Université Pierre et Marie Curie
Cours de cryptographie MM029 - 2009/10
Alain Kraus

Chapitre 0 - Rappels

L'objectif de ce chapitre est de rappeler quelques définitions et résultats de base concernant les groupes, les anneaux et les corps. Ces notions sont supposées connues et ne seront pas traitées explicitement en cours.

Table des matières

1. Définition d'un groupe 1
2. Sous-groupes 3
3. Classes modulo un sous-groupe - Théorème de Lagrange 4
4. Groupe quotient d'un groupe abélien 5
5. Sous-groupe engendré par un élément - Ordre d'un élément 6
6. Morphismes de groupes 8
7. Définition d'un anneau 10
8. Sous-anneaux - Idéaux 12
9. Anneau quotient 13
10. Groupe des éléments inversibles - Corps - Anneaux intègres 14
11. Morphismes d'anneaux 16

1. Définition d'un groupe

Afin de définir un groupe, il convient de se donner un ensemble G et une loi de composition sur interne sur G vérifiant certaines conditions.

Définition 0.1. *On appelle groupe un couple $(G, *)$ formé d'un ensemble G et d'une loi de composition $(x, y) \mapsto x * y$ sur G, tels que les trois conditions suivantes soient vérifiées :*

1) on a $x * (y * z) = (x * y) * z$ quels que soient $x, y, z \in G$ (associativité).

2) Il existe un élément $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$ (existence d'un élément neutre).

3) Pour tout $x \in G$, il existe un élément $y \in G$ tel que $x * y = y * x = e$ (existence d'un symétrique pour tout élément de G).

Si de plus, quels que soient $x, y \in G$, on a $x * y = y * x$ (commutativité), on dit que G est un groupe commutatif ou abélien. C'est la situation que l'on rencontrera dans ce cours.

Un groupe peut être fini ou infini. S'il est fini, on appelle ordre du groupe le nombre de ses éléments i.e. son cardinal.

Notation. Dans la définition ci-dessus, on a utilisé la notation abstraite $*$ pour définir la loi de composition sur G. En théorie des groupes, on note en fait la plupart du temps la loi de composition sous-jacente multiplicativement $(x, y) \mapsto xy$, ou bien additivement $(x, y) \mapsto x + y$. En notation multiplicative, on emploie le mot inverse au lieu du mot symétrique et l'inverse d'un élément x se note x^{-1}. Pour tous $x, y \in G$, on a alors la formule $(xy)^{-1} = y^{-1}x^{-1}$. En notation additive, on dit opposé au lieu de symétrique, et l'on note généralement 0 l'élément neutre et $-x$ l'opposé de x. Dans la pratique, la notation additive est utilisée uniquement pour les groupes abéliens. Cela étant, la notation multiplicative est aussi très souvent employée pour les groupes abéliens. Dans toute la suite, on appellera groupe multiplicatif, un groupe dont la loi de composition est notée multiplicativement, et groupe additif, un groupe dont la loi de composition est notée additivement.

Exemples 0.1.

1) L'ensemble réduit à un seul élément e, avec pour loi de composition $e * e = e$, est un groupe, appelé le groupe trivial.

2) L'ensemble $\mathbb{Z}$ des entiers relatifs muni de la loi de composition $(x, y) \mapsto x+y$ est un groupe commutatif, d'élément neutre 0. On l'appelle le groupe additif des entiers relatifs. En remplaçant $\mathbb{Z}$ par $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on obtient respectivement le groupe additif des nombres rationnels, celui des nombres réels et celui des nombres complexes.

3) L'ensemble $\mathbb{Q}^*$ des nombres rationnels non nuls, muni de la loi de composition $(x, y) \mapsto xy$, est un groupe commutatif, d'élément neutre 1. C'est le groupe multiplicatif des nombres rationnels non nuls. On définit de même les groupes multiplicatifs $\mathbb{R}^*$ et $\mathbb{C}^*$.

4) Soient X un ensemble et G un groupe multiplicatif. L'ensemble G^X des applications de X à valeurs dans G est un groupe muni de la loi de composition définie par

$$(fg)(x) = f(x)g(x) \quad \text{pour tous } f, g \in G^X \text{ et } x \in X.$$

5) **Produit direct de groupes.** Soient $G_1, \cdots, G_n$ des groupes multiplicatifs. Posons

$$G = G_1 \times \cdots \times G_n.$$

La loi de composition sur G définie par l'égalité

$$(x_1, \cdots, x_n).(y_1, \cdots, y_n) = (x_1y_1, \cdots, x_ny_n),$$

munit G d'une structure de groupe. L'élément neutre est $(e_1, \cdots, e_n)$ où e_i est l'élément neutre de G_i. L'inverse d'un élément $x = (x_1, \cdots, x_n)$ est donné par la formule

$$x^{-1} = (x_1^{-1}, \cdots, x_n^{-1}).$$

Le groupe $(G, .)$ est appelé le produit direct des groupes $G_1, \cdots, G_n$, ou bien le groupe produit de $G_1, \cdots, G_n$.

2. Sous-groupes

Soit G un groupe multiplicatif, d'élément neutre e.

Définition 0.2. *Soit H une partie de G. On dit que H est un sous-groupe de G si les conditions suivantes sont réalisées :*

1) l'élément e appartient à H.

2) Pour tous $x, y \in H$, l'élément xy est dans H.

3) Pour tout $x \in H$, l'inverse x^{-1} de x est dans H.

