CHAPITRE 19

Groupes

I Généralités

Définition I.1.

Soit G un ensemble non vide muni d'une application $* : G \times G \to G$, appelée loi de composition interne. On dit que $(G, *)$ est un groupe si

→ $*$ est associative : $\forall x, y, z \in G\ x * (y * z) = (x * y) * z$

→ $*$ admet un élément neutre, i.e. il existe $e \in G$ tel que pour tout$x \in G,\ x * e = x = e * x$.

→ Tout élément admet un inverse, i.e. $\forall x \in G,\ \exists x^{-1} \in G,\ x * x^{-1} = e = x^{-1} * x$

Si $*$ est commutative, i.e. $\forall x, y \in G\ x * y = y * x$, on dit alors que $(G, *)$ est un groupe commutatif ou groupe abélien.

Notations :

→ Lorsque $(G, *)$ est un groupe commutatif, on notera plutôt $(G, +)$. Dans tout le reste du chapitre, on considère G un groupe d'élément neutre e.

→ Lorsque A et B sont deux ensembles disjoints, on note $A \sqcup B$ au lieu de $A \cup B$.

Exercice I.2.

Soit $(H, *)$ un monoïde (i.e. $*$ est associative et admet un élement neutre) tel que tout element admet un inverse à gauche. Montrer que H est un groupe.

Définition I.3.

On dit que $H \subset G$ est un sous-groupe du groupe $(G, *)$ si H est stable par $*$ et $(H, *|_{H\times H}^{H}) = (H, *)$ forme un groupe. On notera $H \leq G$.

Proposition I.4.

$(H, *)$ est un sous-groupe de $(G, *)$ si et seulement si $H \neq \varnothing$ et

$$\forall x, y \in H\ x * y^{-1} \in H$$

Proposition I.5.

Soit $(H, *)$ un sous-groupe de $(G, *)$. Les propositions suivantes sont vraies.

1. G et H ont le même élément neutre.
2. Pour tout $x \in H$, l'inverse de x dans $(H, *)$ est égal à l'inverse de x dans $(G, *)$.
3. $\forall g, h \in G,\ (g * h)^{-1} = h^{-1} * g^{-1}$

Preuve

1. Posons e_G et e_H les éléments neutres respectifs de de $(G,*)$ et $(H,*)$. On a $e_H * e_H = e_H$, donc en multipliant des deux côtés par l'inverse de e_H dans $(G,*)$, on obtient $e_H = e_G$.

2. Soit $a \in H$ et a_H^{-1}, a_G^{-1} ses inverses respectifs dans $(H,*)$ et $(G,*)$. On a $a_H^{-1} * a = e_H = e_G$ donc en multipliant des deux côtés à droite par a_G^{-1}, on obtient $a_G^{-1} = a_H^{-1}$.

3. Pour tout $g, h \in G$, on a $(g*h)*(h^{-1}*g^{-1}) = e$ et donc en multipliant par $(g*h)^{-1}$ des deux côtés à gauche, on obtient $(g*h)^{-1} = h^{-1}*g^{-1}$.

Proposition I.6.

Soit $(G,*)$ un groupe et $S \subset G$. Alors il existe un (unique) sous-groupe minimum (pour l'inclusion) de G contenant S qu'on nomme sous-groupe engendré par S et note $\langle S \rangle$. On a alors

$$\langle S \rangle = \bigcap_{H \leq G,\ S \subset H} H$$

Preuve : Il suffit de vérifier qu'une intersection quelconque de sous-groupes est toujours un sous-groupe. Ceci étant clair, on a alors que $\displaystyle\bigcap_{H \leq G,\ S \subset H} H$ est bien un sous-groupe minimum (pour l'inclusion) contenant S et donc on a bien l'existence. L'unicité provient du fait que, dans un ensemble partiellement ordonné, le minimum est toujours unique s'il existe.

Exercice I.7.

Soit H une partie non vide finie de G. Montrer que

$$H \leq G \iff \forall (x,y) \in H^2,\ x * y \in H$$

Notations :

→ (Translations dans un groupe G) Soit $a \in G$. On note

$$\gamma_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto a * x \end{cases} \quad \text{et} \quad \delta_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto x * a \end{cases}$$

Il s'agit de permutations de G qui sont des morphismes seulement si $a = e$.

→ (Puissances dans un groupe G) Soit $n \in \mathbb{Z}^*$ et $x \in G$. On définit

$$x^n := \underbrace{x^\delta * \cdots * x^\delta}_{|n| \text{ fois}} \quad \text{où } \delta = \begin{cases} 1 \text{ si } n \geq 1 \\ -1 \text{ si } n \leq -1 \end{cases}$$

Pour $n = 0$ on définit $x^0 = e$. Compte tenu de cette définition, il est aisé de vérifier que

$$\forall (n,m) \in \mathbb{Z}^2,\ x^{n+m} = x^n * x^m$$

→ On note $Z(G) = \{x \in G,\ \forall y \in G\ x * y = y * x\}$.

Remarque : lorsqu'on note $+$ au lieu de $*$, on note souvent nx au lieu de x^n.

Définition I.8.

Soit f une application de G vers H. On dit que f est un morphisme (ou homomorphisme) de groupe de $(G, *)$ vers $(H, \Diamond)$ si

$$\forall x, y \in G,\ f(x * y) = f(x) \Diamond f(y)$$

On notera $\mathrm{Hom}(G, H)$ l'ensemble des morphismes de $(G, *)$ vers $(H, \Diamond)$.

Exemples

1. Soit $a \in G$. L'application $j_a : \begin{cases} (\mathbb{Z}, +) & \longrightarrow (G, *) \\ n & \longmapsto a^n \end{cases}$ est un morphisme de groupe.
2. Soit $a \in G$. L'application $\sigma_a : \begin{cases} G & \longrightarrow G \\ x & \longmapsto a * x * a^{-1} \end{cases}$ est un morphisme de groupe bijectif, d'inverse $\sigma_{a^{-1}}$. Ce morphisme est nommé automorphisme intérieur associé à a.
   En effet, en considérant $a, b, g \in G$, on peut affirmer que
   $$\sigma_a \circ \sigma_b(g) = \sigma_a(b * g * b^{-1}) = a * b * g * b^{-1} * a^{-1} = (a * b) * g * (a * b)^{-1} = \sigma_{a*b}(g)$$
   d'où $\sigma_{a*b} = \sigma_a \circ \sigma_b$ et donc, en particulier, $\sigma_a \circ \sigma_{a^{-1}} = \sigma_e = \mathrm{Id} = \sigma_e = \sigma_{a^{-1}} \circ \sigma_a$ ce qui nous permet bien de dire que σ_a est un morphisme bijectif.

Vocabulaire : On dit que $x, y \in G$ sont conjugués s'il existe $a \in G$ tel que $y = a * x * a^{-1} = \sigma_a(x)$. La relation de conjugaison est en fait d'une relation d'équivalence sur G, qui donc le partitionne en classes d'équivalences de conjugaison.

Proposition I.9.

Soit $(G', \Diamond)$ un groupe, e, e' les éléments neutres respectifs de G et G' et $f \in \mathrm{Hom}(G, G')$.

1. $f(e) = e'$
2. Si $H \leq G$ alors $f(H) \leq G'$. En particulier, $\mathrm{Im}\, f = f(G) \leq G'$.
3. Si $K \leq G'$ alors $f^{-1}(K) \leq G$. En particulier, $\mathrm{Ker}\, f = f^{-1}(\{e'\}) \leq G$.
4. f est injective $\Longleftrightarrow \mathrm{Ker}\, f = \{e\} \Longleftrightarrow \mathrm{Ker}\, f \subset \{e\}$

Preuve : Les preuves de ces résultats sont laissées comme exercice au lecteur.

Proposition I.10.

Soit $(H, \Diamond)$ et $(H', \Diamond')$ deux groupes.

1. Les homomorphismes se composent i.e. on peut composer $f \in \mathrm{Hom}(H, H')$ avec $g \in \mathrm{Hom}(G, H)$ pour obtenir $f \circ g \in \mathrm{Hom}(G, H')$.
2. Les isomorphismes (morphismes bijectifs) se composent i.e. on peut composer $f \in \mathrm{Hom}(H, H')$ isomorphisme avec $g \in \mathrm{Hom}(G, H)$ isomorphisme pour obtenir $f \circ g \in \mathrm{Hom}(G, H')$ isomorphisme.
3. L'ensemble des isomorphismes de G vers G, nommés automorphismes de G et notés $\mathrm{Aut}(G)$, forment un groupe pour la loi $\circ$.

Notation : S'il existe un isomorphisme entre deux groupes G et H, on notera $G \simeq H$.

Exemple : L'application $\varphi : \begin{cases} G & \longrightarrow \mathrm{Aut}(G) \\ a & \longmapsto \sigma_a \end{cases}$ est un morphisme de groupes de noyau

$$\operatorname{Ker}\varphi = Z(G) = \{x \in G,\ \forall y \in G,\ x * y = y * x\}$$

En effet, pour tout $a \in G$,

$$a \in \operatorname{Ker} f \iff \sigma_a = \mathrm{Id} \iff \forall x \in G,\ a * x * a^{-1} = x \iff \forall x \in G,\ a * x = x * a$$

Exercice I.11.

Montrer que l'application

$$\varphi : \begin{cases} (G, *) & \longrightarrow (\mathrm{Bij}(G), \circ) \\ a & \longmapsto \gamma_a \end{cases}$$

où $\mathrm{Bij}(G)$ désigne l'ensemble des applications bijectives de l'ensemble G dans lui même, est un morphisme injectif de groupes.

Remarque : Cet exercice montre que tout groupe peut être vu comme un sous-groupe du groupe symetrique (groupe de permutations, eventuellement infini) et que donc si $|G| = n < \infty$, alors G peut être identifié à un sous-groupe de $\mathcal{S}_n$.

Notation : A partir de maintenant, lorsqu'il n'y a pas ambigüité, pour tout $a, b \in G$, nous noterons ab ou $a \cdot b$ au lieu de $a * b$.

Définition I.12.

Soit H un sous-groupe de G. On dit que H est distingué (ou normal) lorsque

$$\forall a \in G,\ \sigma_a(H) = aHa^{-1} \subset H$$

On note dans ce cas $H \trianglelefteq G$. Lorsque cette propriété est vérifiée, on a

$$\forall a \in G,\ aHa^{-1} = H \text{ et } aH = Ha$$

Remarque : Si G est abélien, alors tout sous-groupe $H \leq G$ est distingué.

Exemples

→ $\{e\}$ et G sont des sous-groupes distingués de G.

→ Si G' est un groupe, alors pour tout $f \in \mathrm{Hom}(G, G')$, $\operatorname{Ker} f$ est un sous-groupe distingué de G.

→ Plus généralement, si G' est un groupe, $H' \trianglelefteq G'$ et $f \in \mathrm{Hom}(G, G')$ alors $f^{-1}(H') \trianglelefteq G$.

→ Si G' est un groupe, $H \trianglelefteq G$ et $f \in \mathrm{Hom}(G, G')$ alors $f(H) \trianglelefteq \operatorname{Im} f = f(G)$.

Exercice I.13.

Soit H et K deux sous-groupes de G. Montrer les propositions suivantes.

1. $HK = KH \iff HK$ est un sous-groupe de G
2. Si H est un sous groupe distingué de G alors HK est un sous groupe de G.
3. $H \cap K = \{e\} \iff f : \begin{cases} H \times K & \longrightarrow HK \\ (h,k) & \longmapsto hk \end{cases}$ est bijective.
4. Montrer que si H et K sont distingués et $H \cap K = \{e\}$ alors $\forall (h,k) \in H \times K,\ hk = kh$.
5. Montrer que si $H \cap K = \{e\}$ et $\forall (h,k) \in H \times K,\ hk = kh$ alors f est un isomorphisme.

II Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \geq 2$. On note $\sim$ la relation d'équivalence sur $\mathbb{Z}$ définie par $a \sim b \iff n|a-b \iff a-b \in n\mathbb{Z}$. On note finalement $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'equivalences pour $\sim$. Une telle classe s'écrit $\overline{x} = x + n\mathbb{Z}$. Il est aisé de verifier que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\} = \{\overline{m}, \ldots, \overline{m+n-1}\}$ pour tout m et que ces n éléments sont distincts.

Proposition II.1.

Si X, Y sont deux classes dans $\mathbb{Z}/n\mathbb{Z}$ et $x \in X$, $y \in Y$, alors $\overline{x+y}$ ne dépend que de X et Y.

Remarque : La proposition ci-dessus permet donc de définir une loi $+$ sur $\mathbb{Z}/n\mathbb{Z}$ qui en en fait un groupe abélien.

