stratégie de *dévissage* en groupes dit *simples* permet de l'attaquer. Contentons-nous ici d'observer qu'il n'y a qu'un nombre fini de telles classes d'isomorphismes pour n donné. En effet, d'après la remarque qui suit (transport de structure !), tout groupe d'ordre n est isomorphe à un groupe dont l'ensemble sous-jacent est $\{1, \dots, n\}$, et qu'il n'y a qu'un nombre fini de lois de composition sur un ensemble fini (exactement n^{n^2} sur $\{1, \dots, n\}$, et bien sûr la plupart d'entre elles ne sont pas des lois de groupe).

REMARQUE 2.5. (Transport de structure) *Soient G un groupe, X un ensemble et $\varphi : X \to G$ une bijection. Il existe une unique loi de groupe $\star$ sur X telle que φ soit un isomorphisme de groupes, à savoir $x \star y = \varphi^{-1}(\varphi(x)\varphi(y))$. La vérification est immédiate !* Suivant Bourbaki, on dit que la loi $\star$ est *déduite de celle de G par transport de structure via φ*. Autrement dit, on a simplement indexé les éléments de X par les éléments de G, disons $x_g = \varphi^{-1}(g)$, et posé $x_g \star x_h = x_{gh}$. Par ce procédé, tout ensemble peut être muni d'une loi de groupe. En effet, si X est fini à n éléments, toute bijection $X \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ munit X d'une loi de groupe (isomorphe à $\mathbb{Z}/n\mathbb{Z}$!) par transport de structure. De même, si X est infini, alors X est en bijection avec $(\mathbb{Z}/2\mathbb{Z})^{(X)}$ (Exercice 1.16 Chap. 1) et on peut donc transporter à X la loi de ce dernier. Ces lois étant arbitraires, elles ont toutefois peu d'intérêt en général.

Il existe en général plusieurs isomorphismes différents entre deux groupes isomorphes. Pour de nombreuses questions le choix importera peu, mais pas pour toutes. Si $f : G \to G'$ est un isomorphisme, tous les autres tels isomorphismes sont de la forme $f' = g \circ f$ où $g = f' \circ f^{-1}$ est un isomorphisme $G' \to G'$. Cela conduit à introduire la :

DÉFINITION 2.6. *Si G est un groupe, un automorphisme de G est un isomorphisme $G \to G$. L'ensemble de tous les automorphismes de G est un sous-groupe de S_G noté* $\mathrm{Aut}\, G$.

EXEMPLE 2.7. *Si $g \in G$, l'application $\mathrm{int}_g : G \to G, x \mapsto gxg^{-1}$, est un automorphisme appelé automorphisme intérieur associé à g, ou conjugaison par g.*

Même si de prime abord la notion d'isomorphisme a l'air plus importante que celle de morphisme, c'est cette dernière qui s'avère à l'usage la plus cruciale. Par exemple, pour montrer que deux groupes sont isomorphes, on définira souvent d'abord un morphisme entre les deux, et on essaiera ensuite de montrer qu'il est bijectif.

Notons que si $f : G \to G'$ est un morphisme, alors on a $f(1) = 1$ car $f(1) = f(1^2) = f(1)f(1)$. De plus, pour tout $x \in G$ on a $f(x^{-1}) = f(x)^{-1}$, car $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, et plus généralement $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{Z}$.

EXEMPLE 2.8. Pour $n \geq 2$, la signature d'une permutation définit un morphisme de groupes surjectif $\epsilon : \mathrm{S}_n \to \{\pm 1\}$ (nous le reverrons plus loin). Si V est un k-espace vectoriel de dimension finie non nul, le déterminant définit un morphisme surjectif $\det : \mathrm{GL}(V) \to k^\times$.

On note $\mathrm{Hom}(G, G')$ l'ensemble des morphismes de groupes de $G \to G'$. Il contient toujours au moins le *morphisme trivial* 1, envoyant tout $g \in G$ sur $1_{G'}$. Attention : il n'y a pas de loi de groupe naturelle sur $\mathrm{Hom}(G, G')$ en général, sauf si G' est abélien. Dans ce cas, on définit une loi de groupe sur $\mathrm{Hom}(G, G')$, $(f, f') \mapsto ff'$, en posant $(ff')(g) = f(g)f'(g)$ pour $g \in G$.