Un sous-groupe de G muni de la loi de composition induite par celle de G est un groupe. Une partie H de G est un sous-groupe de G si et seulement si H n'est pas vide, et si pour tous $x, y \in H$, l'élément xy^{-1} est aussi dans H. Si $(H_i)_{i\in I}$ est une famille de sous-groupes de G, l'intersection des H_i est un sous-groupe de G.

Exemples 0.2.

1) Les parties G et $\{e\}$ sont des sous-groupes de G. Le sous-groupe $\{e\}$ s'appelle le sous-groupe trivial de G.

2) Le sous-ensemble de $\mathbb{R}^*$ formé des nombres réels strictement positifs, ainsi que $\{\pm 1\}$, sont des sous-groupes de $\mathbb{R}^*$.

3) Si n est un entier relatif, la partie $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$. On verra dans le chapitre I que tous les sous-groupes de $\mathbb{Z}$ sont de cette forme.

4) Soit x un élément de G. Pour tout entier relatif k, on définit x^k comme suit[(1)] :

$$x^k = \begin{cases} x \cdots x \ (k \text{ facteurs}) & \text{si } \ k \geq 1 \\ e & \text{si } \ k = 0 \\ (x^{-1})^{-k} & \text{si } \ k < 0. \end{cases}$$

[(1)] Soient E un ensemble et $*$ une loi de composition sur E. On définit le composé d'éléments $x_1, \cdots, x_n$ de E par la formule de récurrence :

$$x_1 * x_2 * \cdots * x_n = (x_1 * x_2 * \cdots * x_{n-1}) * x_n.$$

Pour tout $x \in E$ et tout entier $n \geq 1$, on définit la puissance n-ième de x par la formule $x^n = x * \cdots * x$ (n facteurs). Supposons $*$ associative. Vérifions alors que pour tout entier p tel que $1 \leq p \leq n$, on a l'égalité

$$x_1 * \cdots * x_n = (x_1 * \cdots * x_p) * (x_{p+1} * \cdots * x_n).$$

Elle est vraie si $n = 1$. Supposons qu'elle le soit pour un produit de $n-1$ éléments où $n \geq 2$. Posons $x = x_1 * \cdots * x_n$. On a $x = (x_1 * \cdots * x_{n-1}) * x_n$. Soit p un entier compris entre 1 et n. L'égalité à prouver étant satisfaite si $p = n$, on peut supposer $p \leq n-1$. D'après l'hypothèse de récurrence, on a donc $x = \big((x_1 * \cdots * x_p) * (x_{p+1} \cdots * x_{n-1})\big) * x_n$. Puisque $*$ est associative, on obtient $x = (x_1 * \cdots * x_p) * \big((x_{p+1} \cdots * x_{n-1}) * x_n\big)$, d'où l'égalité annoncée.

Quels que soient les entiers relatifs k et k', on vérifie que l'on a les égalités

$$x^k x^{k'} = x^{k+k'}, \quad (x^k)^{-1} = x^{-k}, \quad (x^k)^{k'} = x^{kk'}.$$

Il en résulte que l'ensemble $\{x^k \mid k \in \mathbb{Z}\}$ est un sous-groupe abélien de G.

3. Classes modulo un sous-groupe - Théorème de Lagrange

Soient G un groupe multiplicatif, d'élément neutre e, et H un sous-groupe de G. On associe à H la relation binaire $\mathcal{R}$ sur G définie pour tous $x, y \in G$ par

$$x\mathcal{R}y \Longleftrightarrow x^{-1}y \in H. \tag{1}$$

C'est une relation d'équivalence sur G. La propriété de réflexivité résulte du fait que $e \in H$. Si x, y, z sont dans G, l'égalité $(x^{-1}y)^{-1} = y^{-1}x$ entraîne la propriété de symétrie. En ce qui concerne la transitivité, si l'on a $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x^{-1}y$ et $y^{-1}z$ sont dans H, donc $(x^{-1}y)(y^{-1}z) = x^{-1}z$ l'est aussi, d'où $x\mathcal{R}z$. Pour tout $x \in G$, la classe d'équivalence de x est l'ensemble

$$xH = \{xh \mid h \in H\}.$$

C'est la classe (à gauche) de x modulo H. L'ensemble des classes des éléments de G modulo H se note G/H. On a ainsi

$$G/H = \{xH \mid x \in G\}.$$

On déduit de ce qui précède le théorème de Lagrange, qui est à la base de toute la théorie des groupes finis. Si G est fini, il en est de même de H et G/H. Notons dans ce cas $|G|$, $|H|$ et $|G/H|$ leurs cardinaux respectifs.

Théorème 0.1 (Lagrange). *Supposons G fini. On a l'égalité $|G| = |H| \times |G/H|$. En particulier, l'ordre de H divise celui de G.*

Démonstration : Pour tout $x \in G$, les ensembles H et xH sont en bijection via l'application qui à h associe xh. Le résultat s'en déduit aussitôt car G est la réunion disjointe de ses classes d'équivalence modulo H.

Si l'ensemble G/H est fini (que G soit fini ou non), on dit que $|G/H|$ est l'indice de H dans G.

Exemple 0.3. Supposons G fini d'ordre un nombre premier. Les seuls sous-groupes de G sont G et $\{e\}$.

Remarque 0.1. Supposons que G soit un groupe abélien additif. La relation d'équivalence modulo H définie par (1) s'écrit alors sous la forme

$$x\mathcal{R}y \Longleftrightarrow x - y \in H.$$

Pour tout $x \in G$, la classe de x modulo H se note $x + H$. On a

$$x + H = \Big\{ x + h \;\Big|\; h \in H \Big\} \quad \text{et} \quad G/H = \Big\{ x + H \;\Big|\; x \in G \Big\}.$$

La classe modulo H de l'élément neutre de G est H.

Exemple 0.4. L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$

Prenons $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ où $n \in \mathbb{N}$. Quels que soient $x, y \in \mathbb{Z}$ on a l'équivalence

$$x \text{ et } y \text{ sont en relation modulo } n\mathbb{Z} \Longleftrightarrow x - y \in n\mathbb{Z}.$$

Deux entiers relatifs x et y sont donc en relation modulo $n\mathbb{Z}$ si et seulement si n divise $x - y$. Dans ce cas, on dit que x et y sont congrus modulo n et l'on écrit que l'on a la congruence $x \equiv y$ mod. n. Pour tout $x \in \mathbb{Z}$, la classe de x modulo $n\mathbb{Z}$ est

$$x + n\mathbb{Z} = \Big\{ x + nk \;\Big|\; k \in \mathbb{Z} \Big\}.$$

On la note souvent $\overline{x}$ lorsque l'entier n est sous-entendu. On dit aussi que c'est la classe de x modulo n. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est formé des classes d'équivalence modulo n.

Proposition 0.1. *Supposons $n \geq 1$. Alors $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et l'on a*

$$\mathbb{Z}/n\mathbb{Z} = \Big\{ \overline{0}, \overline{1}, \cdots, \overline{n-1} \Big\}.$$

Démonstration : Soit $a + n\mathbb{Z}$ un élément de $\mathbb{Z}/n\mathbb{Z}$. Il existe des entiers q et r tels que l'on ait $a = nq + r$ avec $0 \leq r < n$ (division euclidienne). Puisque $a - r \in n\mathbb{Z}$, on a donc $\overline{a} = \overline{r}$. Par ailleurs, quels que soient a et b distincts compris entre 0 et $n - 1$, l'entier n ne divise pas $a - b$, autrement dit, on a $\overline{a} \neq \overline{b}$, d'où le résultat.

On dispose de la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui à un entier a associe sa classe modulo n. Dans le cas où $n = 0$, et dans ce cas seulement, c'est une bijection.

4. Groupe quotient d'un groupe abélien

Soit G un groupe abélien additif, d'élément neutre 0. Soit H un sous-groupe de G. On définit sur l'ensemble quotient G/H une loi de composition $\oplus$ comme suit. Soient u, v des éléments de G/H. Il existe $x, y \in G$ tels que $u = x + H$ et $v = y + H$. On pose alors

$$u \oplus v = (x + y) + H, \tag{2}$$

autrement dit, $u \oplus v$ est la classe de $x + y$ modulo H. Il faut bien entendu vérifier que cette définition a un sens, i.e. que $u \oplus v$ ne dépend pas des représentants choisis x et y de u et v.

Considérons pour cela des représentants x' et y' respectivement de u et v. Par définition, $x - x'$ et $y - y'$ sont dans H. Puisque G est abélien, il en résulte que

$$(x - x') + (y - y') = x + y - (x' + y') \in H,$$

ce qui signifie que $x + y$ et $x' + y'$ sont en relation modulo H, d'où notre assertion.

Proposition 0.2. *L'ensemble G/H muni de la loi $\oplus$ est un groupe abélien. On l'appelle le groupe quotient de G par H.*

Démonstration : Le fait que la loi $+$ sur G soit associative et commutative entraîne qu'il en est de même de $\oplus$. L'élément neutre de $\oplus$ est $0 + H = H$ et pour tout $x \in G$, l'opposé de $x + H$ est $-x + H$, où $-x$ est l'opposé de x dans G, d'où le résultat.

Exemple 0.5. Le groupe additif $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

Soit n un entier naturel. En prenant pour $(G, +)$ le groupe des entiers relatifs $(\mathbb{Z}, +)$ et pour H le sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$, on obtient le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, \oplus)$. On notera toujours $+$ la loi $\oplus$ sur $\mathbb{Z}/n\mathbb{Z}$. Le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ ainsi défini est appelé le groupe additif des entiers relatifs modulo n. Quels que soient $a, b \in \mathbb{Z}$, on a d'après (2),

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

L'élément neutre de $\mathbb{Z}/n\mathbb{Z}$ est $n\mathbb{Z}$. On a par ailleurs

$$k\overline{a} = \overline{ka} \quad \text{pour tout } k \in \mathbb{Z}.$$

Proposition 0.3. *Supposons $n \geq 1$. Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ est d'ordre n et ses éléments sont les classes des entiers compris entre 0 et $n - 1$.*

5. Sous-groupe engendré par un élément - Ordre d'un élément

Soit G un groupe multiplicatif, d'élément neutre e. Pour tout $x \in G$, il existe un plus petit sous-groupe de G qui contient $\left\{x\right\}$, à savoir l'intersection des sous-groupes de G qui contiennent $\left\{x\right\}$.

Définition 0.3. *Soit x un élément de G. On appelle sous-groupe de G engendré par x, l'intersection des sous-groupes de G qui contiennent $\left\{x\right\}$. On le notera $< x >$.*

Lemme 0.1. *Soit x un élément de G. On a $< x >= \left\{x^k \mid k \in \mathbb{Z}\right\}$.*

Démonstration : On a vu que $\left\{x^k \mid k \in \mathbb{Z}\right\}$ est un sous-groupe de G. Il contient $\left\{x\right\}$, donc aussi $< x >$. Inversement, soit H un sous-groupe de G tel que x soit dans H. D'après

les propriétés de stabilité d'un sous-groupe, l'ensemble $\left\{x^k \mid k \in \mathbb{Z}\right\}$ est contenu dans H. Par suite, il est contenu dans $< x >$.

Exemples 0.6. Soit n un entier naturel.

1) Le sous-groupe de $\mathbb{Z}$ engendré par n est $n\mathbb{Z}$.

2) Le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de 1 est $\mathbb{Z}/n\mathbb{Z}$.

Définition 0.4. *Supposons G fini. Soit x un élément de G. On appelle ordre de x, l'ordre du sous-groupe de G engendré par x.*

Théorème 0.2. *Supposons G fini. Soit x un élément de G d'ordre m.*

1) On a $m \geq 1$ et m divise l'ordre de G.

2) On a $x^m = e$ et m est le plus petit entier $k \geq 1$ tel que $x^k = e$.

3) Pour tout $n \geq 1$, on a $x^n = e$ si et seulement si m divise n.

4) On a $< x >= \left\{e, x, \cdots, x^{m-1}\right\}$.

Démonstration : 1) La première assertion résulte du théorème de Lagrange.

2) Considérons l'ensemble A défini par l'égalité

$$A = \left\{k \in \mathbb{N} \;\middle|\; 1 \leq k \leq m \;\text{ et }\; x^k = e\right\}.$$

Il s'agit de démontrer que l'on a

$$A = \left\{m\right\}. \tag{3}$$

D'abord, A est non vide. En effet, si A était vide, les éléments $x, x^2, \cdots, x^m, x^{m+1}$, seraient distincts deux à deux et l'ordre de $< x >$ serait strictement plus grand que m (lemme 0.1). Soit u un élément de A. Tout revient à prouver que l'on a $u = m$. Posons

$$B = \left\{e, x, \cdots, x^{u-1}\right\}.$$

Vérifions que $< x >$ est contenu dans B. Soit k un entier relatif. Il existe q et r dans $\mathbb{Z}$ tels que l'on ait

$$k = uq + r \quad \text{avec} \quad 0 \leq r < u.$$

Vu que l'on a $x^u = e$, on obtient ainsi

$$x^k = (x^u)^q x^r = x^r \in B,$$

d'où l'assertion. Le cardinal de B étant au plus u, on a donc $m \leq u$. Puisque u appartient à A, on a aussi $u \leq m$, d'où $u = m$, puis l'égalité (3).

3) Soit n un entier ≥ 1 tel que $x^n = e$. Il existe des entiers q et r tels que $n = mq + r$ avec $0 \leq r < m$. On obtient $x^r = e$, d'où $r = 0$ (seconde assertion), donc m divise n. L'implication réciproque est immédiate.

4) En ce qui concerne la dernière assertion, on déduit de ce qui précède que le cardinal de l'ensemble $\left\{e, x, \cdots, x^{m-1}\right\}$ est m. Il est contenu dans $< x >$, qui est aussi d'ordre m, d'où le résultat.

Comme conséquence du théorème 0.2, on obtient :

Théorème 0.3. *Supposons G fini d'ordre n. Pour tout $x \in G$, on a $x^n = e$.*

6. Morphismes de groupes

Sauf précision contraire, les groupes considérés dans ce paragraphe sont implicitement supposés multiplicatifs.

Définition 0.5. *Soient G et G' des groupes. On appelle morphisme de groupes de G dans G', toute application $f : G \to G'$ telle que l'on ait*

$$f(xy) = f(x)f(y).$$

Exemples 0.7.

1) Soient $\mathbb{R}_+^*$ le sous-groupe de $\mathbb{R}^*$ formé des nombres réels strictement positifs et $\log : \mathbb{R}_+^* \to \mathbb{R}$ la fonction logarithme népérien. La formule

$$\log(xy) = \log(x) + \log(y),$$

définit un morphisme de $(\mathbb{R}_+^*, \times)$ à valeurs dans $(\mathbb{R}, +)$.

2) Soit G un groupe. Pour tout $a \in G$, l'application $f_a : \mathbb{Z} \to G$ définie par $f(n) = a^n$ est morphisme de groupes. En fait, pour tout morphisme f de $\mathbb{Z}$ dans G, il existe $a \in G$ tel que $f = f_a$, comme on le constate en posant $f(1) = a$.

3) Pour tout $n \geq 1$, la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme. Plus généralement, pour tout groupe abélien additif G et tout sous-groupe H de G, l'application $s : G \to G/H$ définie par $s(x) = x + H$ est un morphisme de groupes. Cela résulte de la définition de la loi de groupe sur G/H.

Lemme 0.2. *Soit $f : G \to G'$ un morphisme de groupes. Soient e et e' les éléments neutres de G et G' respectivement.*

1) On a $f(e) = e'$.

2) Pour tout $x \in G$, on a $f(x^{-1}) = f(x)^{-1}$.

Démonstration : Pour tout $x \in G$, on a $f(x) = f(xe) = f(x)f(e)$. Par suite, on a $f(x)^{-1}f(x) = f(x)^{-1}f(x)f(e)$, d'où $e' = f(e)$. On obtient alors

$$e' = f(xx^{-1}) = f(x)f(x^{-1}) \quad \text{et} \quad e' = f(x^{-1}x) = f(x^{-1})f(x).$$

Lemme 0.3. *Soient $f : M \to N$ et $g : N \to P$ des morphismes de groupes. L'application composée $g \circ f : M \to P$ est encore un morphisme de groupes. Si le morphisme $f : M \to N$ est une bijection de M sur N, alors son application réciproque est un morphisme.*

Démonstration : Soient x et y des éléments de M. On a les égalités

$$(g \circ f)(xy) = g\big(f(xy)\big) = g\big(f(x)f(y)\big) = g\big(f(x)\big)g\big(f(y)\big),$$

d'où la première assertion. En ce qui concerne la seconde, considérons des éléments u et v de N. Il s'agit de montrer que l'on a

$$f^{-1}(uv) = f^{-1}(u)f^{-1}(v). \tag{4}$$

Puisque f est une bijection de M sur N, c'est en particulier une injection. Il suffit donc de montrer que les images par f des deux membres de (4) sont égales, autrement dit que l'on a $uv = f\big(f^{-1}(u)f^{-1}(v)\big)$, ce qui résulte du fait que f soit un morphisme.

Définition 0.6. *Soient G et G' des groupes. On appelle isomorphisme de G sur G', tout morphisme bijectif de G sur G'. On dit que G et G' sont isomorphes s'il existe un isomorphisme de G sur G'.*

Exemple 0.8. La fonction logarithme est un isomorphisme de $\mathbb{R}_+^*$ sur $\mathbb{R}$, le morphisme réciproque étant la fonction exponentielle.

Noyau et image d'un morphisme de groupes

Lemme 0.4. *Soit $f : G \to G'$ un morphisme de groupes.*

1) Pour tout sous-groupe H de G, l'image $f(H)$ de H par f est un sous-groupe de G'.

2) Pour tout sous-groupe H' de G', l'image réciproque $f^{-1}(H')$ de H' par f est un sous-groupe de G.

Démonstration : La première assertion est laissée en exercice. Démontrons la seconde. Notons e et e' les éléments neutres de G et G' respectivement. Soit H'un sous-groupe de G'. On a $f(e) = e' \in H'$ donc e appartient à $f^{-1}(H')$. Par ailleurs, si x et y sont dans $f^{-1}(H')$, alors $f(x)$ et $f(y)$ sont dans H' et $f(xy) = f(x)f(y)$ appartient aussi à H', d'où $xy \in f^{-1}(H')$. De même, on a $f(x^{-1}) = f(x)^{-1} \in H'$, donc $x^{-1} \in f^{-1}(H')$.

Définition 0.7. *Soit $f : G \to G'$ un morphisme de groupes. On appelle image de f le sous-groupe $f(G)$ de G'. On appelle noyau de f le sous-groupe $f^{-1}\big(\{e'\}\big)$ de G, où e' est l'élément neutre de G', on le note souvent* $\mathrm{Ker}(f)$*. On a donc*

$$\mathrm{Ker}(f) = \Big\{x \in G \;\Big|\; f(x) = e'\Big\}.$$

Lemme 0.5. *Soit $f : G \to G'$ un morphisme de groupes. Pour que f soit injectif il faut et il suffit que* $\mathrm{Ker}(f)$ *soit réduit à l'élément neutre de G.*

Démonstration : Supposons f injectif. Soit x un élément de $\mathrm{Ker}(f)$. On a les égalités $f(x) = e' = f(e)$, d'où $x = e$. Supposons $\mathrm{Ker}(f) = \{e\}$. Soient x et y deux éléments de G tels que $f(x) = f(y)$. On a $f(x)f(y)^{-1} = e'$ i.e. $f(xy^{-1}) = e'$, d'où $xy^{-1} = e$ puis $x = y$.

Théorème 0.4 (Factorisation des morphismes de groupes). *Soient G un groupe abélien additif et f un morphisme de G dans un groupe G'. Le groupe quotient* $G/\mathrm{Ker}(f)$ *est isomorphe à $f(G)$, via l'application qui à $x + \mathrm{Ker}(f)$ associe $f(x)$.*

Démonstration : Soient x et y des éléments de G tels que $x - y$ appartienne à $\mathrm{Ker}(f)$. On a $f(x - y) = e'$, autrement dit, on a $f(x) = f(y)$. On obtient ainsi une application

$$h : G/\mathrm{Ker}(f) \to f(G)$$

définie pour tout $x \in G$ par l'égalité

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

C'est un morphisme. En effet, quels que soient $x, y \in G$, on a

$$h\big((x + y) + \mathrm{Ker}(f)\big) = f(x + y) = f(x)f(y) = h\big(x + \mathrm{Ker}(f)\big)h\big(y + \mathrm{Ker}(f)\big).$$

Par ailleurs, si $f(x) = e'$, x appartient à $\mathrm{Ker}(f)$, d'où $x + \mathrm{Ker}(f) = \mathrm{Ker}(f)$, donc h est injectif. Par définition, h est une surjection de $G/\mathrm{Ker}(f)$ sur $f(G)$, d'où le résultat.

Exemple 0.9. Soit U le groupe des nombres complexes de module 1. L'application $\mathbb{R} \to U$ qui à $t \in \mathbb{R}$ associe e^{it} (où $i^2 = -1$) est un morphisme de groupes surjectif de noyau $2\pi\mathbb{Z}$. En particulier, les groupes $\mathbb{R}/2\pi\mathbb{Z}$ et U sont isomorphes.

7. Définition d'un anneau

Définition 0.8. *On appelle anneau un triplet formé d'un ensemble A et de deux lois de composition sur A, une addition $(x, y) \mapsto x + y$ et une multiplication $(x, y) \mapsto xy$, tels que les conditions suivantes soient vérifiées :*

1) le couple $(A, +)$ est un groupe commutatif.

2) La multiplication est associative et possède un élément neutre.

3) La multiplication est distributive par rapport à l'addition, ce qui signifie que l'on a

$$x(y + z) = xy + xz \quad \text{et} \quad (x + y)z = xz + yz \quad \text{quels que soient } x, y, z \in A.$$

Si de plus la multiplication est commutative, autrement dit, si l'on a $xy = yx$ quels que soient $x, y \in A$, on dit que A est un anneau commutatif.

On notera 0 l'élément neutre de $(A, +)$ et 1, ou 1_A, l'élément neutre de A pour la multiplication. Rappelons que pour tout $x \in A$, il existe un élément de A, noté $-x$, tel que l'on ait $x + (-x) = 0$ ($-x$ est l'opposé de x).

Lemme 0.6. *Quels que soient $x, y, z \in A$, on a*

$$x(y - z) = xy - xz \quad et \quad (y - z)x = yx - zx.$$

Démonstration : D'après la condition 3, on a $x(y - z) + xz = x(y - z + z) = xy$ et $(y - z)x + zx = (y - z + z)x = yx$, d'où le lemme.

On en déduit par exemple les formules $x0 = 0x = 0$, $x(-y) = -xy$ et $(-y)x = -yx$. En particulier, $(-1)x = -x$. Par convention, on a

$$x^0 = 1_A \quad \text{pour tout } x \in A.$$

Un anneau réduit à un élément, i.e. pour lequel on a $1 = 0$, est dit nul.

Exemples 0.10.

1) En munissant $\mathbb{Z}$ des deux lois de composition usuelles (addition et multiplication) on obtient l'anneau des entiers relatifs, qui est commutatif. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition de la multiplication usuelles sont aussi des anneaux commutatifs.

2) **L'anneau $A[X]$.** Soit A un anneau commutatif. Un polynôme à une indéterminée à coefficients dans A est par définition une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui est nulle à partir d'un certain rang. Les a_n sont appelés les coefficients du polynôme. Sur cet ensemble de polynômes, on définit deux lois de composition, une addition et une multiplication. Si $P = (p_0, p_1, \cdots)$ et $Q = (q_0, q_1, \cdots)$ sont des polynômes à coefficients dans A, on pose

$$P + Q = (p_0 + q_0, p_1 + q_1, \cdots) \quad \text{et} \quad PQ = (s_0, s_1, \cdots) \quad \text{avec} \quad s_n = \sum_{i+j=n} p_i q_j.$$

On vérifie que l'on obtient ainsi un anneau commutatif. Pour tout $a \in A$, on note a le polynôme $(a, 0, \cdots, 0, \cdots)$. Posons $X = (0, 1, 0, \cdots, 0, \cdots)$. Pour tout entier $n \geq 1$, et tout $a \in A$, on vérifie alors que l'on a $aX^n = (0, \cdots, 0, a, 0, \cdots)$, où le $n + 1$-ième terme de la suite est a et où tous les autres sont nuls. Tout polynôme $P = (p_0, p_1, \cdots, p_n, 0, \cdots)$, dont les coefficients d'indices strictement plus grands que n sont nuls, s'écrit alors

$$P = p_0 + p_1 X + \cdots + p_n X^n,$$

qui est la notation polynômiale de P et que l'on utilise exclusivement. On note $A[X]$ l'anneau ainsi obtenu. Bien entendu, on peut désigner le polynôme $(0, 1, 0, \cdots)$ par d'autres lettres que X, pourvu que la lettre choisie n'ait pas été utilisée par ailleurs.

3) **Produit direct d'anneaux.** Soient $A_1, \cdots, A_n$ des anneaux. Il existe sur le produit cartésien

$$A = A_1 \times \cdots \times A_n$$

une structure d'anneau, l'addition et la multiplication étant données par les formules

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n), \tag{5}$$

$$(x_1, \cdots, x_n)(y_1, \cdots, y_n) = (x_1 y_1, \cdots, x_n y_n). \tag{6}$$

Si tous les anneaux A_i sont commutatifs, il en est de même de A. On dit que A est le produit direct des A_i, ou encore l'anneau produit des A_i. Notons que l'élément neutre multiplicatif de A est $(1_{A_1}, \cdots, 1_{A_n})$.

8. Sous-anneaux - Idéaux

Soient A un anneau et B une partie de A.

Définition 0.9. *On dit que B est un sous-anneau de A si les conditions suivantes sont vérifiées :*

1) B est un sous-groupe additif de A.

2) Quels que soient x et y dans B, le produit xy est dans B.

3) L'élément neutre multiplicatif 1_A appartient à B.

On vérifie que si B est un sous-anneau de A, alors B muni des deux lois de composition induites par celles de A est un anneau.

Exemples 0.11.

1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$, lui-même étant un sous-anneau de $\mathbb{C}$.

2) Soit i une racine carrée de -1 dans $\mathbb{C}$. L'ensemble $\mathbb{Z}[i]$ des éléments de la forme $a + ib$ avec $a, b \in \mathbb{Z}$ est sous-anneau de $\mathbb{C}$. On l'appelle l'anneau des entiers de Gauss.

Définition 0.10. *Supposons A commutatif. On dit que B est un idéal de A si les deux conditions suivantes sont vérifiées :*

1) B est un sous-groupe additif de A.

2) Quels que soient $x \in B$ et $y \in A$, le produit xy est dans B.

Exemples 0.12.

1) **Idéaux de $\mathbb{Z}$.** Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où n parcourt $\mathbb{N}$. En effet, ce sont les sous-groupes de $\mathbb{Z}$, et ils vérifient la condition 2 de la définition.

2) **Idéaux principaux.** Supposons A commutatif. Soit a un élément de A. L'ensemble des éléments de la forme ax, où x parcourt A, est un idéal de A. On l'appelle l'idéal principal engendré par a. On le note aA ou (a). Tous les idéaux de $\mathbb{Z}$ sont principaux.

3) L'ensemble $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$.

9. Anneau quotient

Considérons un anneau commutatif A et I un idéal de A. Puisque $(A, +)$ est un groupe abélien et que I est un sous-groupe de A, on peut associer à I la relation d'équivalence $\mathcal{R}$ sur A définie pour tous $x, y \in A$ par la condition

$$x\mathcal{R}y \Longleftrightarrow x - y \in I.$$

L'ensemble quotient A/I, muni de la loi de composition définie pour tous $x, y \in A$ par

$$(x + I) + (y + I) = (x + y) + I, \tag{7}$$

est un groupe abélien, d'élément neutre I i.e. la classe de 0. On va définir une seconde loi de composition sur A/I, appelée multiplication, de sorte que A/I soit, avec l'addition précedente, muni d'une structure d'anneau commutatif. Soient $x + I$ et $y + I$ des éléments de A/I. On définit la multiplication par la formule

$$(x + I)(y + I) = xy + I. \tag{8}$$

Pour que cette définition ait sens, il convient de vérifier qu'elle ne dépend pas des représentants x et y de $x+I$ et de $y+I$. Soient x' et y' dans A tels que $x+I = x'+I$ et $y+I = y'+I$. Il existe r et t dans I tels que $x = x' + r$ et $y = y' + t$. On a

$$xy = x'y' + (x't + ry' + rt).$$

Puisque r et t sont dans I, il en est de même de $x't+ry'+rt$, par suite, $xy-x'y'$ appartient à I, d'où notre assertion.

Théorème 0.5. *L'ensemble A/I muni de l'addition et la multiplication définies par les formules* (7) *et* (8) *est un anneau commutatif. On l'appelle l'anneau quotient de A par I.*

Démonstration : On sait déjà que $(A/I, +)$ est un groupe abélien. La multiplication dans A étant associative et commutative, il en est de même dans A/I comme on le constate directement. Par ailleurs, $1+I$ est l'élément neutre multiplicatif de A/I (car 1 est l'élément

neutre multiplicatif de A). Il reste à vérifier que la multiplication est distributive par rapport à l'addition. Soient x, y, z des éléments de A. On a les égalités

$$(x+I)\big((y+I)+(z+I)\big) = (x+I)\big((y+z)+I\big) = x(y+z)+I = xy+xz+I = (xy+I)+(xz+I),$$

par suite, on a

$$(x+I)\big((y+I)+(z+I)\big) = (x+I)(y+I)+(x+I)(z+I).$$

La deuxième égalité de la définition de la distributivité se vérifie de la même façon.

Exemples 0.13.

1) **L'anneau quotient** $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel non nul. On a vu que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est ainsi muni d'une structure d'anneau commutatif, pour laquelle l'addition et la multiplication sont données par (formules (7) et (8))

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a}\overline{b} = \overline{ab} \quad \text{quels que soient } a, b \in \mathbb{Z}.$$

L'élément neutre additif est $\overline{0} = n\mathbb{Z}$. L'élément neutre multiplicatif est $\overline{1} = 1 + n\mathbb{Z}$, i.e. est l'ensemble des entiers a tels que n divise $a - 1$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ s'appelle l'anneau des entiers modulo n.

2) Soit $F \in A[X]$ un polynôme à coefficients dans un anneau commutatif A. On peut considérer l'anneau quotient $A[X]/(F)$, où (F) est l'idéal principal de $A[X]$ engendré par F. Nous étudierons ces anneaux notamment si $A = \mathbb{Z}/p\mathbb{Z}$, où p est premier. Notons au passage que l'on peut poser comme définition $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$.

10. Groupe des éléments inversibles - Corps - Anneaux intègres

Définition 0.11. *Soient A un anneau et a un élément de A. On dit que a est un élément inversible de A s'il possède un inverse pour la multiplication, autrement dit, s'il existe $b \in A$ tel que l'on ait $ab = ba = 1$. On notera A^* l'ensemble des éléments inversibles de A.*

Si $a \in A$ est inversible, il existe un unique élément $b \in A$ tel que $ab = ba = 1$ et on le note a^{-1}. Si x et y sont dans A^*, le produit xy l'est aussi et son inverse est $y^{-1}x^{-1}$. La multiplication induit ainsi sur A^* une loi de composition. Plus précisément :

Proposition 0.4. *L'ensemble A^*, muni de la multiplication induite par celle de A, est un groupe. On l'appelle le groupe des éléments inversibles de A, ou le groupe des unités de A.*

On étudiera en détails dans le chapitre I le groupe $\big(\mathbb{Z}/n\mathbb{Z}\big)^*$ des éléments inversibles de l'anneau des entiers modulo n.