Proposition II.2.

1. L'application $\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow \mathbb{U}_n \\ \overline{k} & \longmapsto e^{\frac{i2\pi k}{n}} \end{cases}$ est bien définie et est un isomorphisme.
2. L'application $\pi : \begin{cases} \mathbb{Z} & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto \overline{x} \end{cases}$ est un morphisme surjectif de noyau $Ker(\pi) = n\mathbb{Z}$

III Ordre d'un élément

Soit $a \in G$. Remarquons que $\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}$. Introduisons tout d'abord le morphisme suivant

$$j_a : \begin{cases} \mathbb{Z} & \longrightarrow \langle a \rangle \\ m & \longmapsto a^m \end{cases}$$

Pour tout $a \in G$, j_a est un morphisme de groupe surjectif. D'après la proposition I.9, $\operatorname{Ker} j_a$ est un sous groupe de $(\mathbb{Z}, +)$. Il est bien connu que les sous groupes de $\mathbb{Z}$ sont les groupes de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. Deux cas se présentent donc.

→ Si $n \neq 0$, alors $\operatorname{Ker} j_a = n\mathbb{Z}$. On note alors $\omega(a) = n$ et on dit que l'ordre de a est égal à n.

→ Sinon, $\operatorname{Ker} j_a = \{0\}$ et alors j_a est un isomorphisme. Dans ce cas, on note $\omega(a) = \infty$ et on dit que l'ordre de a est infini.

Remarque : Pour tout $a \in G$, on peut également définir $\omega(a)$ comme

$$\omega(a) = \min\{k \in \mathbb{N}^*,\ a^k = e\}$$

Proposition III.1.

Supposons que $\operatorname{Ker} j_a \neq \{0\}$ et posons $n = \omega(a)$. Les propositions suivantes sont vraies.

1. $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ et ces éléments sont distincts. De plus, $\forall k \in \mathbb{Z},\ a^k = e \iff n|k$.
2. $n = \min\{m \in \mathbb{N}^*,\ a^m = e\}$
3. $\forall m \in \mathbb{Z},\ \exists! k \in [\![0; n-1]\!],\ a^m = a^k$
4. $\forall k \in \mathbb{Z},\ \omega(a^k) = \dfrac{n}{n \wedge k}$
5. Si $q|n$ alors $\omega(a^q) = \dfrac{n}{q}$.

Preuve :

1. Montrons d'abord la deuxieme partie de ce point. Pour tout $k \in \mathbb{Z}$, on a

$$a^k = e \iff k \in \operatorname{Ker} j \iff k \in n\mathbb{Z} \iff n|k$$

   et en particulier $a^n = e$. Montrons ensuite que $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.
   - $\to$ ($\supset$) Cette inclusion est évidente.
   - $\to$ ($\subset$) Soit $k \in \mathbb{Z}$. Faisons la division euclidienne de k par n : $k = qn + b$ avec $b \in [\![0; n-1]\!]$. On a alors $a^k = (a^n)^k a^b = e^k a^b = a^b$. Ces éléments sont de plus distincts car si $i, j \in [\![0; n-1]\!]$ vérifient $a^i = a^j$ alors $a^{i-j} = e$ et donc $n|i-j$ d'où $i = j$.
2. D'après le point 1, $\forall k \in [\![1; n-1]\!]$ $a^k \neq e$ et $a^n = e$ d'où le résultat.
3. Ce point est une conséquence directe du point (1).
4. Soit $k, l \in \mathbb{Z}$. On a

$$(a^k)^l = e \iff a^{kl} = e \iff n|kl \iff \frac{n}{n \wedge k} \bigg| \frac{k}{n \wedge k} l \underset{\text{Gauß}}{\iff} \frac{n}{n \wedge k} \bigg| l$$

   L'avant dernière équivalence provient du fait que $\dfrac{k}{n \wedge k} \wedge \dfrac{n}{n \wedge k} = \dfrac{n \wedge k}{n \wedge k} = 1$.
   a^k étant clairement d'ordre fini, en utilisant le point 2, on a $\omega(a^k) = \min\{l \in \mathbb{N}^*\ (a^k)^l = e\} = \dfrac{n}{n \wedge k}$.
5. Ce point est une conséquence directe du point précédent.

IV Actions de morphismes

Proposition IV.1.

Soit G' un groupe d'élément neutre e', $a \in G$, et $f \in \operatorname{Hom}(G, G')$. Les propositions suivantes sont vraies.

1. Si $\omega(a) < \infty$, alors $\omega(f(a)) | \omega(a)$.
2. Si f est injective, alors $\omega(a) = \omega(f(a))$.
3. Si a et b sont deux éléments de G conjugués, i.e. il existe $c \in G$ tel que $a = cbc^{-1}$, alors $\omega(a) = \omega(b)$. En particulier, $\forall x, y \in G,\ \omega(xy) = \omega(yx)$.

Preuve :

1. Supposons que $\omega(a) < \infty$. On a $f(a)^{\omega(a)} = f(a^{\omega(a)}) = f(e) = e'$ et donc $\omega(f(a)) < \infty$ et $\omega(f(a))|\omega(a)$

2. Supposons que f est injective. Deux cas se présentent.

   → Si $\omega(a) = \infty$, alors il est facile de vérifier que $\langle f(a)\rangle = f(\langle a\rangle)$. f est injective et $\langle a\rangle$ est infini, donc $\langle f(a)\rangle$ aussi et donc en utilisant le point 1 de la proposition III.1, on voit qu'on ne peut pas avoir $\omega(a) < \infty$.

   → Si $\omega(a) = n \in \mathbb{N}^*$, alors

$$f(a)^k = e' \iff f(a^k) = f(e) \underset{f \text{ injective}}{\iff} a^k = e \iff \omega(a)|k$$

   On en déduit donc que $\omega(a)|\omega(f(a))$. En combinant ce résultat avec le point (1), on obtient bien que $\omega(a) = \omega(f(a))$.

3. Le fait que a et b soient conjugués se traduit par le fait qu'il existe $z \in G$ tel que $b = \sigma_z(a)$. σ_z est un morphisme injectif, donc en utilisant le point (2), on voit que $\omega(b) = \omega(\sigma_z(a)) = \omega(a)$. Enfin, pour montrer la deuxième partie de ce point, il suffit de voir que $xy = \sigma_x(yx)$.

Exercice IV.2.

Soit $m, n \geq 1$ tel que $m \wedge n = 1$. Déterminer $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

Exercice IV.3.

Soit $(a, b) \in G^2$ tels que $\omega(a) = m \leq \omega(b) = n < \infty$.

1. A-t-on $\omega(ab) < \infty$? *Indice : Penser aux symétries dans $\mathbb{R}^2$.*
2. Supposons que $ab = ba$ et $\omega(a) \wedge \omega(b) = 1$. Montrer que $\omega(ab) = mn$.
3. On suppose toujours que $ab = ba$. Montrer qu'il existe $c \in G$ tel que $\omega(c) = n \vee m$.
4. On suppose maintenant que G est abélien et fini. Montrer qu'il existe $z \in G$ tel que $\forall x \in G,\ \omega(x)|\omega(z)$. En particulier, on montrera l'existence de $z \in G$ tel que $\omega(z) = \displaystyle\bigvee_{x \in G} \omega(x)$.

Proposition (Théorème faible de Lagrange) IV.4.

Supposons que G est commutatif et soit $a \in G$. On a $\omega(a)|\,|G|$.

Preuve : On sait que γ_a est bijective, on a donc

$$\prod_{g \in G} g = \prod_{g \in G} \gamma_a(g) = \prod_{g \in G} (ag) = a^{|G|} \prod_{g \in G} g$$

En multipliant par l'inverse de $\displaystyle\prod_{g \in G} g$ on obtient que $a^{|G|} = e$, ce qui implique d'après la proposition III.1 que $\omega(a)|\,|G|$.

V Groupes cycliques

Définition V.1.

On dit que G est monogène s'il est engendré par un seul élément, i.e. il existe $a \in G$ tel que $G = \langle a \rangle$. Si de plus G est fini, alors on dit qu'il est cyclique.

Remarque V.2.

Supposons que G est monogène, i.e. qu'il existe $a \in G$ tel que $G = \langle a \rangle$. Deux cas se présentent.

1. Si $\omega(a) = \infty$, alors $j : \begin{cases} \mathbb{Z} & \longrightarrow \langle a \rangle \\ m & \longmapsto a^m \end{cases}$ est un isomorphisme.
2. Si $\omega(a) < \infty$, alors $G = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$ avec ces elements distincts. En particulier, on a $|G| = \omega(a)$.

Vocabulaire : Pour tout $a \in G$, lorsque $G = \langle a \rangle$, on dit que a est un élément générateur de G.

Proposition V.3.

Soit $n \in \mathbb{N}^*$. G est cyclique de cardinal n si et seulement si G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De plus, si $\psi : (G, *) \longrightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ et $b \in G$ un générateur de G, i.e. $G = \langle b \rangle$, alors $\psi(b) = \overline{1}$ implique que ψ est un isomorphisme.

Preuve : Montrons tout d'abord l'équivalence.

→ ($\Leftarrow$) Cette implication est facile à montrer.

→ ($\Rightarrow$) Supposons que G est cyclique de cardinal fini égal à n. Il existe donc $a \in G$ tel que $G = \{e, a, \dots, a^{n-1}\}$. Considérons le morphisme de groupe suivant

$$\psi : \begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow (G, *) \\ \overline{k} & \longmapsto a^k \end{cases}$$

On peut facilement montrer que ψ est bien défini et bijectif et alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.
Le dernier point de la proposition découle directement du raisonnement effectué ci-dessus.

Exercice V.4.

Supposons que G est cyclique d'ordre (de cardinal) n et soit a un générateur de G. Soit H un sous groupe de G. Posons $d = |H|$. Montrer que $H = \left\langle a^{\frac{n}{d}} \right\rangle$.

Remarque : Cette remarque peut être très utile dans quelques exercices difficiles. Soit $n \geq 1$. L'ensemble $D_n = \{k \geq 1\ k|n\}$ vérifie $|D_n| \leq 2\sqrt{n} + 1$. En effet, l'application

$$\varphi : \begin{cases} D_n \cap [\![1; \lfloor \sqrt{n} \rfloor]\!] & \longrightarrow D_n \cap [\![\lfloor \sqrt{n} \rfloor; n]\!] \\ d & \longmapsto \dfrac{n}{d} \end{cases}$$

est une bijection et donc

$$\begin{aligned}|D_n| &= \left|D_n \cap [\![1;\lfloor\sqrt{n}\rfloor]\!]\right| + \left|D_n \cap [\![1+\lfloor\sqrt{n}\rfloor;n]\!]\right| \\ &\leq \left|D_n \cap [\![1;\lfloor\sqrt{n}\rfloor]\!]\right| + \left|D_n \cap [\![\lfloor\sqrt{n}\rfloor;n]\!]\right| + 1 \\ &= 2\left|D_n \cap [\![1;\lfloor\sqrt{n}\rfloor]\!]\right| + 1 \leq 2\sqrt{n}+1\end{aligned}$$

Exercice V.5.

Supposons que G est cyclique et posons $|G| = n \geq 2$ et soit a un générateur de G.

1. Montrer que pour tout $k \in \mathbb{Z}$, a^k génère G si et seulement si $k \wedge n = 1$.
2. Posons $\varphi(n) = |\{k \in [\![1;n]\!] \; k \wedge n = 1\}|$. Cette application est nommée l'indicatrice d'Euler. En utilisant la question précédente, montrer que $\sum\limits_{d|n\; d\geq 1} \varphi(d) = n$.

Exercice V.6.

1. Soit $(G_1, *)$ et $(G_2, \diamondsuit)$ deux groupes cycliques. On considère la loi de composition intnerne $\otimes : G_1 \times G_2 \longrightarrow G_1 \times G_2$ définie par

$$\forall (g_1, g_2, g_1', g_2') \in G_1 \times G_2 \times G_1 \times G_2,\; (g_1, g_2) \otimes (g_1', g_2') = (g_1 * g_1',\; g_2 \diamondsuit g_2')$$

   Trouver une condition nécessaire et suffisante pour que $(G_1 \times G_2, \otimes)$ soit cyclique.
2. (Théorème des restes chinois) Soit $a, b \geq 2$. Montrer que $\varphi : \begin{cases} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \overline{x} & \longmapsto (\overline{x}, \overline{x}) \end{cases}$ est bien définie puis que φ est un isomorphisme si et seulement si $a \wedge b = 1$.

Exercice V.7.

Soit A un anneau commutatif unitaire.

1. Soit $P, Q \in A[X]$ avec Q de coefficient dominant égal à 1 (i.e. $Q = 1$ ou Q est unitaire) (ici, on désigne par 1 l'élément neutre pour la multiplication de l'anneau A).
   Montrer que l'on peut effectuer "la" division euclidienne de P par Q
2. On suppose que A est intègre et $\deg P \geq 0$. Montrer que P possède au plus $\deg P$ racines distinctes
3. Soit $(\mathbb{K}, +, \times)$ un corps et $(G, \times)$ un sous-groupe fini de $(\mathbb{K}^*, \times)$, où $\mathbb{K}^*$ est l'ensemble des éléments de $\mathbb{K}$ inversible pour la loi $\times$. Montrer que G est cyclique.

Remarque à propos de l'exercice V.7 : La question 1 demande montrer que lorsqu'un polynôme $Q \in A[X]$ est de coefficient dominant égal à 1, on peut effectuer la division euclidienne de tout polynôme $P \in A[X]$ par Q. Ce résultat est aussi vrai lorsque le coefficient dominant de Q est inversible, mais devient faux lorsque ce n'est pas le cas. Lorsque A est un corps, tous les éléments de A sauf 0 sont inversibles, on peut donc toujours effectuer la division euclidienne par un polynôme non nul.

VI Groupe engendré par une partie

Proposition VI.1.

Pour tout $A \subset G$, il existe un plus petit sous-groupe $\langle A \rangle$ de G contenant A appelé sous-groupe engendré par A. De plus, on a

$$\langle A \rangle = \bigcap_{H \leq G \ A \subset H} H = \{a_1^{\alpha_1} \dots a_n^{\alpha_n},\ n \in \mathbb{N},\ a_1, \dots, a_n \in A,\ \alpha_1, \dots, \alpha_n \in \mathbb{Z}\}$$

Preuve : L'existence et la première égalité ont déjà étés établis à la proposition I.6. Montrons la seconde égalité, i.e.

$$\langle A \rangle = \underbrace{\{a_1^{\alpha_1} \dots a_n^{\alpha_n},\ n \in \mathbb{N},\ a_1, \dots, a_n \in A,\ \alpha_1, \dots, \alpha_n \in \mathbb{Z}\}}_{B}$$

Il est facile de montrer que B est bien un sous-groupe de G contenant A. On en déduit donc que $\langle A \rangle \subset B$. Montrons l'inclusion réciproque. Pour tout $n \in \mathbb{N}$ $a_1, \dots, a_n \in A \subset \langle A \rangle$ et $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$, par stabilité, on a $a_1^{\alpha_1} \dots a_n^{\alpha_n} \in \langle A \rangle$, d'où l'égalité voulue.

Vocabulaire : On dit que $S \neq \varnothing$ est générateur (de G) si $G = \langle S \rangle$

Exemple : $(\mathcal{S}_n, \circ)$ est généré par les transposition de la forme $(i\ i+1)$, i.e.

$$\mathcal{S}_n = \langle \{(i\ i+1),\ i \in [\![1; n-1]\!]\} \rangle$$

Exercice VI.2.

Supposons que $(G, *)$ soit un groupe fini abélien et soit p un nombre premier tel que $\forall g \in G,\ \omega(g) | p$ (ou d'une manière équivalente, $\forall g \in G,\ g^p = e$). Montrer qu'il existe $n \in \mathbb{N}$ tel que $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Exercice VI.3.

Soit $H \neq \{e\}$ un groupe où e est son élément neutre. Notons $\mathbb{P}$ l'ensemble des nombres premiers. On pose $\mathrm{Sg}(H)$ l'ensemble des sous-groupes de H. Montrer que les propositions suivantes sont équivalentes.

1. $\mathrm{Sg}(H) = \{\{e\}, H\}$
2. $\exists p \in \mathbb{P},\ H \simeq \mathbb{Z}/p\mathbb{Z}$
3. $\forall g \in H \setminus \{e\},\ \langle g \rangle = H$
4. $\exists p \in \mathbb{P},\ |H| = p$

VII Compléments

1. Classes latérales et groupe quotient

Proposition VII.1.

Soit H un sous groupe de G. La relation $\sim_g$ sur G^2 définie par

$$\forall a, b \in G,\ a \sim_g b \Longleftrightarrow b \in aH$$

est une relation d'équivalence. La classe d'équivalence de a pour $\sim_g$ est aH et est appelée classe à gauche selon H de a. On note cette classe $\overline{a}$.

Remarque :

→ En fait, on peut également définir la même notion d'équivalence à droite $\sim_d$ par $a \sim_d b \Longleftrightarrow b \in Ha$. Ces deux relations sont les mêmes si et seulement si H est distingué. Dans ce cas, on la notera simplement $\sim$. Nous discuterons un peu plus de cette notion d'équivalence à droite et à gauche dans les compléments de ce chapitre.

→ Une manière équivalente de définir cette relation est

$$a \sim_g b \Longleftrightarrow b^{-1}a \in H \text{ et } a \sim_d b \Longleftrightarrow ab^{-1} \in H$$

Définition et Proposition VII.2.

Soit H un sous-groupe distingué de G. Les propriétés suivantes sont vraies.

1. Le produit de deux classes à gauche selon H est une classe à gauche selon H.
2. Pour ce produit, l'ensemble des classes à gauche selon H forme un groupe, noté G/H.
3. Pour tout $a, b \in G$, $\gamma_{ba^{-1}}$ est une bijection entre aH et bH et par conséquent lorsque H est fini, $\forall a \in G,\ |aH| = |H|$, i.e. toute classe à gauche selon H est en bijection avec H.
4. L'élément neutre de G/H est H (ou d'une manière équivalente $\overline{e}$).

Preuve :

1. Pour tout $a, b \in G$, on a $aH * bH = a * b * H * H = abH$.
2. Il suffit d'appliquer la définition d'un groupe pour démontrer ce point.
3. Remarquons que
   - $\gamma_{ba^{-1}}(aH) \subset bH$ et $\gamma_{ab^{-1}}(bH) \subset aH$
   - L'application $\gamma_{ab^{-1}} : bH \longrightarrow aH$ est un inverse (et donc l'unique inverse) de $\gamma_{ba^{-1}}$ et donc $\gamma_{ba^{-1}}$ est bijective

   Par conséquent, pour tout $a, b \in G$, $|aH| = |bH|$ et en particulier $|aH| = |eH| = |H|$.
4. $H = \overline{e}$ donc pour tout $a \in G$, $\overline{ea} = \overline{ae} = \overline{a}$ donc H est bien l'élément neutre de G/H.

Remarque :

→ Pour bien comprendre cette notion de groupe quotient, il faut voir que pour tout $a \in G$, la classe $\overline{a}$ comme une sorte d'ensemble d'éléments de même "reste" que a dans G pour une certaine "division". Lorsque $*$ est additive, on peut faire l'analogie avec $\mathbb{Z}/n\mathbb{Z}$. En effet, $(n\mathbb{Z}, +) \trianglelefteq (\mathbb{Z}, +)$ et le groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$ est tout simplement égal au groupe bien connu $\mathbb{Z}/n\mathbb{Z}$. Dans ce cas, lorsque $+$ est additive, en pensant à cet exemple, on peut voir les classes $\overline{a} = a + H$ comme l'ensemble des éléments de même "restes" que a "modulo H". Dans l'exemple de $\mathbb{Z}/n\mathbb{Z}$, on a bien entendu $H = n\mathbb{Z}$.

→ L'égalité $|H| = |aH| = |Ha|$ reste vraie même si H n'est pas distingué dans G.

Notation : Même lorsque H est un sous-groupe non distingué de G, on notera G/H l'ensemble des classes à gauche de G selon H, i.e. l'ensemble $\{\overline{g},\ g \in G\} = \{gH,\ g \in G\}$. Dans ce cas, G/H n'est pas un groupe, car lorsque G est non abélien, le produit de deux classes à gauche n'est pas forcément une classe à gauche. De la même manière, on notera par $H\backslash G$ l'ensemble des classes à droite de G selon H i.e. l'ensemble $\{Hg,\ g \in G\}$.

Proposition VII.3.

Soit H un sous-groupe distingué de G. Les proposition suivantes sont vraies.

1. L'application $\pi : \begin{cases} G & \longrightarrow G/H \\ a & \mapsto aH \end{cases}$ est un morphisme surjectif de noyau $\operatorname{Ker}\pi = H$. On l'appelera la surjection canonique.
2. Soit G' un groupe et $f \in \operatorname{Hom}(G, G')$. Il existe $\tilde{f} \in \operatorname{Hom}(G/\operatorname{Ker} f, G')$ injective d'image $\operatorname{Im} f$ tel que $f = \tilde{f} \circ \pi$. En particulier, $G/\operatorname{Ker} f$ est isomorphe à $\operatorname{Im} f$.

Preuve :

1. C'est clairement un morphisme par ce qui précède. Soit $a \in \operatorname{Ker}\pi$. On a $aH = H$, il existe donc $g \in H$ tels que $ae = g$, i.e. $a = g \in H$. On en déduit donc que $\operatorname{Ker}\pi \subset H$. L'implication réciproque est évidente.
2. Posons $H = \operatorname{Ker} f$ et considérons l'application

$$\tilde{f} : \begin{cases} G/H & \longrightarrow G' \\ aH & \longmapsto f(a) \end{cases}$$

Cette application est bien définie (elle est indépendante du représentant), est clairement un morphisme et est injective. En effet, pour tout $U \in \operatorname{Ker}\tilde{f}$, il existe $a \in G$ tels que $U = aH$. On a alors

$$\tilde{f}(U) = e' \iff \tilde{f}(aH) = e' \iff f(a) = e' \iff a \in \operatorname{Ker} f \iff aH = H$$

et donc $\operatorname{Ker}\tilde{f} = \{H\}$, et H est l'élément neutre de G/H. On en déduit donc que $\tilde{f}$ induit un isomorphisme entre G/H et $\operatorname{Im} f$ et que en particulier $G/\operatorname{Ker} f$ et $\operatorname{Im} f$ sont isomorphes.

Théorème (Théorème de Lagrange) VII.4.

Supposons que G est fini. Soit H un sous groupe de G. On a $|H| \mid |G|$.

Preuve : Les classes à gauche selon H, $\{aH,\ a \in G\}$, sont disjointes et en nombre fini. Il existe donc $p \in \mathbb{N}^*$ et $a_1, \ldots, a_p \in G$ tels que $G = \bigsqcup_{k=1}^{p} a_k H$. Cette union étant disjointe et d'après la proposition VII.1 tous ces ensembles sont de même cardinal égal à $|H|$, on peut écrire

$$|G| = \left|\bigsqcup_{k=1}^{p} a_k H\right| = \sum_{k=1}^{p} |a_k H| = p\,|H|$$

et alors finalement $|H| \mid |G|$.

Remarques :

→ Avec ce théorème, on aurait pu facilement montrer la proposition IV.4. En effet, pour tout $a \in G$, $\langle a \rangle$ est un sous-groupe de G, donc d'après le théorème de Lagrange, on a $|\langle a \rangle| \mid |G|$. D'après la proposition III.1, on a $|\langle a \rangle| = \omega(a)$, ce qui permet de conclure.

→ En rejetant un coup d'oeil à la preuve du théorème, il est facile de voir que lorsque H est un sous-groupe de G avec G fini, alors $|G| = |G/H| \times |H|$ et par conséquent $|G/H| = |G| / |H|$.

On notera $[G : H] := |G/H|$ qu'on nommera l'indice de H dans G. Ce dernier peut être défini même si G est infini et que, si G est fini, on obtient $|G : H] = |G|/|H|$.

Exercice VII.5.

Soit p, q deux nombres premiers distincts et $(H, *)$ un groupe abélien tel que $|H| = pq$. Montrer que $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Exercice VII.6.

Supposons que G est un groupe fini et H un sous-groupe de G d'indice $[G : H] = 2$ i.e. $|G| = 2|H|$. Montrer que H est un sous groupe distingué de G et que donc H contient tous les carrés.

2. Actions de groupes

Dans cette partie, on considère X un ensemble non vide.

Définition VII.7.

Une action de groupe (à gauche) est une application $\bullet : G \times X \to X$, telle que

→ $\forall x \in X,\ e \bullet x = x$

→ $\forall g, h \in G\ \forall x \in X\ (gh) \bullet x = g \bullet (h \bullet x)$

Remarque : On peut également définir les actions de groupe d'une autre manière. En effet, en considérant $\phi : G \longrightarrow \mathrm{Bij}(X)$ un morphisme de groupe de $(G, *)$ dans $(\mathrm{Bij}(X), \circ)$, pour tout $g \in G$ et $x \in X$, on peut remplacer $g \bullet x$ par $\phi(g)(x)$.

Exemples :

→ Lorsque $X = G$, $\phi_1 : (g, h) \longmapsto \gamma_g(h)$ $(g \bullet h = \gamma_g(h))$ et $\phi_2 : (g, h) \longmapsto \sigma_g(h)$ $(g \bullet h = \sigma_g(h))$ sont des actions de groupe. ϕ_1 est appelée action de translation à gauche et ϕ_2 est appelée action de conjugaison.

→ $\phi_3 : (g, h) \longmapsto \delta_g(h)$ une action de groupe seulement si G est abélien.

Définition VII.8.

Soit $x \in X$.

→ L'ensemble $O(x) = \{g \bullet x,\ g \in G\}$ est appelé orbite de x.

→ L'ensemble $\mathrm{Stab}(x) = \{g \in G,\ g \bullet x = x\}$ est appelé stabilisateur de x.

Proposition VII.9.

Soit $\bullet : G \times X \longmapsto X$ une action de groupe. Les propositions suivantes sont vraies.

1. Pour tous $x, y \in X$, on a $O(x) \cap O(y) = \varnothing$ ou $O(x) = O(y)$. De plus, on a $X = \bigcup_{x \in X} O(x)$.
2. Pour tout $x \in X$, $\text{Stab}(x)$ est un sous-groupe de G. De plus, on a l'implication suivante pour tout $y \in X$
$$y = g \bullet x \Longrightarrow \text{Stab}(y) = g\text{Stab}(x)g^{-1} = \sigma_g(\text{Stab}(x))$$
3. Soit $x \in X$. L'application $\phi_x : \begin{cases} G/\text{Stab}(x) & \longrightarrow O(x) \\ \overline{g} & \longmapsto g \bullet x \end{cases}$ est bien définie et est une bijection. En particulier, si G est fini, $|G/\text{Stab}(x)| = |G|/|\text{Stab}(x)| = |O(x)|$.
4. (Fomule des classes) Supposons G et X sont finis et soit $k \in \mathbb{N}^*$ et $(x_i)_{i \in [\![1;k]\!]}$ un système de représentants des orbites de G i.e. $X = \bigsqcup_{i \in [\![1;k]\!]} O(x_i)$ et pour tout $i, j \in [\![1;k]\!]$ différents, $O(x_i) \neq O(x_j)$. On a $|X| = \sum_{i \in [\![1;k]\!]} |O(x_i)| = \sum_{i \in [\![1;k]\!]} \frac{|G|}{|\text{Stab}(x_i)|}$.

Preuve :

1. Soit $\sim$ la relation sur X^2 définie par $\forall x, y \in X,\ x \sim y \Longleftrightarrow y \in O(x)$. Montrons que la relation $\sim$ est une relation d'équivalence.
   - $\rightarrow$ Réflexivité : on a pour tout $x \in X$, $e \bullet x = x$ donc $x \in O(x)$ et alors $x \sim x$.
   - $\rightarrow$ Symétrie : soit $x, y \in X$. Supposons que $x \sim y$. On dispose donc de $g \in G$ tel que $g \bullet x = y$. On a alors $g^{-1} \bullet y = g^{-1} \bullet g \bullet x = x$ et alors $x \in O(y)$, i.e. $y \sim x$.
   - $\rightarrow$ Transitivité : soit $x, y, z \in X$ tels que $x \sim y$ et $y \sim z$. Il existe donc $g, h \in G$ tels que $g \bullet x = y$ et $h \bullet y = z$ et alors $g \bullet h \bullet x = z$. On en déduit donc que $gh \bullet x = z$ et donc $z \in O(x)$, i.e. $x \sim z$.

   On peut également facilement voir que pour tout $x \in X$, $O(x)$ est la classe d'équivalence de x pour $\sim$. On peut donc partitionner X en classes d'équivalences pour $\sim$, i.e. pour tout $x, y \in X$, on a $O(x) \cap O(y) = \varnothing$ ou $O(x) = O(y)$ et $X = \bigcup_{x \in X} O(x)$.
2. Soit $x \in X$. La preuve du fait que $\text{Stab}(x)$ est un sous-groupe de G ne présente pas de difficulté et est donc laissé comme exercice au lecteur. Soit $y \in G$ et $h \in G$, on a alors
$$\begin{aligned} h \in \text{Stab}(y) &\Longleftrightarrow h \in \text{Stab}(g \bullet x) \Longleftrightarrow h \bullet (g \bullet x) = g \bullet x \\ &\Longleftrightarrow (g^{-1}hg) \bullet x = x \Longleftrightarrow g^{-1}hg \in \text{Stab}(x) \\ &\Longleftrightarrow h \in g\text{Stab}(x)g^{-1} \end{aligned}$$
   Et donc $\text{Stab}(g \bullet x) = g\text{Stab}(x)g^{-1}$
3. D'abord ϕ_x est clairement bien définie (indépendante du représentant). Montrons que ϕ_x est injective. Soit $g, h \in G$ On a
$$\begin{aligned} \phi_x(\overline{g}) = \phi_x(\overline{h}) &\Longrightarrow g \bullet x = h \bullet x \Longrightarrow (g^{-1}h) \bullet x = x \\ &\Longrightarrow g^{-1}h \in \text{Stab}(x) \Longrightarrow h \in g\text{Stab}(x) \\ &\Longrightarrow h \in \overline{g} \Longrightarrow \overline{h} = \overline{g} \end{aligned}$$
   Donc ϕ_x est bien injective. Elle est de plus clairement surjective par définition de $O(x)$, ce qui nous permet de conclure qu'elle est bien bijective.

4. On sait d'après le point (1) que les ensembles $(O(x_i))_{i\in[\![1;k]\!]}$ sont dijoints. De plus, d'après le point 3, pour tout $x \in X$, $G/\text{Stab}(x)$ est en bijection avec $O(x)$, i.e. $|G/\text{Stab}(x)| = |O(x)|$. On en déduit donc que
$$|X| = \left|\bigsqcup_{i\in[\![1;k]\!]} O(x_i)\right| = \sum_{i=1}^{k} |O(x_i)| = \sum_{i=1}^{k} |G/\text{Stab}(x_i)| = \sum_{i=1}^{k} \frac{|G|}{|\text{Stab}(x_i)|}$$

Exercice VII.10.

Soit G un groupe fini et $H \leq G$ tel que $[G : H] = p$ où p est le plus petit premier qui divise l'ordre de G. Montrer que $H \trianglelefteq G$ et que donc H contient toutes les puissances $p-$emes

3. Application : action de conjugaison

Cette section traite le cas particulier de l'action par conjugaison/automorphisme intérieur sur G fini
$$\bullet : \begin{cases} G \times G & \longrightarrow G \\ (g, a) & \longmapsto gag^{-1} \end{cases}$$

Définition VII.11.

Soit $a \in G$.

→ L'ensemble $O(a) = \{xax^{-1},\ x \in G\}$ est appelé orbite de a.

→ L'ensemble $C(a) = \{x \in G,\ xa = ax\} = \{x \in G,\ xax^{-1} = a\} = \text{Stab}(a)$ est appelé commutant de a. Il s'agit de l'ensemble des éléments de G qui commutent avec a.

Remarque : Pour tout $a \in G$, on a $a \in Z(G) \iff C(a) = G \iff O(a) = \{a\}$.

Proposition VII.12.

Soit $a \in G$. Les proposition suivantes sont vraies.

1. $C(a)$ est un sous-groupe de G et $|G/C(a)| = |O(a)|$.
2. $|G| = |C(a)| \times |O(a)|$
3. (Formule des classes) Soit R un ensemble de représentants des classes de conjugaison (ou des orbites) non réduites à un singleton et R' les représentants des orbites réduits à un singleton (i.e. les éléments qui commutent avec touts les éléments de G), alors
$$|G| = \sum_{x\in R'} |O(x)| + \sum_{x\in R} |O(x)| = |Z(G)| + \sum_{x\in R} \frac{|G|}{|C(x)|}$$

Preuve : Les preuves de ces résultats sont des applications directes de la proposition VII.9.

L'exercice suivant est une application de la proposition ci-dessus.

Exercice VII.13.

Soit $n \in \mathbb{N}^*$ et p un nombre premier. On suppose que $|G| = p^n$. Montrer que le centre de G, $Z(G)$, n'est pas réduit à un singleton. En particulier, si $n \leq 2$ alors G est abélien

Le théorème suivant est également une application de la proposition ci-dessus.

Théorème (Théorème de Cauchy) VII.14.

Supposons que G est fini et soit p un nombre premier tel que $p||G|$. Il existe $x \in G,\ \omega(x) = p$.

Preuve : Posons $n = |G|$ et considérons l'ensemble $E = \{(x_1, \dots, x_p) \in G^p\ x_1 \dots x_p = e\}$. Il est aisé de voir que

$$\begin{aligned}|E| &= |\{(x_1, \dots, x_p) \in G^p\ x_1 \dots x_p = e\}| \\ &= \left|\{(x_1, \dots, x_{p-1}, x_{p-1}^{-1} \dots x_1^{-1}),\ (x_1, \dots, x_{p-1}) \in G^{p-1}\}\right| = \left|G^{p-1}\right|\end{aligned}$$

et alors $|E| = n^{p-1}$. Considérons l'action de groupe de permutation circulaire sur E

$$\bullet : \begin{cases} \mathbb{Z}/p\mathbb{Z} \times E & \longrightarrow E \\ (\overline{k}, (x_1, \dots, x_p)) & \longmapsto (x_{\sigma^k(1)}, \dots x_{\sigma^k(p)}) \end{cases}$$

où $\sigma = (1\ 2\ \dots\ p)$. On notera par abus de notation $k \bullet x$ au lieu de $\overline{k} \bullet x$ (remarquer au passage que ce n'est pas vraiment un abus de notation vu que c'est plutôt l'action de $\mathbb{Z}$ qui est court-circuitée par $\mathbb{Z}/p\mathbb{Z}$). Remarquons que pour tout $k, l \in \mathbb{Z},\ k \bullet (l \bullet x) = (k + l) \bullet x$. S'il existe $k \in \mathbb{Z}$ tel que $\overline{k} \neq \overline{0}$ et $k \bullet x = x$, alors d'après Bezout, étant donné que k est premier avec p, il existe $u, v \in \mathbb{Z}$ tels que $uk + vp = 1$ et alors, en supposant sans perte de généralité que $u \geq 0$ et $v \leq 0$

$$1 \bullet x = (uk + vp) \bullet x = vp \bullet (uk \bullet x) = \underbrace{-p \bullet \dots \bullet -p}_{-v \text{ fois}} \bullet \underbrace{k \bullet \dots \bullet k}_{u \text{ fois}} \bullet x = x$$

Le fait que $1 \bullet x = x$ est équivalent à $(x_1, x_2, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$ i.e.

$$x_1 = x_2,\ x_2 = x_3,\ \dots,\ x_{p-1} = x_p$$

et alors pour tout $k \in \mathbb{Z},\ k \bullet x = x$ i.e. $O(x)$ ne contient qu'un seul élément. On en déduit que pour tout $x \in E$, deux cas sont possibles : $\forall k, l \in \mathbb{Z},\ k \bullet x \neq l \bullet x$ et alors $O(x)$ contient p éléments, ou alors $\forall k \in \mathbb{Z},\ k \bullet x = x$ et donc $O(x)$ contient un seul élément. En posant S_1 l'ensemble des orbites à un seul élément et S_2 l'ensemble des orbites à p éléments, le fait que E est union disjointe des orbites de l'action de groupe $\bullet$ nous permet de dire que

$$|G|^{p-1} = |E| = \left|\bigcup_{X \in S_1} X\right| + \left|\bigcup_{X \in S_2} X\right| = |S_1| + p\,|S_2|$$

p divise $|G|$, donc p divise aussi $|S_1| = |K|$. $O((e, \dots, e)) \in S_1$ et $p \geq 2$ donc $|K| = |S_1| \geq 2$. Il existe donc $x \in E \setminus \{e\}$ tel que $x^p = e$.

Lorsque G est abélien, on dispose d'une preuve plus rapide.

Exercice (Inspiré du TD d'Alain Troesh) VII.15.

Supposons que G est un groupe abélien fini et soit p un nombre premier.

1. Soit K un sous groupe distingué de G. Montrer que s'il existe $x \in G/K$ d'ordre p alors il en existe un aussi d'ordre p dans G.
2. On suppose que $p||G|$, montrer qu'il existe $x \in G,\ \omega(x) = p$.
3. Soit $a \geq 1$. On suppose que $p^a||G|$. Montrer que $\exists H \leq G$ d'ordre p^a
4. Soit H et L deux sous groupes de G tels que $|H| \wedge |L| = 1$. G est commutatif, donc HL est un sous-groupe de G. Considérons le morphisme de groupes

$$\psi : \begin{cases} H \times L & \longrightarrow HL \\ (h, l) & \longmapsto hl \end{cases}$$

   Montrer que ψ est bijectif et en déduire que $|HL| = |H| \times |L|$.
5. En déduire que pour tout $n \in \mathbb{N}^*$, si $n||G|$, alors il existe H un sous groupe de G tel que $|H| = n$.

Correction de l'exercice I.2. :

Soit e' l'élément neutre de H. Pour tout $a \in H$, on note a_g^{-1} un inverse à gauche de a, i.e. un élément de H tel que $a_g^{-1}a = e'$. Soit $a \in H$. On a

$$a_g^{-1}aa_g^{-1} = e'a_g^{-1} = a_g^{-1}$$

On a donc

$$a \cdot a_g^{-1} = e' \cdot a \cdot a_g^{-1} = (a_g^{-1})_g^{-1}a_g^{-1} \cdot a \cdot a_g^{-1} = (a_g^{-1})_g^{-1}a_g^{-1} = e'$$

a admet donc aussi un inverse à droite qui est forcément le même qu'à gauche et donc H est un groupe.

Correction de l'exercice I.7. :

→ ($\Rightarrow$) Cette implication est évidente.

→ ($\Leftarrow$) $*$ est associative sur H, il faut donc simplement vérifier l'existence de l'inverse dans H et l'élément neutre. Soit $a \in H$. H étant fini, on dispose de $i, j \in \mathbb{N}$ tels que $1 \leq i < j$ et $a^i = a^j$. Si $j = i+1$ alors $a = e$ et donc $a^{-1} = e \in H$. Sinon, $j \geq i+2$ et donc $b = a^{j-i-1} \in H$. Montrons que $b = a^{-1}$. On a

$$ba = a^{j-i-1}a = a^{j-i} = e = aa^{j-i-1} = ab$$

donc tout élément de H admet un inverse dans H pour $*$. L'existence de l'élément neutre vient simplement du fait que si $a \in H$, alors $a^{-1} \in H$ et alors $e = a * a^{-1} \in H$.

Correction de l'exercice I.11. :

Le fait que ce soit un morphisme est clair. En effet, pour tout $a, b \in G$ et $x \in G$, on a

$$\varphi(a*b)(x) = \gamma_{a*b}(x) = a*b*x = \gamma_a \circ \gamma_b(x) = \varphi(a) \circ \varphi(b)(x)$$

et alors $\varphi(a*b) = \varphi(a) \circ \varphi(b)$.

Montrons à présent que φ est injective. Pour cela, on va montrer que $\operatorname{Ker}\varphi = \{\mathrm{Id}\}$. Soit $a \in \operatorname{Ker}\varphi$. On a $\varphi(a)(e) = e$ et donc $a \cdot e = e$ d'où $a = e$ et alors $\operatorname{Ker}\varphi = \{e\}$.

Remarque : Le seul élément a de G tel que γ_a admet un point fixe est e.

Correction de l'exercice I.13. :

1. Montrons cette proposition par double implication.

   → ($\Rightarrow$) Supposons que HK est un sous-groupe de G. On a alors

   $$HK \underset{HK \leq G}{=} (HK)^{-1} = K^{-1}H^{-1} \underset{H \text{ et } K \leq G}{=} KH$$

   La première égalité est due au fait qu'étant donné que HK est un sous-groupe de G, alors l'application $i : \begin{cases} HK & \longrightarrow HK \\ x & \longmapsto x^{-1} \end{cases}$ est bijective.

   → ($\Rightarrow$) Supposons que $HK = KH$ utilisons la proposition $I.4$ pour montrer que HK est un sous-groupe de G. $HK \neq \varnothing$ il suffit donc de vérifier que

   $$\forall (h, k, h', k') \in H \times K \times H \times K,\ (hk)(h'k')^{-1} \in HK$$

   Méthode 1 (Rapide) : On a pour tout $(h, k, h', k') \in H \times K \times H \times K$,

   $$(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1} \underset{K \leq G}{\in} hKh'^{-1} \underset{H \leq G}{\subset} HKH \underset{HK=KH}{=} HHK \underset{H \leq G}{=} HK$$

Méthode 2 (Même chose mais en plus détaillé) : Soit $(h,k,h',k') \in H \times K \times H \times K$. On a $(hk)(h'k')^{-1} = \underbrace{hkk'^{-1}}_{\in HK=KH} h'^{-1}$. Il existe donc $(h'',k'') \in H \times K$ tel que $hkk'^{-1} = k''h''$, et alors on peut écrire $(hk)(h'k')^{-1} = k''h''h' \in KH = HK$.

2. Supposons que H est un sous-groupe distingué de G. Deux méthodes sont possibles.
   - → **Méthode 1 :** On a pour tout $(h,k,h',k') \in H \times K \times H \times K$, $(hk)(h'k') = hkh'k' = hkh'k^{-1}kk'$. H est un sous-groupe distingué de G, donc $kh'k^{-1} \in H$. Il existe donc $h'' \in H$ tel que $kh'k^{-1}$. On a donc $(hk)(h'k') = hh'''k' \in HK$. De plus, HK est non vide, donc d'après l'exercice I.7, HK est bien un sous-groupe de G.
   - → **Méthode 2 :** En utilisant la proposition VII.1, on peut écrire
   $$HK = \bigcup_{k\in K} Hk \underset{H \trianglelefteq G}{=} \bigcup_{k \in K} kH = KH$$
3. Montrons le résultat par double implication.
   - → $(\Leftarrow)$ Soit $x \in H \cap K$. On a $f(x,e) = x = f(e,x)$ et donc, par injectivité, $x = e$.
   - → $(\Rightarrow)$ Supposons que $H \cap K = \{e\}$. f est surjective par définition. Soit $(h,k,h',k') \in H \times K \times H \times K$. On a
   $$f(h,k) = f(h',k') \iff hk = h'k' \iff h'^{-1}h = k'k^{-1} \underset{H\cap K=\{e\}}{=} e \iff h = h' \text{ et } k = k'$$
   donc f est bijective.
   Remarque : Si les éléments de H et K ne commutaient pas entre eux, f ne serait pas forcément un morphisme.
4. Supposons que H et K sont des sous-groupes distingués de G et que $H \cap K = \{e\}$. Pour tout $(h,k,h',k') \in H \times K \times H \times K$, on a
$$hkh^{-1}k^{-1} \in hKh^{-1}k^{-1} \cap hkHk^{-1} \underset{H \text{ et } K \trianglelefteq G}{=} Kk^{-1} \cap hH \underset{H \text{ et } K \leq G}{=} K \cap H = \{e\}$$
et donc $hk = kh$
5. Supposons que les éléments de H et K commutent entre eux et que $H \cap K = \{e\}$. D'après la question 3, f est bijective. De plus, f est un morphisme (facile à vérifier) et donc un isomorphisme.

Correction de l'exercice IV.2. :

Notons $\overline{1}_{\mathbb{Z}/m\mathbb{Z}}$ la classe de 1 dans $\mathbb{Z}/m\mathbb{Z}$. Soit $f \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. On sait que $f(\overline{1}_{\mathbb{Z}/m\mathbb{Z}}) \in \mathbb{Z}/n\mathbb{Z}$ et donc $nf(\overline{1}_{\mathbb{Z}/m\mathbb{Z}}) = 0$. En particulier, $\omega(f(\overline{1}_{\mathbb{Z}/m\mathbb{Z}}))|n$. De même, $\omega(f(\overline{1}_{\mathbb{Z}/m\mathbb{Z}}))|\omega(\overline{1}_{\mathbb{Z}/m\mathbb{Z}}) = m$ et donc $\omega(f(\overline{1}_{\mathbb{Z}/m\mathbb{Z}}))|m \wedge n = 1$ i.e. $f(1) = 0$ et alors $f = 0$. On en déduit donc que $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{0\}$.

Attention : La loi considérée ici est additive, donc pour tout $a \in \mathbb{Z}/m\mathbb{Z}$ (ou $\mathbb{Z}/n\mathbb{Z}$), on note $\omega(a) = \min\{k \geq 1, ka = 0\}$ au lieu de $\omega(a) = \min\{k \geq 1, a^k = 1\}$.

Correction de l'exercice IV.3. :

1. Considérons l'exemple où $(G,*) = (\mathrm{GL}(\mathbb{R}^2), \circ)$. Soit $\theta, \theta' \in \mathbb{R}$ et $S_\theta, S_{\theta'}$ les symétries par rapport aux axes faisant respectivement un angle θ et θ' par rapport à l'axe des abscisses dans le sens trigonométrique. On rappelle que
$$S_\theta \circ S_{\theta'} = R_{\theta-\theta'}$$
où pour tout $\alpha \in \mathbb{R}$, R_α désigne la rotation d'angle θ dans le sens trigonométrique dans $\mathbb{R}^2$.
En particulier, si on prend θ et θ' vérifiant $\dfrac{\theta-\theta'}{2\pi} \in \mathbb{R} \setminus \mathbb{Q}$ alors
$$S_\theta^2 = \mathrm{Id},\ S_{\theta'}^2 = \mathrm{Id} \text{ et } \forall n \in \mathbb{N},\ R_{\theta-\theta'}^n = R_{n(\theta-\theta')}$$

Pour tout $n \in \mathbb{N}$, $n(\theta - \theta') \notin 2\pi\mathbb{Z}$ car $\dfrac{\theta - \theta'}{2\pi} \notin \mathbb{Q}$ et alors $R_{n(\theta-\theta')} \neq \mathrm{Id}$. On en déduit donc que S_θ et $S_{\theta'}$ sont d'ordre 2 mais leur produit est d'ordre infini.

2. On a $(ab)^{mn} = (a^m)^n (b^n)^m = e$, donc ab est d'ordre fini et $\omega(ab)|mn$. Posons $l = \omega(ab)$. Remarquons maintenant que $(ab)^l = e$ et donc $(ab)^{lm} = e = (a^m)^l b^{lm} = b^{lm}$ d'où $n|ml$ et donc par Gauß, étant donné que $m \wedge n = 1$, on a $n|l$. On peut montrer de la même manière que $m|l$ et que donc, vu que $m \wedge n = 1$, on a $mn|l$ et finalement $l = mn$.
3. Décomposons m et n en facteurs premiers. Soit $r \in \mathbb{N}$, $p_1, \ldots, p_r$ des nombres premiers distincts et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, $\beta_1, \ldots, \beta_r \in \mathbb{N}$ tels que

$$m = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \text{ et } n = p_1^{\beta_1} \ldots p_r^{\beta_r}$$

Quitte à réordonner les p_i, supposons sans perte de généralité qu'il existe $k \in [\![1;r]\!]$ tel que

$$\forall i \in [\![1;k]\!],\ \max(\alpha_i, \beta_i) = \alpha_i \text{ et } \forall i \in [\![k+1;r]\!],\ \max(\alpha_i, \beta_i) = \beta_i$$

posons ensuite

$$m' = p_{k+1}^{\alpha_{k+1}} \ldots p_r^{\alpha_r},\ n' = p_1^{\beta_1} \ldots p_k^{\beta_k},\ a' = a^{m'} \text{ et } b' = b^{n'}$$

On a alors $\omega(a') = \dfrac{m}{m'}$ et $\omega(b') = \dfrac{n}{n'}$ ce qui donne

$$\omega(a') \wedge \omega(b') = \frac{n \wedge m}{n'm'} = \frac{n \wedge m}{p_1^{\min(\alpha_1,\beta_1)} \ldots p_r^{\min(\alpha_r,\beta_r)}} = \frac{n \wedge m}{n \wedge m} = 1$$

et donc d'après la question précédente

$$\omega(a'b') = \omega(a')\omega(b') = \frac{mn}{m'n'} = \frac{mn}{m \wedge n} = m \vee n$$

4. Posons $S = \{\omega(x),\ x \in G\}$. Étant donné que S est fini non vide, on peut, en utilisant la question précédente, trouver un élément $z \in G$ tel que $\omega(z) = \bigvee_{m \in S} m$ qui vérifie bien la propriété voulue.

Correction de l'exercice V.4. :

On envisage deux méthodes.

