/(M/N) \simeq G/M.$$

□

Exercice 5.20. Soient $N_0 \subset N_1 \subset N_2 \subset N_3$ quatre sous-groupes normaux d'un groupe G. Définissons

$$\overline{G} := G/N_0 \text{ et } \overline{N_i} := N_i/N_0 \lhd G/N_0,$$

pour $i = 1, 2, 3$. Puis, définissons

$$\overline{\overline{G}} := \overline{G}/\overline{N_1} \text{ et } \overline{\overline{N_i}} := \overline{N_i}/\overline{N_1} \lhd \overline{G}/\overline{N_1},$$

pour $i = 2$ et 3. Finalement, définissons

$$\overline{\overline{\overline{G}}} := \overline{\overline{G}}/\overline{\overline{N_2}} \text{ et } \overline{\overline{\overline{N_3}}} := \overline{\overline{N_3}}/\overline{\overline{N_2}} \lhd \overline{\overline{G}}/\overline{\overline{N_2}}.$$

Montrer que

$$\overline{\overline{\overline{G}}}/\overline{\overline{\overline{N_3}}} \simeq G/N_3.$$

Exercice 5.21. Soient N et M deux sous-groupes normaux de G. Montrer que $G/(N \cap M)$ est isomorphe à un sous-groupe du produit cartésien $G/N \times G/M$.

5.6. **Morphismes vers un groupe abélien.** Pour un groupe G on écrit souvent G_{ab} à la place du groupe quotient G/G', où G' est le sous-groupe dérivé de G. C'est un groupe abélien, le plus grand groupe quotient de G qui est abélien.

Théorème 5.6. *Soit $h : \ G \longrightarrow H$ un homomorphisme. Alors il existe un (unique) homomorphisme $g : \ G_{ab} \longrightarrow H$, tel que*

$$h = g \circ \nu_{G'}$$

si et seulement si $\mathrm{Im}(h)$ *est abélien si et seulement si* $G' \subset \mathrm{Ker}(h)$.

$$\begin{tikzcd} G \arrow[rr, "h"] \arrow[dr, "\nu_{G'}"'] & & H \\ & G_{ab} \arrow[ur, "\exists ?\ g"'] & \end{tikzcd}$$

Preuve. Si g existe, alors $\mathrm{Im}(h) = \mathrm{Im}(g)$ est l'image d'un groupe abélien G_{ab}, donc est abélien. Supposons $\mathrm{Im}(h)$ est abélien, donc $G' \subset \mathrm{Ker}(h)$ et on peut appliquer le théorème fondamental des homomorphismes. Ça donne l'existence de g, tel que $h = g \circ \nu_{G'}$. $\square$

Exercice 5.22. Soit A un groupe abélien. Montrer que l'application $h \mapsto \overline{h}$ induit une correspondance biunivoque entre $\mathrm{Mor}(G, A)$ et $\mathrm{Mor}(G_{ab}, A)$. Ici $\mathrm{Mor}(G, A) = \{h : G \longrightarrow A;\ h \text{ est un morphisme}\}$.

Montrer que $\mathrm{Mor}(\mathrm{Alt}_n, A)$ contient seulement un élément si $n \geq 5$.

Exercice 5.23. Soit $N \lhd G$. Montrer que $N \lhd (G'N) \lhd G$; $G/G'N$ est abélien; $G'N/N = \nu_N(G')$ et $(G/N)' = (G'N)/N$.

5.7. **Le théorème de correspondance.** Si on connaît les sous-groupes (normaux) de G/N, on connaît aussi les sous-groupes (normaux) de G contenant N.

Théorème 5.7. *Soit $N \lhd G$ et $\nu : G \longrightarrow G/N$ l'application naturelle.*

(i) Les sous-groupes de G/N sont en correspondance biunivoque avec les sous-groupes de G qui contiennent N.

(ii) Les sous-groupes normaux de G/N sont en correspondance biunivoque avec les sous-groupes normaux de G qui contiennent N.

Les correspondances sont données par

$$G/N > K \mapsto \nu^{-1}(K) < G \quad \text{et } G > H \mapsto \nu(H) < G/N.$$

Preuve. Posons $\Omega := \{H < G;\ H \supset N\}$ et $\Psi := \{K < G/N\}$ et les applications $\phi :\ \Omega \longrightarrow \Psi$ et $\eta :\ \Psi \longrightarrow \Omega$ définies par $\phi(H) := \nu_N(H)$ et $\eta(K) := \nu_N^{-1}(K)$. Il faut montrer que $\phi \circ \eta = \mathbf{1}$ et $\eta \circ \phi = \mathbf{1}$. C'est facile est laissé comme exercice. $\square$

Exercice 5.24. Soit $n \in \mathbb{Z}_{>0}$ un nombre entier. Décrire les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ en utilisant le théorème de correspondance.

Exercice 5.25. (i) Soit $G' \subset H < G$. Montrer que $H \lhd G$ en utilisant le théorème de correspondance.

(ii) Donner un exemple d'un sous-groupe $H \lhd G' \lhd G$, mais H n'est pas normal dans G.

(ii) Soit $\phi : G \longrightarrow G$ un automorphisme. Montrer que $\phi(G') = G'$, et plus généralement $\phi(G^{(n)}) = G^{(n)}$, pour chaque n.

(iii) On a $G' \lhd G$ et $G'' \lhd G'$. Montrer qu'on a aussi $G'' \lhd G$. Et plus généralement, si $N \lhd G$, alors $N^{(n)} \lhd G$ pour chaque n.

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA