Lycée Carnot
ECS 4 – Mathématiques
A. Troesch

Septembre 2005

Correction du Devoir Maison n° 2 – Groupes, lemme des cinq

Partie I – Groupes.

1. Exemples.
   (a) Il n'y a pas grand chose à vérifier : l'addition de $\mathbb{Z}$ est bien associative et commutative, 0 joue le rôle d'élément neutre puisque pour tout $x \in \mathbb{Z}$, $x+0=0+x=x$, et l'inverse de x est $-x$, puisque $x+(-x)=(-x)+x=0=e$. Ainsi $\mathbb{Z}$ est un groupe abélien.
   Je pourrais répéter exactement la même chose mot pour mot pour $\mathbb{R}$ et $\mathbb{C}$. Ainsi, $\mathbb{R}$ et $\mathbb{C}$ sont des groupes abéliens.
   (b) $\mathbb{N}$ n'est pas un groupe, car l'existence de l'inverse fait défaut : En effet, aucun entier $n \in \mathbb{N}^*$ n'admet d'inverse ; en effet, si n admettait un inverse $m \in \mathbb{N}$ on aurait : $0 = n+m \geqslant n > 0$, puisque $m \geqslant 0$. D'où une contradiction/
   (c) Là encore, il n'y a pas grand chose à vérifier. L'addition ainsi définie est clairement associative et commutative, 0 est l'élément neutre, et le seul élément 0 de $\{0\}$ admet un opposé : lui-même.
   (d) Voilà qui est plus intéressant. Le groupe étant de petit cardinal, on peut vérifier toutes les propriétés voulues à la main.
   - L'associativité résulte des calculs suivants :

$$\begin{array}{ll} (0+0)+0=0+0=0 & 0+(0+0)=0+0=0 \\ (0+0)+1=0+1=1 & 0+(0+1)=0+1=1 \\ (0+1)+0=1+0=1 & 0+(1+0)=0+1=1 \\ (0+1)+1=1+1=0 & 0+(1+1)=0+0=0 \\ (1+0)+0=1+0=1 & 1+(0+0)=1+0=1 \\ (1+0)+1=1+1=0 & 1+(0+1)=1+1=0 \\ (1+1)+0=0+0=0 & 1+(1+0)=1+1=0 \\ (1+1)+1=0+1=1 & 1+(1+1)=1+0=1 \end{array}$$

   - La commutativité est immédiate de par la définition
   - 0 est l'élément neutre.
   - Tout élément a un opposé : 0 est l'opposé de lui-même, et de même 1 est l'opposé de lui-même.

   Par conséquent, $\mathbb{Z}/2\mathbb{Z}$ est un groupe abélien.
   (e) - Associativité. Soit $(x,y,z) \in (\mathbb{Z}/n\mathbb{Z})^3$. Soit $t = x \dot{+} y$. Ainsi, $t \equiv x+y \mod n$. Par conséquent, $(x \dot{+} y) \dot{+} z \equiv t+z \equiv x+y+z \mod n$ (on utilise ici l'associativité dans $\mathbb{Z}$). Puisque $(x \dot{+} y) \dot{+} z \in [\![0, n-1]\!]$, il en résulte que $(x \dot{+} y) \dot{+} z$ est le reste de la division euclidienne de $x+y+z$ par n. On montre de même que $x \dot{+} (y \dot{+} z) \equiv x+y+z \mod n$, puis que $x \dot{+} (y \dot{+} z)$ est aussi le reste de la division euclidienne de $x+y+z$ par n. Par conséquent, $(x \dot{+} y) \dot{+} z = x \dot{+} (y \dot{+} z)$
   - La commutativité résulte immédiatement de la commutativité de l'addition de $\mathbb{Z}$.
   - 0 est clairement l'élément neutre.
   - Si $x = 0$, il est opposé de lui-même. Soit $x \in [\![1, n-1]\!]$. L'entier $n-x$ est alors élément de $[\![1, n-1]\!]$, et puisque $x+(n-x) = n$, on obtient : $x \dot{+} (n-x) = 0$. Ainsi, $n-x$ est l'opposé de x. Tout élément admet donc un opposé.