Il y a des liens forts entre sous-groupes et morphismes. Si $f : G \to G'$ est un morphisme de groupes, son *noyau* est défini par

$$\ker f = f^{-1}(\{1\}) = \{g \in G \mid f(g) = 1\}.$$

C'est manifestement un sous-groupe de G. Par exemple, le noyau de $\mathrm{GL}(V) \stackrel{\det}{\to} k^\times$ est un sous-groupe de $\mathrm{GL}(V)$ noté $\mathrm{SL}(V)$ et appelé *groupe spécial linéaire* de V. De même $\mathrm{Im} f = f(G)$ est un sous-groupe de G'. Plus généralement, on a :

PROPOSITION 2.9. *Soit $f : G \to G'$ un morphisme de groupes. Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'. Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.*

DÉMONSTRATION — Découle immédiatement des définitions et des identités $f(1) = 1$, $f(xy) = f(x)f(y)$ et $f(x^{-1}) = f(x)^{-1}$ pour $x, y \in G$. □

L'énoncé suivant est simple mais important.

PROPOSITION 2.10. *Soit $f : G \to G'$ un morphisme de groupes. Notons $\mathscr{A}$ l'ensemble des sous-groupes de G contenant* $\ker f$*, et $\mathscr{B}$ celui des sous-groupes de G' inclus dans* $\mathrm{Im}\, f$*, tous deux ordonnés par l'inclusion $\subset$. Alors les applications $\mathscr{A} \to \mathscr{B}, A \mapsto f(A)$, et $\mathscr{B} \to \mathscr{A}, B \mapsto f^{-1}(B)$, sont des bijections croissantes réciproques.*

DÉMONSTRATION — Noter que pour tout sous-ensemble $H \subset G$ on a $f(H) \subset f(G) = \mathrm{Im}\, f$, et pour H' sous-groupe de G' on a $\ker f = f^{-1}(\{1\}) \subset f^{-1}(H')$: les applications du (iii) sont bien définies. Le fait qu'elles soient croissantes viennent des faits généraux $f(X) \subset f(Y)$ pour toutes parties $X \subset Y$ de G, et $f^{-1}(X') \subset f^{-1}(Y')$ pour toutes parties $X' \subset Y'$ de G'.

Pour toute partie $H' \subset \mathrm{Im}\, f$, on a trivialement $f(f^{-1}(H')) = H'$. Il ne reste donc qu'à montrer que pour tout sous-groupe H de G contenant $\ker f$, on a $f^{-1}(f(H)) = H$. L'inclusion $H \subset f^{-1}(f(H))$ est encore évidente. Réciproquement, soit $g \in f^{-1}(f(H))$. On a $f(g) \in f(H)$, donc $f(g) = f(h)$ pour un certain $h \in H$, puis $f(gh^{-1}) = 1$ et donc $gh^{-1} = k$ avec $k \in \ker f$. On en déduit $g = kh \in H$ car H est un sous-groupe de G contenant $\ker f$. On a montré $H = f^{-1}(f(H))$. □

Nous appliquerons souvent ce résultat dans le cas où f est surjective, auquel cas $\mathscr{B}$ est l'ensemble de tous les sous-groupes de G'. Un second énoncé important est :

PROPOSITION 2.11. *Soit $f : G \to G'$ un morphisme de groupes. Alors les fibres non vides de f sont en bijection avec* $\ker f$*. En particulier :*

(i) f est injective si, et seulement si, on a $\ker f = \{1\}$.

(ii) si G est fini, on a $|G| = |\mathrm{Im}\, f|\, |\ker f|$.

DÉMONSTRATION — Soit $g \in G$. L'application $\mathrm{L}_g : G \mapsto G, x \mapsto gx$, est bijective, d'inverse $\mathrm{L}_{g^{-1}}$. Comme f est un morphisme de groupes, L_g et $\mathrm{L}_{g^{-1}}$ induisent des bijections réciproques entre $\ker f = f^{-1}(\{1\})$ et $f^{-1}(\{h\})$, où $h = f(g)$. Cela montre la première assertion. Le (i) et (ii) s'en déduisent. □

REMARQUE 2.12. *Tout morphisme injectif $f : G \to G'$ définit un isomorphisme de groupes $f : G \xrightarrow{\sim} f(G)$.*

En guise d'application des concepts de ce paragraphe, montrons le résultat suivant dû à Cayley.

PROPOSITION 2.13. *(Cayley) Tout groupe d'ordre fini n est isomorphe à un sous-groupe de S_n.*

Cela démontre d'une part le rôle central du groupe S_n en théorie des groupes finis, mais aussi toute la difficulté à classifier les sous-groupes de S_n en général.

DÉMONSTRATION — Pour $g \in G$ notons $\mathrm{L}_g : G \to G, x \mapsto gx$, la multiplication à gauche par g. C'est une bijection de G d'inverse $\mathrm{L}_{g^{-1}}$. De plus, on a $\mathrm{L}_g \circ \mathrm{L}_h = \mathrm{L}_{gh}$, autrement dit l'application $G \to \mathrm{S}_G, g \mapsto \mathrm{L}_g$, est un morphisme de groupes. Il est injectif, car $\mathrm{L}_g = \mathrm{id}_G$ entraîne $g = 1$ (prendre $x = 1$). C'est donc un isomorphisme sur son image (Remarque 2.12), qui est un sous-groupe de S_G. On conclut par le lemme général suivant, appliqué à une bijection $\{1, \ldots, n\} \to G$ (autrement dit, à une numérotation des éléments de G). □

LEMME 2.14. *Soit $\varphi : X \to Y$ une bijection. Alors l'application $\varphi_{X,Y} : \mathrm{S}_X \to \mathrm{S}_Y, \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$, est un isomorphisme de groupes.*

DÉMONSTRATION — On vérifie immédiatement que $\varphi_{X,Y}$ est un morphisme, ainsi que les égalités $\varphi_{X,Y} \circ (\varphi^{-1})_{Y,X} = \mathrm{id}_Y$ et donc $(\varphi^{-1})_{Y,X} \circ \varphi_{X,Y} = \mathrm{id}_X$ (par symétrie). □

On dispose de définitions naturelles de morphismes entre d'autres structures que les groupes. Un *morphisme de monoïdes* est une application $f : X \to Y$, avec X et Y des monoïdes, telle que $f(xy) = f(x)f(y)$ pour tout $x, y \in X$, et $f(1) = 1$.

DÉFINITION 2.15. *Un morphisme d'anneaux est une application $f : A \to B$, avec A et B des anneaux, qui est à la fois un morphisme de groupes additifs et de monoïdes multiplicatifs : pour tout $a, b \in A$ on a $f(a + b) = f(a) + f(b)$, $f(1) = 1$ et $f(ab) = f(a)f(b)$.*

Dans les deux cas, un isomorphisme est un morphisme bijectif (auquel cas, son inverse est également un morphisme). Tout (iso-)morphisme d'anneaux $A \to B$ induit un (iso-)morphisme de groupes $A^\times \to B^\times$. Plus généralement :

EXEMPLE 2.16. Tout morphisme d'anneaux $f : A \to B$ induit un morphisme d'anneaux $\mathrm{M}_n(A) \to \mathrm{M}_n(B), (m_{i,j}) \mapsto (f(m_{i,j}))$, et donc un morphisme de groupes $\mathrm{GL}_n(A) \to \mathrm{GL}_n(B)$. Par exemple, le morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}, k \mapsto \overline{k}$, induit un morphisme de groupes $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ (réduction modulo N).

EXEMPLE 2.17. Si V est un k-espace vectoriel de dimension finie, et si l'on se donne une k-base $e = (e_1, \ldots, e_n)$ de V, alors l'application $u \mapsto \mathrm{Mat}_e(u)$ (matrice associée) induit un isomorphisme d'anneaux $\mathrm{End}(V) \xrightarrow{\sim} \mathrm{M}_n(k)$, et donc un isomorphisme de groupes $\mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(k)$.

3. Groupes cycliques et monogènes

Soient G un groupe et $g \in G$. On s'intéresse au sous-groupe de G

$$\langle g \rangle := \{g^m \mid m \in \mathbb{Z}\}$$

engendré par g. Quand la loi de G est notée additivement, ce sous-groupe est aussi noté $\mathbb{Z}\, g = \{mg |\, m \in \mathbb{Z}\}$. Rappelons d'abord la classique : [4]

PROPOSITION 3.1. *Les sous-groupes de $\mathbb{Z}$ sont les $\mathbb{Z}n$ avec $n \in \mathbb{Z}$.*

DÉMONSTRATION — Soit H un sous-groupe de $\mathbb{Z}$. On peut supposer $H \neq \{0\}$, car $\{0\} = \mathbb{Z}\, 0$. L'ensemble $A = H \cap \mathbb{N}_{>0}$ est alors non vide (considérer $h \mapsto -h$), et possède donc un plus petit élément, que l'on note n. On a clairement $\mathbb{Z}n \subset H$. Soit $h \in H$. Par division euclidienne on a $h = an + b$ avec $a, b \in \mathbb{Z}$ et $0 \leq b < n$, mézalor $b = h - an \in H$ car H est un sous-groupe, donc $b = 0$ par minimalité de n, *i.e.* $h \in \mathbb{Z}n$. □

Soient G un groupe et $g \in G$. Considérons l'application

$$\varphi : \mathbb{Z} \to \langle g \rangle, \;\; m \mapsto g^m. \tag{5}$$

On constate que c'est un morphisme de groupe surjectif. Deux cas se présentent :

(Cas a) Soit φ est injectif, *i.e.* tous les éléments g^m, avec $m \in \mathbb{Z}$, sont distincts. On dit alors que g est *d'ordre infini*. Dans ce cas φ définit un isomorphisme $\mathbb{Z} \simeq \langle g \rangle$.

(Cas b) Soit φ n'est pas injectif. Dans ce cas, son noyau $\ker \varphi$ est un sous-groupe non $\{0\}$ de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un unique $n \geq 1$ par la Proposition 3.1. On dit alors que g est d'ordre fini, et l'entier n est appellé *ordre de g*, et parfois noté $\mathrm{ord}(g)$ ou $|g|$. Par construction, c'est le plus petit entier $m \geq 1$ vérifiant $g^m = 1$. Pour tout $m \in \mathbb{Z}$, on a aussi $g^m = 1 \Leftrightarrow n|m$.

PROPOSITION 3.2. *Soit $g \in G$ d'ordre fini n, alors $\langle g \rangle$ a exactement n éléments, à savoir $1, g, \ldots, g^{n-1}$, et on a un isomorphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \overline{m} \to g^m$.*

DÉMONSTRATION — La relation $g^n = 1$ entraîne $g^m \equiv g^{m'}$ pour $m \equiv m' \bmod n$. D'après la Proposition 2.1 Chap. 1, φ définit donc par passage au quotient une application $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \overline{m} \mapsto g^m$: c'est l'application de l'énoncé. Par définition de la loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, on constate que $\overline{\varphi}$ est un morphisme de groupes. Il est clairement surjectif. Mais son noyau est trivial car $g^m = 1$ équivaut à $\overline{m} = \overline{0}$ par le premier point : c'est donc un isomorphisme. Comme $\mathbb{Z}/n\mathbb{Z}$ admet pour représentants $\{0, 1, \ldots n-1\}$ (division euclidienne par n), on en déduit que $\langle g \rangle$ a exactement n éléments, à savoir les g^r pour $0 \leq r < n$. □

DÉFINITION 3.3. *Un groupe G est dit monogène s'il existe $g \in G$ avec $G = \langle g \rangle$. Un tel élément g est appelé générateur de G. On dit que G est cyclique s'il est monogène et fini.*

4. On préfère souvent la notation $n\mathbb{Z}$ pour $\mathbb{Z}n$. La seconde est pourtant plus naturelle du point de vue groupe, car on a $\langle n \rangle = \mathbb{Z}n$.

Par exemple, le groupe $\mathbb{Z}$ (additif) est monogène infini engendré par l'élément 1. De même, pour tout entier $n \geq 1$, le groupe μ_n (resp. $\mathbb{Z}/n\mathbb{Z}$) est cyclique d'ordre n engendré par $e^{2i\pi/n}$ (resp. $\overline{1}$). À isomorphisme près, les cas (a) et (b) ci-dessus montrent que ce sont les seules possibilités.

COROLLAIRE 3.4. *Un groupe G est monogène infini si, et seulement si, on a $G \simeq \mathbb{Z}$. Un groupe G est cyclique d'ordre $n \geq 1$ si, et seulement si, on a $G \simeq \mathbb{Z}/n\mathbb{Z}$.*

Dans les deux cas, l'isomorphisme construit fait correspondre au générateur g (arbitrairement choisi) de G le générateur fixe 1 (resp. $\overline{1}$) de $\mathbb{Z}$ (resp. $\mathbb{Z}/n\mathbb{Z}$). On a montré en particulier qu'il existe, à isomorphisme près, un unique groupe cyclique d'ordre n. Certains auteurs notent C_n un groupe cyclique arbitraire d'ordre n. En notation additive, il y a presque toujours intérêt à avoir en tête $\mathrm{C}_n = \mathbb{Z}/n\mathbb{Z}$. En notation multiplicative, et suivant les goûts, choisir $\mathrm{C}_n = \mu_n$ permet d'éviter parfois les confusions. [5]

Les générateurs du groupe $\mathbb{Z}$ sont les $k \in \mathbb{Z}$ tels que $\mathbb{Z}k = \mathbb{Z}$, *i.e.* $k = \pm 1$. Décrivons tous ceux d'un groupe cyclique d'ordre n, disons engendré par un élément g donné. Pour $k \in \mathbb{Z}$, on a les équivalences :

(a) l'élément g^k engendre G,

(b) le sous-groupe $\langle g^k \rangle \subset G$ contient g,

(c) il existe $k' \in \mathbb{Z}$ tel que $kk' \equiv 1 \bmod n$,

(d) $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(e) k et n sont premiers entre eux.

Seule l'équivalence (c) $\Leftrightarrow$ (e) n'est pas tautologique, mais c'est le théorème de Bezout. Par exemple, les générateurs de μ_n sont les racines *primitives* n-èmes de l'unité.

COROLLAIRE 3.5. *Un groupe cyclique d'ordre n a exactement $\varphi(n)$ générateurs.*

LEMME 3.6. *Si $g \in G$ est d'ordre fini n, et si $d \geq 1$, alors g^d est d'ordre fini égal à $\frac{n}{(n,d)}$. En particulier, si d divise n alors g^d est d'ordre n/d.*

DÉMONSTRATION — En effet, pour $k \in \mathbb{Z}$ on a

$$(g^d)^k = g^{dk} = 1 \;\Leftrightarrow\; n \,|\, dk \;\Leftrightarrow\; \frac{n}{(n,d)} \,|\, \frac{d}{(n,d)}k \;\Leftrightarrow\; \frac{n}{(n,d)} \,|\, k. \tag{6}$$

La dernière équivalence vient de ce que $\frac{n}{(n,d)}$ et $\frac{d}{(n,d)}$ sont premiers entre eux. □

Terminons par une description des sous-groupes d'un groupe cyclique. Si G est un groupe abélien, et pour $d \in \mathbb{Z}$, l'application $G \to G, x \mapsto x^d$, est un morphisme. Son image $G^{(d)} = \{x^d,\ x \in G\}$ est donc un sous-groupe (*puissances d-èmes*, c'est aussi $dG = \{dx,\ x \in G\}$ en loi additive). Son noyau est souvent noté $G[d] := \{g \in G \,|\, g^d = 1\}$ et appelé sous-groupe de *d-torsion* de G.

LEMME 3.7. *Soient $G = \langle g \rangle$ cyclique d'ordre n et $d \geq 1$ entier. Le sous-groupe $G^{(d)} = \langle\, g^d \,\rangle$ est cyclique d'ordre $n/(n,d)$, et on a $G[d] = \langle\, g^{n/(n,d)} \,\rangle = G^{(n/(n,d))}$.*

5. Une source potentielle de confusions est que $\mathbb{Z}/n\mathbb{Z}$ est muni d'une addition et d'une multiplication.