→ **Méthode 1 (plus intuitive) :** H est un sous-groupe de G qui est généré par a, donc tout élément de H s'écrit sous forme de a^l avec $l \in \mathbb{N}$. Soit $l = \min\{k \in \mathbb{N}^*,\ a^k \in H\}$. Montrons que $\left\langle a^l \right\rangle = H$. Supposons le contraire, i.e. qu'il existe $m \in \mathbb{N}$ tel que $a^m \notin \left\langle a^l \right\rangle$ et $a^m \in H$. On peut donc écrire $m = ql + r$ avec $q \in \mathbb{Z}$ et $r \in [\![0; l-1]\!]$ (car k ne divise pas m). On a alors

$$a^r = a^{-ql} a^{ql+r} = \left(a^l\right)^{-q} a^m \in H$$

ce qui est absurde par définition de l. On en déduit donc que $H = \left\langle a^l \right\rangle$. D'après la proposition IV.4, $\omega a^l | H$, on a alors $\left(a^l\right)^d = e$ et donc $a^{dl} = e$. D'après le point 1 de la proposition 1, on a $n|dl$. De plus, d'après la proposition IV.4, H étant un sous-groupe cyclique de G, on a $d|n$ et donc $\left.\dfrac{n}{d}\right| l$. Posons donc $l = \alpha \dfrac{n}{d}$ avec $\alpha \in \mathbb{N}$. On a alors

$$H = \left\langle a^l \right\rangle = \left\langle a^{\alpha \frac{n}{d}} \right\rangle \subset \left\langle a^{\frac{n}{d}} \right\rangle$$

On a de plus d'après le point 5 de la proposition III.1, $\left|\left\langle a^{\frac{n}{d}} \right\rangle\right| = \dfrac{n}{n/d} = d = |H|$ et donc $|H| = \left\langle a^{\frac{n}{d}} \right\rangle$.

→ **Méthode 2 (plus rapide) :** a est un générateur de G donc l'application $\varphi : \begin{cases} \mathbb{Z} & \longrightarrow G \\ k & \longmapsto a^k \end{cases}$ est surjective et $\operatorname{Ker}\varphi = n\mathbb{Z}$. On a donc $H = \varphi(\varphi^{-1}(H))$ et d'après la proposition I.9, $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, i.e. de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$. De plus, $\{e\} \subset H$ et donc

$$n\mathbb{Z} = \varphi^{-1}(\{e\}) \subset \varphi^{-1}(H) = k\mathbb{Z}$$

On en déduit alors que $k|n$ et que

$$H = \varphi(k\mathbb{Z}) = \{a^l,\ l \in k\mathbb{Z}\} = \left\langle a^k \right\rangle$$

De plus, $d = |H| = \left|\left\langle a^k \right\rangle\right| = \dfrac{n}{k}$ et donc $k = \dfrac{n}{d}$ et finalement $H = \left\langle a^{\frac{n}{d}} \right\rangle$.

Correction de l'exercice V.5. :

1. Soit $k \in \mathbb{Z}$. D'après le point (4) de la proposition III.1, on a $\omega(a^k) = \dfrac{\omega(a)}{\omega(a) \wedge k} = \dfrac{n}{n \wedge k}$. On en déduit donc que
$$G = \left\langle a^k \right\rangle \Longleftrightarrow \omega(a^k) = n \Longleftrightarrow \frac{n}{n \wedge k} = n \Longleftrightarrow n \wedge k = 1$$

2. On envisage deux méthodes.

→ **Méthode 1 :** Notons pour tout $d \in \mathbb{N}^*$ diviseur de n $G_d = \{b \in G,\ \omega(b) = d\}$. On sais que d'après l'exercice V.4, pour tout d diviseur positif de n, tout sous-groupe de cardinal d est égal à $H_d = \left\langle a^{\frac{n}{d}} \right\rangle$. On a donc

$$b \in G_d \Longleftrightarrow |\langle b \rangle| = d \underset{\langle b \rangle \leq G}{\Longleftrightarrow} \langle b \rangle = H_d$$

On a donc pour tout d diviseur positif de n,

$$\begin{aligned} |G_d| &= |\{b \in G,\ \omega(b) = d\}| \\ &= \left|\left\{\left(a^{\frac{n}{d}}\right)^k,\ k \in \mathbb{N},\ \left\langle a^{\frac{kd}{n}} \right\rangle = H_d\right\}\right| \\ &= |\{k \in [\![1; d]\!],\ k \wedge d = 1\}| = \varphi(d) \end{aligned}$$

L'avant dernière égalité est due au fait que $a^{\frac{n}{d}}$ est un générateur de H_d et donc d'après la question précédente $\left(a^{\frac{n}{d}}\right)^k$ génère H_d si et seulement si $k \wedge d = 1$. On a alors

$$n = |G| = \left| \bigsqcup_{d|n,\ d\geq 1} G_d \right| = \sum_{d|n,\ d\geq 1} |G_d| = \sum_{d|n,\ d\geq 1} \varphi(d)$$

→ **Méthode 2 :** On a

$$\begin{aligned} n = |[\![1;n]\!]| &= \left| \bigsqcup_{d|n,\ d\geq 1} \{k \in [\![1;n]\!]\ k \wedge n = d\} \right| \\ &= \sum_{d|n,\ d\geq 1} |\{k \in [\![1;n]\!]\ k \wedge n = d\}| \\ &= \sum_{d|n,\ d\geq 1} \left| \left\{ k \in d \times [\![1;\frac{n}{d}]\!],\ \frac{k}{d} \wedge \frac{n}{d} = 1 \right\} \right| \\ &= \sum_{d|n,\ d\geq 1} \left| \left\{ k \in [\![1;\frac{n}{d}]\!],\ k \wedge \frac{n}{d} = 1 \right\} \right| \\ &= \sum_{d|n,\ d\geq 1} \varphi\left(\frac{n}{d}\right) = \sum_{d|n,\ d\geq 1} \varphi(d) \end{aligned}$$

La dernière égalité est vraie car

$$h : \begin{cases} \{d \geq 1,\ d|n\} & \longrightarrow \{d \geq 1,\ d|n\} \\ d & \longmapsto \dfrac{n}{d} \end{cases}$$

est une bijection.

Correction de l'exercice V.6. :

1. Notons $n = |G_1|$, $m = |G_2|$ et a, b des générateurs de G_1 et G_2 respectivement. On note également e_1 et e_2 les éléments neutres respectifs de $(G_1, *)$ et $(G_2, *)$. On envisage deux cas possibles.
   → **Cas** 1 : $n \wedge m = 1$.
   Soit $z = (a, b) = (e_1, b) \otimes (a, e_2)$. On a clairement $\omega((a, e_2)) = n$ et $\omega((e_1, b)) = m$ donc d'après l'exercice IV.3. $\omega(z) = mn$ et donc étant donné que $|G_1 \times G_2| = mn$, alors $G_1 \times G_2 = \langle z \rangle$, i.e. $(G_1 \times G_2, \otimes)$ est cyclique.
   → **Cas** 2 : $n \wedge m \neq 1$.
   Posons alors $l = n \vee m$. Il est clair que $\forall z \in G_1 \times G_2,\ z^l = (e_1, e_2)$ et donc $G_1 \times G_2$ ne peut pas être cyclique car pour tout $z \in G$, $|\langle z \rangle| \leq l < mn = |G_1 \times G_2|$.

   On en déduit donc que $G_1 \times G_2$ est cyclique si et seulement si $|G_1| \wedge |G_2| = 1$.
2. Pour vérifier que f est bien définie, il faut vérifier que tout élément de $\mathbb{Z}/ab\mathbb{Z}$ a une image unique par f. On doit donc vérifier que pour tout $x, y \in \mathbb{Z}$, si dans $\mathbb{Z}/ab\mathbb{Z}$ on a $\overline{x} = \overline{y}$, alors $\varphi(\overline{x}) = \varphi(\overline{y})$. Notons pour tout $z \in \mathbb{Z}$ et $r \geq 2$, $\overline{z}_{(r)}$ la classe de z dans $\mathbb{Z}/r\mathbb{Z}$.

   Considérons donc $x, y \in \mathbb{Z}$ tels que dans $\mathbb{Z}/ab\mathbb{Z}$, on ait $\overline{x} = \overline{y}$. Il existe donc $k \in \mathbb{Z}$ tel que $x = y + kab$. On a alors

   $$\varphi\left(\overline{x}_{(ab)}\right) = \left(\overline{x}_{(a)}, \overline{x}_{(b)}\right) = \left(\overline{y}_{(a)} + \overline{kab}_{(a)}, \overline{y}_{(b)} + \overline{kab}_{(b)}\right) = \left(\overline{y}_{(a)}, \overline{y}_{(b)}\right) = \varphi\left(\overline{y}_{(ab)}\right)$$

   φ est donc bien définie. Il est également facile de vérifier qu'il s'agit d'un morphisme. Montrons maintenant qu'il s'agit d'un isomorphisme si et seulement si $a \wedge b = 1$.
   → $(\Leftarrow)$ Supposons que $a \wedge b = 1$. On a $\varphi\left(\overline{1}_{(ab)}\right) = \left(\overline{1}_{(a)}, \overline{1}_{(b)}\right)$. D'après la question 1, étant donné que $\overline{1}_{(a)}$ et $\overline{1}_{(b)}$ sont d'ordre respectivement a et b et $a \wedge b = 1$, alors $\omega\left(\left(\overline{1}_{(a)}, \overline{1}_{(b)}\right)\right) = ab$. On a de plus

   $$\left\langle \left(\overline{1}_{(a)}, \overline{1}_{(b)}\right) \right\rangle = \left\langle \varphi\left(\overline{1}_{(ab)}\right) \right\rangle \subset \operatorname{Im} \varphi$$

   et donc

   $$|\operatorname{Im} \varphi| \geq \left| \left\langle \left(\overline{1}_{(a)}, \overline{1}_{(b)}\right) \right\rangle \right| = ab$$

or $|\operatorname{Im}\varphi| \leq |\mathbb{Z}/aZ \times \mathbb{Z}/b\mathbb{Z}| = ab$, donc $|\operatorname{Im}\varphi| = ab$ et alors $\operatorname{Im}\varphi = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, i.e. φ est surjective. De plus, on a $|\mathbb{Z}/ab\mathbb{Z}| = ab = |\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}|$ donc la surjectivité de φ nous donne directement que φ est bijective, c'est donc un isomorphisme.

→ ($\Rightarrow$) Supposons que $a \wedge b = d > 1$. On a alors $a \vee b \in]0, ab[$ et donc $\overline{a \vee b}_{(ab)} \neq \overline{0}_{(ab)}$, mais

$$\varphi\left(\overline{a \vee b}_{(ab)}\right) = \left(\overline{a \vee b}_{(a)}, \overline{a \vee b}_{(b)}\right) = \left(\overline{0}_{(a)}, \overline{0}_{(b)}\right)$$

On en déduit que $\operatorname{Ker}\varphi \neq \left\{\overline{0}_{(ab)}\right\}$ et que donc φ n'est pas injective. φ ne peut donc pas être un isomorphisme.

Correction de l'exercice V.7. :

1. Soit $P \in A[X]$ et $Q \in A[X]$ de coefficient dominant égal à 1. Il s'agit de montrer la proposition suivante

$$\exists! B, R \in A[X],\ P(X) = B(X)Q(X) + R(X),\ \deg R < \deg Q$$

→ **Existence :** Procédons par récurrence forte sur le degré de P. Posons $n = \deg P$.

- Si $\deg P = 0$, alors si $\deg Q > 0$, $B = 0$ et $R = P$ conviennent. si $\deg Q = 0$ i.e. $Q = 1$, alors $R = 0$ et $B = P$ conviennent.
- Soit $n \in \mathbb{N}$. Suppsons que la propriété est vraie pour tout n, i.e. pour tout polynôme P de degré inférieur ou égal à n,

$$\exists B, R \in A[X],\ P(X) = B(X)Q(X) + R(X),\ \deg R < \deg Q$$

Montrons que la propriété est vraie pour $n+1$. On suppose que P est de degré $n+1$ et on pose

$$P(X) = \sum_{k=0}^{n+1} a_k X^k \text{ et } Q(X) = X^r + H(X)$$

avec $r = \deg Q$ et $H \in A[X]$ tel que $\deg H < r$. Si $r > n+1$, alors $B = 0$ et $R = Q$ conviennent. Si $r \leq n+1$ on a alors

$$P(X) - a_{n+1}X^{n+1-r}Q(X) = \sum_{k=0}^{n} a_k X^k - a_{n+1}X^{n+1-r}H(X)$$

On a donc

$$\deg(P(X) - a_{n+1}X^{n+1-r}Q(X)) = \deg\left(\sum_{k=0}^{n} a_k X^k - a_{n+1}X^{n+1-r}H(X)\right) \leq n$$

Par hypothèse de récurrence, il existe $\tilde{B}, \tilde{R} \in A[X]$ tels que $\deg \tilde{R} < \deg Q$ tels que

$$P(X) - a_{n+1}X^{n+1-r}Q(X) = \tilde{B}(X)Q(X) + \tilde{R}(X)$$

et alors on a

$$P(X) = (\tilde{B}(X) + a_{n+1}X^{n+1-r})Q(X) + R(X)$$

on en déduit que $B(X) = \tilde{B}(X) + a_{n+1}X^{n+1-r}$ et $\tilde{R}(X) = R(X)$ conviennent, d'où l'existence.