   Cela montre que $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien.
   (f) $(\mathbb{R}^*, +)$ n'est pas un groupe : il ne possède pas d'élément neutre. En effet, pour tout $x \neq 0$, et tout $y \in \mathbb{R}^*$, $x+y \neq y$, et x n'est donc pas un neutre.
   $(\mathbb{R}^*, \times)$ en revanche est un groupe : la multiplication dans $\mathbb{R}^*$ est associative, commutative, 1 est un neutre, tout $x \in \mathbb{R}^*$ admet un opposé $x^{-1} = \dfrac{1}{x}$.
   Ainsi, $(\mathbb{R}^*, \times)$ est bien un groupe, et il est abélien.
   (g) Pareil !

(h) Erratum : il fallait considérer l'ensemble $\mathfrak{S}E$ des bijections de E dans lui-même ! Sinon les éléments ne sont bien sûr pas inversibles.

$\mathfrak{S}E$ est un groupe. En effet, la composition est associative, on dispose d'un neutre (la fonction identité id_E), et tout $f \in \mathfrak{S}E$ admet un inverse, à savoir la fonction réciproque f^{-1}.

Le groupe $\mathfrak{S}E$ n'est bien sûr pas abélien en général : la composition n'est pas commutative. Par exemple, soit $E = \{1, 2, 3\}$, et soit f définie par $f(1) = 2$, $f(2) = 1$ et $f(3) = 3$, et g définie par $g(1) = 1$, $g(2) = 3$ et $g(3) = 2$. Alors $g \circ f \neq f \circ g$. En effet $g \circ f(1) = 3$ alors que $f \circ g(1) = 2$.

Remarquez que pour montrer qu'une propriété est fausse, on cherche un contre-exemple. C'est la seule façon rigoureuse de faire.

2. • Associativité : soit (g, h), (g', h') et (g'', h'') trois éléments de $G \times H$. Alors :

$$[(g, h) \cdot (g', h')] \cdot (g'', h'') = (g \cdot g', h \cdot h') \cdot (g'', h'') = ((g \cdot g') \cdot g'', (h \cdot h') \cdot h'').$$

De la même façon,

$$(g, h) \cdot [(g', h') \cdot (g'', h'')] = (g \cdot (g' \cdot g''), h \cdot (h' \cdot h'').$$

Comme les lois de G et de H sont associatives, on en déduit que :

$$[(g, h) \cdot (g', h')] \cdot (g'', h'') = (g, h) \cdot [(g', h') \cdot (g'', h'')] .$$

• Élément neutre : soit 1_G et 1_H les éléments neutres de G et H. Alors $(1_G, 1_H)$ est élément neutre de $G \times H$. En effet, soit $(g, h) \in G \times H$, alors :

$$(g, h) \cdot (1_G, 1_H) = (g \cdot 1_G, h \cdot 1_H) = (g, h), \qquad \text{et} \qquad (1_G, 1_H) \cdot (g, h) = (1_G \cdot g, 1_H \cdot h) = (g, h).$$

• Inverse : soit $(g, h) \in G \times H$). Cet élément admet un inverse dans $G \times H$, donné par (g^{-1}, h^{-1}). En effet :

$$(g, h) \cdot (g^{-1}, h^{-1}) = (g \cdot g^{-1}, h \cdot h^{-1}) = (1_G, 1_H), \qquad \text{et} \qquad (g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} \cdot g, h^{-1} \cdot h) = (1_G, 1_H).$$

• Commutativité : si G et H sont abéliens, soit (g, h) et (g', h') deux éléments de $G \times H$. Alors :

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h') = (g' \cdot g, h' \cdot h) = (g', h') \cdot (g, h).$$

3. Soit G un groupe, et soit $H \subset G$ un sous-ensemble de G.

(a) Supposons que le sous-ensemble $H \subset G$ du groupe G vérifie les trois conditions. Alors, la stabilité de H par la loi de G permet de restreindre la loi de G en une loi sur H (c'est-à-dire une application de $H \times H$ vers H).
- Cette loi est associative, comme conséquence immédiate de l'associativité de la loi de G.
- Le neutre 1 de G est dans H. En effet, H est non vide. Il existe donc $x \in H$. Mais alors $x^{-1} \in H$, et par stabilité, $x \cdot x^{-1} \in H$, donc $1 \in H$. Le neutre 1 de G est clairement aussi neutre pour H.
- La stabilité de H par passage à l'inverse fournit la troisième propriété requise pour les groupes.

Ainsi, H est un groupe.

(b) On considère la loi $+$ de $\mathbb{R}$.
- Tout d'abord $\mathbb{Z} \subset \mathbb{R}$;
- $\mathbb{Z}$ est non vide, puisque $0 \in \mathbb{Z}$;
- pour tout $x, y \in \mathbb{Z}$, $x + y \in \mathbb{Z}$;
- si $x \in \mathbb{Z}$, alors $-x \in \mathbb{Z}$.

Par conséquent, $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$.

(c) • Tout d'abord, $n\mathbb{Z} \subset \mathbb{Z}$;
- $n\mathbb{Z}$ est non vide, puisqu'il contient 0 ;
- soit $x, y \in n\mathbb{Z}$. Alors $x \equiv 0 \mod n$ et $y \equiv 0 \mod n$, donc $x + y \equiv 0 \mod n$, et par conséquent $x + y \in n\mathbb{Z}$;
- soit $x \in n\mathbb{Z}$. Alors $x \equiv 0 \mod n$, et par conséquent $-x \equiv 0 \mod n$, donc $-x \in n\mathbb{Z}$.

Ainsi, d'après (3a), $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

(d) • On a $S^1 \subset \mathbb{C}$;
- $1 \in S^1$, donc S^1 n'est pas vide.
- Si z_1 et z_2 sont dans S^1, alors $|z_1 z_1| = |z_1| \cdot |z_2| = 1 \cdot 1 = 1$. Ainsi, $z_1 z_2$ est dans S^1.
- Si $z_1 \in S^1$, alors $z_1 \neq 0$, et $|z_1^{-1}| = |z_1|^{-1} = 1$.. Donc $z_1^{-1} \in S^1$.

Ainsi, S^1 est un sous-groupe de $(\mathbb{C}^*, \times)$.

(e) On l'a déjà montré dans (3a). Le but de la question était juste de bien vous faire remarquer ce point.

(f) On va montrer que $H \cap K$ est un sous-groupe de G. J'utilise une notation multiplicative.
- $H \cap G$ est non vide puisque $1 \in H$ et $1 \in K$, donc $1 \in H \cap K$.
- Soit $x, y \in H \cap K$. Alors $x, y \in H$, et comme H est un groupe, $x \cdot y \in H$. De même, $x \cdot y \in K$. Donc $x \cdot y \in H \cap K$.
- Soit $x \in H \cap K$. Alors $x \in H$, et comme H est un groupe, x est inversible dans H, c'est-à-dire $x^{-1} \in H$. De même, $x^{-1} \in K$. Ainsi, $x^{-1} \in H \cap K$.

On en déduit que $H \cap K$ est un sous-groupe de G.

(g) En revanche, $H \cup K$ n'a aucune raison d'être un sous-groupe. Considérez par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$. Ceci n'est pas un sous-groupe de $\mathbb{Z}$, puisqu'il n'est pas stable par l'addition : par exemple, $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Partie II – Morphismes de groupes

1. En prenant $x = y = 1_G$, on obtient : $f(1_G) \cdot f(1_G) = f(1_G \cdot 1_G) = f(1_G)$. Or, H étant un groupe, $f(1_G)$ est inversible dans H. Ainsi,

$$f(1_G)^{-1} \cdot f(1_G) \cdot f(1_G) = f(1_G)^{-1} \cdot f(1_G), \qquad \text{soit :} \qquad 1_H \cdot f(1_G) = 1_H, \qquad \text{soit :} \qquad f(1_G) = 1_H.$$