Démonstration — En effet, on a $G^{(d)} = \langle g^d \rangle$, et le Lemme 3.6 montre que g^d est d'ordre $n/(n,d)$. De plus, tout élément de G est de la forme g^k avec $k \in \mathbb{Z}$, et (6) montre que l'on a $(g^k)^d = 1 \iff \frac{n}{(n,d)} \mid k$. On a bien montré $G[d] = \langle g^{n/(n,d)} \rangle$. □

Proposition 3.8. *Soit G un groupe cyclique d'ordre n. L'application $d \mapsto G^{(d)}$ est une bijection de l'ensemble des diviseurs de n sur l'ensemble des sous-groupes de G, et pour deux diviseurs d, d' de n on a $d|d' \Leftrightarrow G^{(d)} \supset G^{(d')}$.*

En particulier, tout sous-groupe d'un groupe cyclique est cyclique, et uniquement déterminé par son ordre, car on a $|G^{(d)}| = n/d$ pour $d|n$.

Démonstration — Soit g un générateur de G. On applique la Proposition 2.10 (iii) au morphisme surjectif $\varphi : \mathbb{Z} \to G, m \mapsto g^m$, de noyau $n\mathbb{Z}$. Les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$ sont les $d\mathbb{Z}$ avec $n \in d\mathbb{Z}$, *i.e.* $d|n$. On conclut car on a $\varphi(d\mathbb{Z}) = \langle g^d \rangle = G^{(d)}$ et $d\mathbb{Z} \subset d'\mathbb{Z} \Leftrightarrow d'|d$. □

Décrivons maintenant les automorphismes d'un groupe cyclique.

Proposition 3.9. *Soit G un groupe cyclique d'ordre $n \geq 1$. Les automorphismes de G sont les $\varphi_k : g \mapsto g^k$, avec $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. De plus, l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), k \mapsto \varphi_k$, est un isomorphisme de groupes.*

Démonstration — Pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, l'application $\varphi_k : G \to G, g \mapsto g^k$, est bien définie car on a $g^n = 1$ pour tout $g \in G$. C'est clairement un morphisme de groupes. On a $\varphi_{kk'} = \varphi_k \circ \varphi_{k'}$ et $\varphi_1 = \mathrm{id}$: cela montre à la fois que φ_k est un isomorphisme pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, et que l'application $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), k \mapsto \varphi_k$, est un morphisme de groupes. Pour voir que φ est bijectif on fixe un générateur g_0 de G. On a $\varphi_k(g_0) = g_0^k$, et donc $g_0^k = g_0$ implique $k \equiv 1$ dans $\mathbb{Z}/n\mathbb{Z}$ car g_0 est d'ordre n, donc φ est injectif. Soit α un automorphisme quelconque de G. Il envoie le générateur g_0 sur un autre générateur, nécessairement de la forme g_0^k avec $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ par l'analyse ci-dessus. On a donc $\alpha(g_0) = \varphi_k(g_0)$, puis $\alpha = \varphi_k$ car g_0 engendre G. □

Terminons ce paragraphe par un rappel sur l'isomorphisme chinois des restes. Rappelons que si A et B sont deux anneaux, on dispose d'une structure d'anneau naturelle sur $A \times B$ appelé *anneau produit* : l'addition et la multiplication sont effectuées coordonnée par coordonnée, et le neutre multiplicatif est $(1,1)$.

Proposition 3.10. *(Isomorphisme chinois) Soient $m, n \in \mathbb{Z}$ premiers entre eux. L'application $\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, $k \mapsto (k \bmod n, k \bmod m)$ définit par passage au quotient un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Démonstration — Si on a $k \equiv k' \bmod mn$ alors $k \equiv k' \bmod n$ et $k \equiv k' \bmod m$: donc l'application de l'énoncé passe bien au quotient, et induit une application $f : \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $\overline{k} \mapsto (\overline{k}, \overline{k})$ pour tout $k \in \mathbb{Z}$. Ce f est trivialement un morphisme d'anneaux. Si $\overline{k}$ est dans $\ker f$, on a $m|k$ et $n|k$, et donc $mn|k$ car m et n sont premiers entre eux, *i.e.* $\overline{k} = 0$. Ainsi, f est injective, puis bijective car sa source et son but ont même cardinal mn : c'est un isomorphisme. □