→ **Unicité :** Soit $B_1, B_2, R_1, R_2 \in A[X]$ tels que $\deg R_1 \leq \deg Q$, $\deg R_2 \leq \deg Q$ et

$$P(X) = B_1(X)Q(X) + R_1(X) = B_2(X)Q(X) + R_2(X)$$

On a alors

$$(B_1(X) - B_2(X))Q(X) = R_1(X) - R_2(X)$$

Si $B_1 - B_2 \neq 0$, alors étant donné que Q est non nul, on a

$$\begin{aligned}
\deg(R_1 - R_2) &= \deg((B_1 - B_2)Q) && (1)\\
&= \deg\left((B_1 - B_2)X^r + (B_1 - B_2)H\right) && (2)\\
&= \deg(B_1 - B_2) + \deg Q \geq \deg Q && (3)
\end{aligned}$$

ce qui est absurde. On en déduit que $B_1 = B_2$ et que $R_1 = R_2$, d'où l'unicité.

Attention : Lorsque $U, V \in A[X]$ et que A n'est pas intègre, on a pas forcément l'égalité $\deg(UV) = \deg U + \deg V$, mais ici, on peut passer de la ligne (2) à (3) car le coefficient dominant de Q est égal à 1. Ce passage serait également vrai si le coefficient dominant de Q n'est pas un diviseur de zéro.

2. Montrons ce résultat par récurrence sur le degré de P encore une fois.
   - Lorsque $\deg P = 0$, P n'a clairement pas de racines (le cas $P = 0$ correspond à $\deg P = -\infty$).
   - Soit $n \in \mathbb{N}$. Supposons que la propriété est vraie lorsque $\deg P \in [\![0; n]\!]$ et supposons maintenant que $\deg P = n + 1$. Si P n'admet pas de racines, la propriété est vraie. Supposons que P admet une racine $a \in A$. La question précédente nous permet d'effectuer la division euclidienne de P par $X - a$ (ce polynôme est de coefficient dominant égal à 1). Il existe donc $B, R \in A[X]$ tel que
   $$\deg R < \deg(X - a) = 1 \text{ et } P(X) = (X - a)B(X) + R(X)$$
   On a de plus $0 = P(a) = R(a)$ et R est constant donc $R = 0$. B est de degré n, donc par hypothèse de récurrence, B admet au plus n racines et donc $P(X) = (X - a)B(X)$ admet au plus $n + 1 = \deg P$ racines.
3. Si G est cyclique, alors nécessairement on a $|G| = \bigvee_{x \in G} \omega(x)$. Notre intuition est donc de considérer un élément de G d'ordre le plus grand qu'on peut trouver (ici égal à n) et d'essayer de montrer qu'il engendre G. Posons $n = \bigvee_{x \in G} \omega(x)$. D'après la question 4 de l'exercice IV.3, il existe $z \in G$ tel que $\omega(z) = \bigvee_{x \in G} \omega(x) = n$. n est un multiple de tous les ordres des éléments de G, donc pour tout $x \in G$, $x^n = 1$. On posant Z l'ensemble des racines de $X^n - 1$ dans $\mathbb{K}$, on voit que $G \subset Z$. D'après la question précédente, le polynôme $X^n - 1$ admet au plus n racines, donc on a $|G| \leq |Z| \leq n$. De plus, on a $n = |\langle z \rangle| \leq |G|$ et donc $|G| = n = |\langle z \rangle|$ et $\langle z \rangle \subset G$, et finalement $G = \langle z \rangle$, i.e. G est cyclique.

Correction de l'exercice VI.2. :

On peut voir G comme un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En effet, en considérant les lois (bien définies)

$$+ : \begin{cases} G \times G & \longrightarrow G \\ (x, y) & \longmapsto x * y \end{cases} \quad \text{et } \cdot : \begin{cases} \mathbb{Z}/p\mathbb{Z} \times G & \longrightarrow G \\ (\overline{k}, x) & \longmapsto x^k \end{cases}$$

on peut voir que $(G, +, \cdot)$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. G est fini et donc de dimension finie. En posant $n = \dim_{\mathbb{Z}/p\mathbb{Z}} G$, on peut affirmer l'existence d'une base de G, $(x_1, \ldots, x_n)$. On peut donc affirmer que tout $x \in G$ s'écrit d'une manière unique sous forme de

$$x = \overline{k_1} \cdot x_1 + \cdots + \overline{k_n} \cdot x_n,\ \overline{k_1}, \ldots, \overline{k_n} \in \mathbb{Z}/p\mathbb{Z}$$

En considérant donc l'isomorphisme (il est facile de montrer qu'il est bien défini et qu'il s'agit d'un isomorphisme)

$$\varphi : \begin{cases} G & \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \\ \overline{k_1}x_1 + \cdots + \overline{k_n}x_n & \longmapsto (\overline{k_1}, \ldots, \overline{k_n}) \end{cases}$$

On voit donc que $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$. En particulier, on remarquera que $|G| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$.

Remarque : En utilisant le théorème de Cauchy (VII.14), on peut très facilement montrer qu'il existe $n \in \mathbb{N}^*$ tel que $|G| = p^n$. En effet, pour tout $g \in G \setminus \{e\}$, $g^p = e$ et donc $\omega(g)|p$ i.e. $\omega(g) = p$. Pour tout nombre premier q, si $q|\,|G|$, alors par le thorème de Cauchy il existe $g \in G$ tel que $\omega(g) = q$ et alors $q = p$. p est donc le seul nombre premier qui divise $|G|$ ce qui signifie qu'il existe $n \in \mathbb{N}^*$ tel que $|G| = p^n$.

Correction de l'exercice VI.3. :

Montrons le résultat par implications successives.

→ (1) ⇒ (2) Montrer que $H \simeq \mathbb{Z}/p\mathbb{Z}$ est équivalent à montrer que H est engendré par un élément d'ordre p premier. En effet, s'il existe $x \in H$ tel que $\langle x\rangle = G$ et $\omega(x) = p \in \mathbb{P}$, alors il est facile de montrer que l'application $\psi : \begin{cases} H & \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ x^k & \longmapsto \overline{k} \end{cases}$ est bien définie et est un isomorphisme et que donc en particulier $H \simeq \mathbb{Z}/p\mathbb{Z}$.

Montrons maintenant que G est engendré par un élément d'ordre premier. Soit $x \in G \setminus \{e\}$. $\langle x\rangle \in \mathrm{Sg}(H) \setminus \{\{e\}\}$ et donc $\langle x\rangle = H$. Montrons que $\omega(x)$ est premier.

Si $\omega(x) = \infty$, alors $\langle x^2\rangle$ est un sous-groupe de G. Il est facile de vérifier que $\langle x^2\rangle \neq \langle x\rangle$ et alors on a $\langle x^2\rangle = \{e\}$, i.e. $\omega(x) \leq 2$ ce qui est en contradiction avec le fait que $\omega(x) = \infty$. On en déduit donc que $\omega(x)$ est fini.

Soit d un diviseur de $\omega(x)$ supérieur ou égal à 2. D'après la proposition III.1, on a $\omega(x^d) = \dfrac{\omega(x)}{d}$ ce qui donne nécessairement $\left\langle x^d\right\rangle \in \mathrm{Sg}(H) \setminus \{H\}$ et donc $\left\langle x^d\right\rangle = \{e\}$, ce qui signifie que $x^d = e$, et alors encore d'après la proposition III.1 $\omega(x)|d$ et finalement $d = \omega(x)$. On en déduit donc que les seuls diviseurs positifs de $\omega(x)$ sont 1 et $\omega(x)$, i.e. que $\omega(x)$ est premier (ou égal à 1, mais ce cas est impossible car $x \neq e$). En posant $p = \omega(x)$, on en déduit d'après ce qui précède que $H \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premier.

→ (2) ⇒ (3) Si $H \simeq \mathbb{Z}/p\mathbb{Z}$, alors et $|G| = |\mathbb{Z}/p\mathbb{Z}| = p$, ce qui implique d'après le théorème de Lagrange faible (IV.4) que tout élément a de $H \setminus \{e\}$ divise p et donc $\omega(a) \in \{1, p\}$. On en déduit alors que pour tout $a \in H \setminus \{e\}$, $|\langle a\rangle| = \omega(a) = p = |H|$ i.e. $\langle a\rangle = H$, d'où le résultat.

→ (3) ⇒ (4) G est monogène, on peut donc considérer $g \in G$ tel que $\langle g\rangle = G$. Deux cas se présentent.

- Si $\omega(g) = \infty$, on a par hypothèse $\langle g^2\rangle = G$ ce qui est impossible. En effet, $g \notin \langle g^2\rangle$ car sinon il existerait $k \in \mathbb{Z}$ tel que $g^{2k} = g$, i.e. $g^{2k-1} = e$ ce qui est absurde.
- Si $\omega(g) = n \in \mathbb{N}^*$, alors le morphisme

$$\psi' : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow H \\ \overline{k} & \longmapsto g^k \end{cases}$$

  est bien défini et est bijectif. On en déduit alors que $H \simeq Z/n\mathbb{Z}$. De plus, si d est un diviseur positif de n différent de n, alors d'après le point 5 de la proposition III.1, $\left|\left\langle g^d\right\rangle\right| = \omega(g^d) = \dfrac{n}{d}$. On a donc

$$\frac{n}{d} = \omega(g^d) = \left|\left\langle g^d\right\rangle\right| = |H| = n$$

  et donc $d = 1$. On en déduit alors que les seuls diviseurs de n sont 1 et n, i.e. que n est premier et alors $|H| = |\mathbb{Z}/n\mathbb{Z}| = n \in \mathbb{P}$.

→ (4) ⇒ (1) Soit L un sous-groupe de H. H est cyclique donc d'après le résultat de l'exercice V.4 L est également cyclique. On a donc d'après le théorème faible de Lagrange (IV.4) $|L|\,|\,|H|$, mais H est premier, donc $|L| \in \{1, |H|\}$ et finalement $\mathrm{Sg}(H) = \{H, \{e\}\}$.

Correction de l'exercice VII.5. :

D'après le théorème faible de Lagrange (IV.4), l'ordre de tout élément de H divise pq et donc pour tout $a \in H \setminus \{e\}$, $\omega(a) \in \{p, q, pq\}$.

- → Si tout élément de $H \setminus \{e\}$ est d'ordre p, alors d'après l'exercice VI.2, il existe $n \in \mathbb{N}$ tel que $|H| = p^n$ ce qui est absurde.
- → De même, si tout élément de $H \setminus \{e\}$ est d'ordre q, alors il existe $n \in \mathbb{N}$ tel que $|H| = q^n$ ce qui est absurde.
- → S'il existe un élément $a \in H$ d'ordre pq, alors $\langle a \rangle = H$ et donc d'après la proposition V.3, $H \simeq \mathbb{Z}/pq\mathbb{Z}$.
- → S'il existe un élément $a \in H$ d'ordre p et un élément $b \in H$ d'ordre q, alors d'après la question 2 de l'exercice IV.3, $\omega(ab) = pq$ et donc $H = \langle ab \rangle$ et alors pour les mêmes raisons qu'au point précédent, on a $H \simeq \mathbb{Z}/pq\mathbb{Z}$.

Finalement, d'après le théorème chinois (exercice V.6), on a $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et finalement $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Correction de l'exercice VII.6. :

On a par hypothèse $|G/H| = 2$ donc il y a deux classes à gauche. Soit $a \in G \setminus H$. On a $aH \neq H$, donc $G/H = \{H, aH\}$. De la même manière, G a deux classes à droite et donc étant donné que $Ha \neq H$, ces deux classes sont H et Ha. On a donc $G = aH \sqcup H = Ha \sqcup H$ et alors $aH = Ha = G \setminus H$. De même, lorsque $a \in H$, on a $aH = H = Ha$ et alors en déduit donc que H est bien un sous-groupe distingué de G. Montrons à présent que H contient tous les carrés. $|G/H| = 2$ donc l'ordre de tout élément de G/H divise 2, i.e. pour tout $x \in H$, $(xH)^2$ est égal à H, l'élément neutre du groupe G/H. On en déduit que pour tout $x \in G$, $H = xHxH = x^2H$ et alors $x^2 \in H$. H contient donc tous les carrés.