2. On commence par montrer que $\mathrm{Ker}(f)$ est un sous-groupe de G :
- Par définition, $\mathrm{Ker}(f) \subset G$;
- $\mathrm{Ker}(f)$ est non vide, puisqu'il contient 1_G, d'après la question précédente ;
- Soit $x, y \in \mathrm{Ker}(f)$. Alors $f(xy) = f(x)f(y) = 1_H \cdot 1_H = 1_H$. Donc $xy \in \mathrm{Ker}(f)$.
- Soit $x \in \mathrm{Ker}(f)$. Alors $f(x^{-1}) \cdot f(x) = f(x^{-1} \cdot x) = f(1_G) = 1_H$. Ainsi :

$$f(x^{-1}) = f(x^{-1}) \cdot f(x) \cdot f(x)^{-1} = 1_H \cdot f(x)^{-1} = 1_H \cdot 1_H^{-1} = 1_H.$$

Donc $x^{-1} \in \mathrm{Ker}(f)$.

On en déduit que $\mathrm{Ker}(f)$ est un sous-groupe de G.

Étudions maintenant $\mathrm{Im}(f)$.
- Par définition, $\mathrm{Im}(f) \subset H$;
- $\mathrm{Im}(f)$ est non vide, puisqu'il contient 1_H, d'après la question précédente (image de 1_G) ;
- Soit $y, y' \in \mathrm{Im}(f)$. Alors, il existe x et x' dans G tels que $f(x) = y$ et $f(x') = y'$. On en déduit que $f(xx') = f(x)f(x') = yy'$. Donc $yy' \in \mathrm{Im}(f)$.
- Enfin, si $y \in \mathrm{Im}(f)$, il existe x tel que $f(x) = y$; alors :

$$f(x^{-1})y = f(x^{-1})f(x) = f(x^{-1}x) = f(1_G) = 1_H,$$

et de même $yf(x^{-1}) = 1_H$. Ainsi, $y^{-1} = f(x^{-1})$, et par conséquent, $y^{-1} \in \mathrm{Im}(f)$.

On en déduit que $\mathrm{Im}(f)$ est un sous-groupe de H.

3. Exemples (attention, dans la plupart des exemples, les groupes sont additifs, et le neutre est 0 et non 1)

(a)
- f est un homomorphisme : Soit $m, m' \in \mathbb{Z}$. Alors :

$$f(m + m') = n \cdot (m + m') = n \cdot m + n \cdot m' = f(m) + f(m').$$

- Noyau : $f(m) = 0$ est équivalent à $n \cdot m = 0$. Deux cas se produisent : si $n = 0$, alors l'égalité est vérifiée pour tout $m \in \mathbb{Z}$, et $\mathrm{Ker}(f) = \mathbb{Z}$; sinon, $n \cdot m = 0$ si et seulement si $m = 0$, et donc $\mathrm{Ker}(f) = 0$.
- Image : $y \in \mathrm{Im}(f)$ si et seulement si il existe m tel que $y = n \cdot m$, c'est-à-dire si et seulement si y est divisible par n. Ainsi, $\mathrm{Im}(f) = n\mathbb{Z}$.

(b)
- f est un homomorphisme : Soit $m, m' \in \mathbb{Z}$. Alors $f(m) \equiv m \mod n$ et $f(m') \equiv m' \mod n$, d'où $f(m) + f(m') \equiv m + m' \mod n$. D'autre part, $f(m) \dot{+} f(m') \equiv f(m) + f(m') \mod n$, d'où finalement :

$$f(m) \dot{+} f(m') \equiv m + m' \mod n.$$

D'un autre coté, on a aussi $f(m + m') \equiv m + m' \mod n$. Ainsi, $f(m + m') \equiv f(m) \dot{+} f(m') \mod n$, et comme ils sont tous deux éléments de $\{0, \dots n-1\}$ par définition, on obtient l'égalité : $f(m + m') = f(m) \dot{+} f(m')$.

- Noyau : Soit $m \in \mathbb{Z}$. $f(m) = 0$ si et seulement si le reste de la division euclidienne de m par n est 0, donc si et seulement si m est divisible par n. Ainsi, $\mathrm{Ker}(f) = n\mathbb{Z}$.
- Image : Pour tout $m \in \{0, \dots, n-1\} = \mathbb{Z}/n\mathbb{Z}$, $f(m) = m$, et donc $m \in \mathrm{Im}(f)$. PAr conséquent, $\mathrm{Im}(f) = \mathbb{Z}/n\mathbb{Z}$.

(c)
- f est un homomorphisme : soit $x, y \in \mathbb{R}$. Alors $f(x+y) = \mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y = f(x)f(y)$.
Remarquez qu'ici, on a une loi additive pour le groupe de départ, et une loi multiplicative pour le groupe d'arrivée.
- Noyau : Le neutre de $(\mathbb{R}^*, \times)$ étant 1, il faut étudier $f^{-1}(1)$. Un réel x appartient à $\mathrm{Ker}(f)$ si et seulement si $\mathrm{e}^x = 1$, donc si $x = 0$. Ainsi, $\mathrm{Ker}(f) = \{0\}$.
- Image : La fonction exponentielle est croissante, de limites 0 et $+\infty$ en $-\infty$ et $+\infty$. Ainsi, d'après le théorème des valeurs intermédiaires (l'exponentielle est continue !), $\mathbb{R}_+^* \subset \mathrm{Im}(f)$. Puisque pour tout $x \in \mathbb{R}$, $\mathrm{e}^x > 0$, on a aussi $\mathrm{Im}(f) \subset \mathbb{R}_+^*$. Donc $\mathrm{Im}(f) = \mathbb{R}_+^*$.

(d) Un dernier exemple !
- f est bien à valeurs dans S^1, et f est un homomorphisme ; on fait à nouveau la remarque que loi loi du groupe d'arrivée est multiplicative. Soit $x, y \in \mathbb{R}$. Alors

$$f(x+y) = \mathrm{e}^{\mathrm{i}(x+y)} = \mathrm{e}^{\mathrm{i}\,x}\mathrm{e}^{\mathrm{i}\,y} = f(x)f(y).$$

- Noyau : Nous avons à résoudre l'équation $\mathrm{e}^{\mathrm{i}\,x} = 1$, dont les solutions sont les multiples de 2π. Ainsi, $\mathrm{Ker}(f) = 2\pi\mathbb{Z}$.
- Image : Soit $z \in S^1$. On utilise la notation exponentielle de z : il existe r et θ tels que $z = r\mathrm{e}^{\mathrm{i}\,\theta}$. r est le module de z, donc $r = 1$. Ainsi, $z = \mathrm{e}^{\mathrm{i}\,\theta} = f(\theta)$. Donc $z \in \mathrm{Im}(f)$. On en déduit que $\mathrm{Im}(f) = S^1$.

4. (a) Cas de la surjectivité. Si f est surjective, par définition : $\forall x \in H,\ \exists y \in G,\ f(y) = x$.
On en déduit que $\mathrm{Im}(f) = H$.
Réciproquement, si $\mathrm{Im}(f) = H$, pour tout $y \in H$, on a $y \in \mathrm{Im}(f)$, donc il existe $x \in H$ tel que $f(x) = y$, ce qui montre la surjectivité.

(b) Cas de l'injectivité. Si f est injective, alors $|f^{-1}(1_H)| \leqslant 1$. Comme $1_G \in f^{-1}(1_H)$, on en déduit que :

$$\mathrm{Ker}(f) = f^{-1}(1_H) = \{1_G\}.$$

Réciproquement, si $\mathrm{Ker}(f) = \{1_G\}$, soit x, y tels que $f(x) = f(y)$. Alors, puisque f est un homomorphisme, $f(xy^{-1}) = 0$. Ainsi, $xy^{-1} \in \mathrm{Ker}(f)$, puis $xy^{-1} = 1_G$, soit $x = y$. Cela prouve l'injectivité de f.

5. Sont injectifs : (3a) (si $n \neq 0$), (3c).
Sont surjectifs : (3a) (si $n = 1$), (3b), (3d)
Aucun n'est bijectif.

6. Soit G un groupe (additif), de neutre 0_G. On considère le groupe 0 de la question I-1c.

(a) S'il existe un morphisme $f : 0 \to G$, il vérifie $f(0) = 0_G$. Comme 0 est le seul élément du groupe nul, cette relation détermine entièrement f. Réciproquement, ceci définit de manière évidente un homomorphisme. Ainsi, il existe un unique homomorphisme de 0 vers G.
Son noyau est lui-même $\{0\}$, et sa seule image étant 0_G, son image est $\mathrm{Im}(f) = \{0_G\}$.
Ce morphisme est donc injectif, mais pas surjectif, sauf si $G = 0$. Il n'est donc un isomorphisme que si $G = 0$.

(b) S'il existe un morphisme $f : G \to 0$, pour tout $x \in G$, $f(x) \in 0$, donc $f(x) = 0$. Ainsi, il n'y a qu'une façon de définir f. Réciproquement, cela définit bien un homomorphisme (immédiat !). Donc il existe un unique homomorphisme $f : G \to 0$.
La seule image possible d'un élément de G est 0, donc $\mathrm{Im}(f) = \{0\}$. De plus, pour tout $x \in G$, $f(x) = 0$, donc $\mathrm{Ker}(f) = G$.
Il en résulte que f est surjective, et n'est injective que lorsque $G = 0$. Dans ce cas et seulement dans ce cas, f est un isomorphisme.

7. Soit $x, y \in G$. Alors :

$$g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x)g \circ f(y).$$

Donc $g \circ f$ est un homomorphisme.

Partie III – Suites exactes

1. Soit $i \in [\![1, n-2]\!]$.
   - Supposons que $f_{i+1} \circ f_i = 0$. Soit $y \in \mathrm{Im}(f_i)$. Alors il existe $x \in G_i$ tel que $f_i(x) = y$. Ainsi :
   $$f_{i+1}(y) = f_{i+1}(f_i(x)) = f_{i+1} \circ f_i(x) = 0.$$
   Donc $y \in \mathrm{Ker}(f_{i+1})$. Ainsi, $\mathrm{Im}(f_i) \subset \mathrm{Ker}(f_{i+1})$.
   - Réciproquement, si $\mathrm{Im}(f_i) \subset \mathrm{Ker}(f_{i+1})$, soit $x \in G_i$. Alors :
   $$f_{i+1} \circ f_i(x) = f_{i+1}(f_i(x)) = 0,$$
   car $f_i(x) \in \mathrm{Im}(f_i)$, donc $f_i(x) \in \mathrm{Ker}(f_{i+1})$.
2. (a) Si $0 \longrightarrow G \xrightarrow{f} H$ est une suite exacte, alors $\mathrm{Ker}(f) = \mathrm{Im}(0) = 0$. Donc f est injective. Réciproquement, si f est injective, alors $\mathrm{Ker}(f) = 0 = \mathrm{Im}(0)$.

   (b) Si $G \xrightarrow{f} H \longrightarrow 0$ est une suite exacte, alors $\mathrm{Im}(f) = \mathrm{Ker}(0) = H$, donc f est surjective. Réciproquement, si f est surjective, $\mathrm{Im}(f) = H = \mathrm{Ker}(0)$.
3. - Tout d'abord, le morphisme $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ est injectif (question II-5). Ainsi, cela fournit l'exactitude de la suite $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$.
   - L'image de $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ est $n\mathbb{Z}$ (question II-3a), et le noyau de $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est $n\mathbb{Z}$ aussi (question II-3b), d'où l'exactitude de la suite $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.
   - Le morphisme $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est surjectif (question II-5), d'où l'exactitude de $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$

   Ainsi, la suite $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$ est une suite exacte.
4. On vérifie d'abord que f et g sont des homomorphismes :
   $$\begin{aligned} &f(0+1) = f(1+0) = f(1) = 2 = f(0) + f(1) = f(1) + f(0);\\ &f(0+0) = f(0) = 0 = f(0) + f(0);\\ &f(1+1) = f(0) = 0 = f(1) + f(1). \end{aligned}$$
   D'autre part, g associe la parité : $g(x)$ vaut 0 si x est pair, et 1 si x est impair. Le respect de l'addition par g provient alors des règles usuelles de parité des sommes. Montrons maintenant que la suite est exacte.
   - f est injective. En effet, si $x \neq y$, alors $x = 0$ et $y = 1$, ou l'inverse. Supposons $x = 0$ et $y = 1$, l'autre cas étant similaire. Alors $f(x) = 0$ et $f(y) = 2$, donc $f(x) \neq f(y)$. Ainsi, f est injective, et $0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{f} \mathbb{Z}/4\mathbb{Z}$ est exacte.
   - L'image de f est $\{0, 2\}$, et le noyau de g est aussi clairement $\{0, 2\}$, d'où l'exactitude de la suite $\mathbb{Z}/2\mathbb{Z} \xrightarrow{f} \mathbb{Z}/4\mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z}$.
   - g est clairement surjective, d'où l'exactitude de $\mathbb{Z}/4\mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$

   Ainsi, la suite $0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{f} \mathbb{Z}/4\mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ est exacte.
5. Remarquez pour commencer que f et g sont des homomorphismes :
   en effet : $\forall (x, y) \in G^2,\ f(xy) = (xy, 1_H) = (x, 1_H)(y, 1_H) = f(x)f(y)$,
   et de même : $\forall ((x, y), (x', y')) \in (G \times H)^2,\ g((x, y)(x', y')) = g(xx', yy') = yy' = g(x, y)g(x', y')$.
   $G \longrightarrow G \times H$ est injective et $G \times H \longrightarrow H$ est surjective. Il suffit donc de s'assurer que $\mathrm{Ker}(g) = \mathrm{Im}(f)$.
   Or : $\forall x \in G, f(x) = (x, 1_H)$, donc $\mathrm{Im}(f) = G \times \{1_H\}$.
   De plus : $\mathrm{Ker}(g) = \{(x, y) \in G \times H \mid g(x, y) = 1_H, \text{ i.e. } y = 1_H\} = G \times \{1_H\}$.
   Ainsi, $\mathrm{Ker}(g) = \mathrm{Im}(f)$. Cela montre l'exactitude au centre de la suite.

   Ainsi, $0 \longrightarrow G \xrightarrow{f} G \times H \xrightarrow{g} H \longrightarrow 0$ est une suite exacte.

Partie IV – Lemme des quatre, lemme des cinq.

1. **Lemme des cinq, version faible.**

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0, \end{array}$$

(a) On suppose que α et γ sont injectives. Soit $x \in \mathrm{Ker}(\beta)$. Alors $\beta(y) = 0$, donc $g' \circ \beta(y) = 0$. En utilisant la commutativité du deuxième carré, $\gamma \circ g(y) = g' \circ \beta(y) = 0$. Comme γ est injective, cela implique $g(y) = 0$. Donc $y \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ (exactitude de la suite). Ainsi, il existe $y \in A$ tel que $f(y) = x$. Alors, $0 = \beta(x) = \beta \circ f(y) = f' \circ \alpha(y)$ (commutativité du deuxième carré). Comme f' et α sont injective (exactitude + hypothèse), $f' \circ \alpha$ est injective, et l'égalité $f' \circ \alpha(x) = 0$ implique $x = 0$. Ainsi, $\mathrm{Ker}(\beta) = \{0\}$, ce qui montre l'injectivité de β.

(b) Supposons que α et γ sont surjectives. Montrons que β est surjective. Soit $y \in B'$. Comme g et γ sont surjectives, il existe $x \in B$ tel que $\gamma \circ g(x) = g'(y)$. Ainsi,

$$g'(y - \beta(x)) = g'(y) - g' \circ \beta(x) = g'(y) - \gamma \circ g(x) = g'(y) - g'(y) = 0$$

(on a utilisé la commutativité du deuxième carré). Donc $y - \beta(x) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$. Il existe donc $z \in A'$ tel que $f'(z) = y - \beta(x)$. De plus, α étant surjective, il existe $t \in A$ tel que $\alpha(t) = z$. Alors $f' \circ \alpha(t) = y - \beta(x)$, et par commutativité du premier carré, $\beta(f(t)) = y - \beta(x)$. On en déduit que $y = \beta(x + f(t))$. Ainsi, $y \in \mathrm{Im}(\beta)$. L'homomorphisme β est donc surjectif.

(c) On applique simultanément les deux questions précédentes : α et γ sont injectives, donc β est injective ; α et γ sont surjectives, donc β est surjective. Ainsi, β est bijective.

2. **Lemme des quatre.**

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D', \end{array}$$

(a) Supposons β et δ injective, et α surjective. Alors, soit $x \in \mathrm{Ker}(\gamma)$. On a alors $\delta \circ h(x) = h' \circ \gamma(x) = h'(0) = 0$, et donc, puisque δ est injective, $h(x) = 0$. Ainsi, $x \in \mathrm{Ker}(h) = \mathrm{Im}(g)$. Il existe donc $y \in B$ tel que $g(y) = x$.
Alors $g' \circ \beta(y) = \gamma \circ g(y) = \gamma(0) = 0$. Ainsi, $\beta(y) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$. Il existe donc $z \in A'$ tel que $f'(z) = \beta(y)$. De plus, α étant surjective, il existe $t \in A$ tel que $\alpha(t) = z$. On en déduit que $\beta \circ f(t) = f' \circ \alpha(t) = f'(z) = \beta(y)$. Comme β est injective, il en résulte que $y = f(t)$, puis $x = g(y) = g \circ f(t)$.
Souvenons-nous que $\mathrm{Ker}(g) = \mathrm{Im}(f)$, et donc que $g \circ f = 0$. Ainsi, $x = g \circ f(t) = 0$. Par conséquent, $\mathrm{Ker}(\gamma) = \{0\}$, et γ est injective !

(b) Supposons α et γ surjectives et δ injective. Soit $x \in B'$. Comme γ est surjective, il existe $y \in C$ tel que $\gamma(y) = g'(x)$. Alors $\delta \circ h(y) = h' \circ \gamma(y) = h' \circ g'(x) = 0$ (car $h' \circ g' = 0$). Comme δ est injective, cela implique que $h(y) = 0$. Ainsi, $y \in \mathrm{Ker}(h) = \mathrm{Im}(g)$. Il existe donc $z \in B$ tel que $g(z) = y$.
Alors : $g' \circ \beta(z) = \gamma \circ g(z) = \gamma(y) = g'(x)$. Ainsi, $g'(x - \beta(z)) = 0$. Il en résulte que $x - \beta(z) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$. Donc, il existe $t \in A'$ tel que $f'(t) = x - \beta(z)$; α étant surjective, il existe $u \in A$ tel que $\alpha(u) = t$.
Alors : $\beta \circ f(u) = f' \circ \alpha(u) = f'(t) = x - b(z)$. On en déduit que $x = \beta(f(u) + z)$, donc $x \in \mathrm{Im}(\beta)$, ce qui montre que β est surjective. Ouf !

3. **Lemme des cinq, version forte.**

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E', \end{array}$$

(a) Comme α est surjective, et β et δ injectives, la question (2a) amène l'injectivité de γ
Comme ε injective et β et δ surjectives, la question (2b) amène la surjectivité de β.
Ainsi, β est un isomorphisme.

(b) La raisonnement précédent montre que pour que γ soit injective, il suffit que α soit surjective et β et δ injectives ; pour que γ soit surjective, il suffit que ε soit injective, et β et δ surjectives.

(c) Ainsi, pour que γ soit un isomorphisme, il suffit que β et δ soient des isomorphismes, que α soit surjective et que ε soit injective.

(d) La version faible du lemme des cinq est le cas particulier ou $A = A' = 0$ et $E = E' = 0$. Dans ce cas α et ε sont les homomorphismes nuls de 0 vers 0, et sont donc injectifs et surjectifs. La version faible du lemme des cinq résulte alors directement de la version forte.