Correction de l'exercice VII.10. :

Intuition : Pour montrer que H est distingué, il faut et il suffit de montrer que pour tout $h \in H$ et $a \in G$, $haH = aH$. En effet, lorsque cela est vérifié, alors on a pour tout $a \in G$ et $h \in H$, $a^{-1}haH = a^{-1}aH = H$ et donc $a^{-1}ha \in H$. Ceci donne directement que $a^{-1}Ha = H$ ce qui signifie que H est un sous-groupe distingué de G.

Pour montrer que pour tout $h \in H$ et $a \in G$, $haH = H$, on va considérer une action de groupe $\bullet$ telle que pour tout $h \in H$ et $a \in G$, $h \bullet aH = haH$.

Considérons donc l'action de groupe $\bullet$ de H sur G/H définie par

$$\bullet : \begin{cases} H \times G/H & \longrightarrow G/H \\ (h, aH) & \longmapsto haH \end{cases}$$

Pour montrer que H est distingué, il suffit de montrer que pour tout $h \in H$ et $a \in G$, $haH = aH$, i.e. que $O(aH) = \{aH\}$. Soit $a \in G$. Supposons que $|O(aH)| \neq 1$. D'après le point 3 de la proposition VII.9, on a $O(aH)| \,|\, |H|$. De plus, par le théorème de Lagrange (VII.4), H étant un sous-groupe de G, on a $|H| \,|\, |G|$ et donc $|O(aH)| \,|\, |G|$. p étant le plus petit diviseur de $|G|$ strictement supérieur à 1, on en déduit que $|O(aH)| \geq p$. Remarquons de plus que pour tout $h \in H$, $h \bullet H = H$ et donc $O(H) = \{H\}$.

On a alors d'après le point 4 de la proposition VII.9, si R est l'ensemble des représentants des orbites de l'action $\bullet$ de H sur G/H, alors

$$p = |G/H| = \sum_{x \in R} |O(x)| \geq |O(H)| + |O(aH)| \geq p + 1$$

ce qui est absurde, donc $|O(aH)| = 1$ i.e. $O(aH) = \{aH\}$ donc H est bien un sous-groupe distingué de G.

Une version plus courte utilisant des notion plus avancées sera exposée dans un chapitre complément à celui-ci qui sera publié plus-tard.

Correction de l'exercice VII.13. :

Soit R l'ensemble des représentants de classes de conjugaison de G non réduites à un singleton. En appliquant la formules des classes à G (point 3 de la proposition VII.12), on obtient

$$|Z(G)| = |G| - \sum_{x\in R} |O(x)| = |G| - \sum_{x\in R} \frac{|G|}{C(x)}$$

On a de plus pour tout $x \in R$, $\left.\frac{|G|}{|C(x)|}\right| |G|$ et $|G| = p^n$, donc tous les diviseurs strictement positifs de $|G|$ sont de la forme p^k avec $k \in [\![0; n]\!]$. De plus, pour tout $x \in R$, $\frac{|G|}{|C(x)|} = |O(x)| \neq 1$ et alors

$$\forall x \in R,\ \exists k \in [\![1; n]\!],\ \frac{|G|}{|C(x)|} = p^k$$

et donc

$$Z(G) \equiv p^n - \sum_{x\in R} \frac{|G|}{|C(x)|} \equiv 0[p]$$

De plus, $e \in Z(G)$ donc $Z(G) \geq p$. $Z(G)$ n'est alors pas réduit à un singleton.

Supposons à présent que $n \leq 2$ et montrons que G est abélien.

→ Si $n = 1$, alors on a $p = |G| \geq |Z(G)| \geq p$ donc $|Z(G)| = p$ et alors $Z(G) = G$ i.e. G est abélien.

→ Si $n = 2$, alors on sait que $Z(G)$ est un sous-groupe de G, donc par le théorème de Lagrange (VII.4), $|Z(G)| \,|\, |G|$ et donc $|Z(G)| = p$ ou $|Z(G)| = p^2$. Si $|Z(G)| = p^2$, alors on peut dire comme avant que $Z(G) = G$ et alors que G est abélien.

Soit $x \in G \setminus Z(G)$. On sait encore une fois, d'après le théorème de Lagrange (VII.4), que $|\langle x\rangle| \,|\, |G|$, et $x \neq e$, donc $|\langle x\rangle| \in \{p, p^2\}$. Si $|\langle x\rangle| = p^2$, alors $G = \langle x\rangle$ et on en déduit immédiatement que G est commutatif. Sinon, on a encore une fois d'après Lagrange $|\langle\{x\} \cup Z(G)\rangle| \in \{p, p^2\}$ et $|\langle\{x\} \cup Z(G)\rangle| > |\langle x\rangle| = p$ et donc $|\langle\{x\} \cup Z(G)\rangle| = p^2$ et alors $\langle\{x\} \cup Z(G)\rangle = G$. D'après la proposition VI.1, on peut écrire

$$G = \langle\{x\} \cup Z(G)\rangle = \{a_1^{\alpha_1} \dots a_n^{\alpha_n},\ n \in \mathbb{N},\ a_1, \dots, a_n \in \{x\} \cup Z(G),\ \alpha_1, \dots, \alpha_n \in \mathbb{Z}\}$$

il est facile de montrer que ce groupe est abélien, et donc on en déduit que G est abélien.

Correction de l'exercice VII.15. :

1. Soit $x \in G$ tel que $\omega(\overline{x}) = p$. En considérant le morphisme introduit à la proposition VII.3

$$\pi : \begin{cases} G & \longrightarrow G/K \\ x & \longmapsto \overline{x} = xK \end{cases}$$

on peut affirmer d'après le point 1 de la proposition IV.1 que $\omega(\pi(x))|\omega(x)$ i.e. $p|\omega(x)$. On a alors d'après le point 5 de la proposition III.1, $\omega\left(x^{\frac{\omega(x)}{p}}\right) = \frac{\omega(x)}{\omega(x)/p} = p$.

2. Posons $G = kp$ avec $k \in \mathbb{N}^*$ et procédons par récurrence forte sur k

→ Si $k = 1$, alors $|G| = p$, alors la propriété est vraie d'après l'exercice VI.3.

→ Soit $k \in \mathbb{N}$, suppsons que pour tout $l \in [\![1; k]\!]$, si $|G| = lp$, alors G vérifie la propriété voulue. Supposons maintenant que $|G| = (k+1)p$ et montrons qu'il existe un élément de G d'ordre p. Soit $x \in G \setminus \{e\}$.

- Si $p|\omega(x)$, alors encore une fois, d'après le point 5 de la proposition III.1,

$$\omega\left(x^{\frac{\omega(x)}{p}}\right)=\frac{\omega(x)}{\omega(x)/p}=p$$

- Si $p\nmid\omega(x)$, alors on a $|G/\langle x\rangle|=\dfrac{|G|}{\omega(x)}=\dfrac{k+1}{\omega(x)}p$ et $\dfrac{k+1}{\omega(x)}\in[\![1;k]\!]$ (bien entendu, $\dfrac{k+1}{\omega(x)}\in\mathbb{N}$ car étant donné que $\omega(x)\wedge p=1$, d'après Gauss $\omega(x)|k+1$). On en déduit alors par hypothèse de récurrence qu'il existe $y\in G/\langle x\rangle$ tel que $\omega(y)=p$ et alors d'après la question 1, il existe $z\in G$ tel que $\omega(z)=p$ ce qui bien le résultat voulu.

3. Procédons par récurrence forte sur a.
   - → Lorsque $a=1$, la propriété est vraie d'après la question précédente.
   - → Soit m le plus grand entier tel que $p^m|\,|G|$ et soit $k\in[\![1;m-1]\!]$. Supposons que le résultat est vrai pour tout $a\in[\![1;k]\!]$ et montrons qu'il est également vrai pour $a=k+1$. Par hypothèse de récurrence, il existe H sous-groupe de G tel que $|H|=p^k$. On a alors $|G/H|=|G|/p^k$ et $k\leq m-1$ donc $p|\,|G/H|$. On sait donc d'après la question précédente (qui donne le résultat pour $a=1$) qu'il existe M un sous-groupe de G/H tel que $|M|=p$. Considérons l'endomorphisme (identique à celui considéré à la question 1)

$$\pi:\begin{cases}G&\longrightarrow G/H\\ x&\longmapsto xH\end{cases}$$

et en posant $L=\pi^{-1}(M)$ (c'est un groupe) et considérant le morphisme de groupe

$$\tilde{\pi}:\begin{cases}L&\longrightarrow M\cap\operatorname{Im}\pi\\ x&\longmapsto \pi(x)\end{cases}$$

π est surjective par définition, donc $M\cap\operatorname{Im}\pi=M$. On a de plus d'après la proposition VII.3,

$$L/\operatorname{Ker}\tilde{\pi}\simeq\operatorname{Im}\tilde{\pi}\tag{4}$$

On a de plus, M est un sous-groupe de G/H et contient donc son élément neutre H, et alors

$$H=\operatorname{Ker}\pi=\pi^{-1}(\{H\})\subset\pi^{-1}(M)=L$$

et alors

$$\operatorname{Ker}\tilde{\pi}=L\cap\operatorname{Ker}\pi=\operatorname{Ker}\pi=H$$

et donc $\operatorname{Ker}\tilde{\pi}=\operatorname{Ker}\pi$. De plus, on a également

$$\operatorname{Im}\tilde{\pi}=\pi(L)=\pi(\pi^{-1}(M))=M\cap\operatorname{Im}\pi\underset{\pi\text{ surjective}}{=}M\cap G/H=M$$

et donc on peut réécrire l'égalité (1) comme $L/H=M$ ce qui donne

$$|L|=|H|\times|M|=p^k\times p=p^{k+1}$$

L est donc un sous-groupe de G de cardinal p^{k+1}, ce qui est bien le résultat voulu.

4. D'abord, par commutation, $HL=LH$ et donc ce dernier est bien un sous-groupe de G (voir question 1 exercice I.13). De même, par commutation, ψ est bien un morphisme de groupes. Montrons maintenant que ψ est injective. On envisage deux méthodes.
   - → **Méthode 1 (à la main) :** Soit $(h,l)\in\operatorname{Ker}\psi$. On a alors $hl=e$. Posons $p=\omega(h)$ et $q=\omega(l)$. D'après le théorème de Lagrange, on a $p|\,|H|$ et $q|\,|L|$. De plus, on a $|H|\wedge L=1$ ce qui donne

$p \wedge q = 1$. On a alors d'après Bezout, il existe $u, v \in \mathbb{Z}$ tels que $up + vq = 1$. On a alors

$$e = (hl)^{vq} = h^{1-up} l^{vq} = h \text{ et } e = (hl)^{up} = h^{up} l^{1-vq} = l$$

et donc $(h, l) = (e, e)$. On en déduit donc que $\operatorname{Ker} \psi = \{(e, e)\}$ et que donc ψ est injective.

→ **Méthode 2 :** Soit $(h, l) \in \operatorname{Ker} \psi$. On a alors $hl = e$ et donc $h = l^{-1} \in H \cap L$.
Or, $H \cap L \leq H$ et $H \cap L \leq L$ et donc, par Lagrange, $|H \cap L| \mid |H| \wedge |L| = 1$ i.e. $H \cap L = \{e\}$.
Ainsi, $h = l = e$ et donc ψ est injective.

ψ est clairement surjective donc bijective et donc $|HL| = |H \times L| = |H| \times |L|$.

5. On peut montrer facilement par récurrence en utilisant la question précédente le résultat suivant. Pour tout $r \in \mathbb{N}^*$, si $H_1, \ldots, H_r$ sont r sous-groupes de G tels que pour tout $i, j \in [\![1; r]\!]$ différents, $|H_i| \wedge |H_j| = 1$, alors $H_1 \ldots H_r$ est un sous-groupe de G et

$$|H_1 \ldots H_r| = |H_1| \times \cdots \times |H_r|$$

Écrivons maintenant la décomposition en produits de nombres premiers de n ($n = 1$ étant trivial). Soit $r \in \mathbb{N}^*$, $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$ et $p_1, \ldots, p_r$ r nombres premiers distincts tels que $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. D'après la question 3, pour tout $k \in [\![1; r]\!]$, il existe H_k un sous groupe de G tel que $|H_k| = p_k^{\alpha_k}$. De plus, on a clairement pour tout $i, j \in [\![1; r]\!]$ différents $|H_i| \wedge |H_j| = 1$ et alors on en déduit que $H_1 \ldots H_r$ est un sous-groupe de G et que $|H_1 \ldots H_r| = p_1^{\alpha_1} \ldots p_r^{\alpha_r} = n$.

*   *
*