Lemme 0.7. *Soient A et B des anneaux. Le groupe des éléments inversibles de l'anneau produit $A \times B$ est $A^* \times B^*$. Autrement dit, on a $(A \times B)^* = A^* \times B^*$. En particulier, si A et B sont finis, on a $\big|(A \times B)^*\big| = |A^*||B^*|$.*

Démonstration : Soit (a, b) un élément inversible de $A \times B$. Il existe $(c, d) \in A \times B$ tel que $(a, b)(c, d) = (c, d)(a, b) = (1_A, 1_B)$. D'après la formule (6), on obtient ainsi les égalités $ac = ca = 1_A$ et $bd = db = 1_B$, ce qui prouve que $a \in A^*$ et que $b \in B^*$. Inversement, si (a, b) est un élément de $A^* \times B^*$, il existe $c \in A$ et $d \in B$ tels que $ac = ca = 1_A$ et $bd = db = 1_B$. Par suite, on a $(a, b)(c, d) = (c, d)(a, b) = (1_A, 1_B)$, d'où $(a, b) \in \big(A \times B\big)^*$.

Lemme 0.8. *Soient A un anneau commutatif et I un idéal de A. Alors, $I = A$ si et seulement si il existe un élément inversible dans I.*

Démonstration : Supposons qu'il existe $x \in I \cap A^*$. Dans ce cas, $xx^{-1} = 1$ est dans I, par suite, pour tout $y \in A$, l'élément $y.1 = y$ est aussi dans I, d'où $I = A$.

Définition 0.12. *Un anneau A est un corps si l'on a $1 \neq 0$, et si tout élément non nul de A est inversible i.e. si l'on a $A^* = A - \big\{0\big\}$.*

Par définion, un corps possède donc au moins deux éléments, à savoir 0 et 1. Si A est un anneau commutatif et est un corps, on dit que A est un corps commutatif. Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs.

Définition 0.13. *Soit K un corps. On appelle sous-corps de K tout sous-anneau L de K qui est un corps. On dit alors que K est un surcorps de L.*

Les seuls idéaux d'un corps commutatif K sont $\big\{0\big\}$ et K. Le produit de deux éléments non nuls dans un corps est non nul. Les corps commutatifs sont en particulier des anneaux intègres :

Définition 0.14. *Un anneau A est dit intègre s'il est commutatif, non réduit à 0 i.e. on a $1 \neq 0$, et si le produit de deux éléments non nuls de A est non nul.*

Les anneaux $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont intègres, et plus généralement, tout sous-anneau d'un corps commutatif est un anneau intègre.

Proposition 0.5. *Soit A un anneau intègre fini. Alors A est un corps.*

Démonstration : Soit a un élément non nul de A. Il s'agit de montrer que a est inversible. On considère pour cela l'application de A à valeurs dans A qui à x associe ax. Elle est injective, car pour tout $x, y \in A$, si l'on a $ax = ay$, alors, $a(x - y) = 0$ et puisque A est intègre, cela entraîne $x = y$. L'anneau A étant fini, cette application est donc aussi une surjection, en particulier, 1 possède un antécédent, autrement dit, il existe $b \in A$ tel que $ab = 1$ (et $ba = 1$ car A est commutatif), d'où le résultat.

Exemples 0.14.

1) Soit n un entier ≥ 1. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

2) Si A et B sont des anneaux non nuls, l'anneau produit $A \times B$ n'est jamais intègre, comme le montre l'égalité $(1,0)(0,1) = (0,0)$.

Définition 0.15. *Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.*

Définition 0.16. *Un anneau A est dit euclidien si les conditions suivantes sont satisfaites :*

1) il est intègre.

2) Il existe une application $\sigma : A - \{0\} \to \mathbb{N}$ telle que pour tous a et b dans A avec $b \neq 0$, il existe q et r dans A tels que l'on ait

$$a = bq + r \quad avec \quad r = 0 \quad ou \quad \sigma(r) < \sigma(b).$$

On dit que σ est un stathme euclidien.

Exemples 0.15. Les anneaux $\mathbb{Z}$ et $K[X]$, où K est un corps commutatif, sont des anneaux euclidiens. Il en est de même de $\mathbb{Z}[i]$.

Lemme 0.9. *Tout anneau euclidien est principal.*

Démonstration : Soient A un anneau euclidien et I un idéal non nul de A. Il existe a non nul dans I tel que $\sigma(a)$ soit minimum. Vérifions que $I = (a)$. Soit x un élément de I. Il existe q et r dans A tels que $x = aq + r$ avec $r = 0$ ou $\sigma(r) < \sigma(a)$. Puisque r est dans I, le caractère minimal de a entraîne $r = 0$, donc x est dans (a), d'où le résultat (l'inclusion inverse est immédiate).

11. Morphismes d'anneaux

Définition 0.17. *Soient A et B des anneaux. On appelle morphisme d'anneaux de A dans B, toute application f de A dans B vérifiant les conditions suivantes :*

1) on a les égalités

$$f(x+y) = f(x) + f(y) \quad et \quad f(xy) = f(x)f(y) \quad quels\ que\ soient\ x, y \in A.$$

2) On a $f(1_A) = 1_B$.

Par exemple, si A est un anneau commutatif et I un idéal de A, la surjection canonique $A \to A/I$, qui à x associe $x + I$, est un morphisme d'anneaux.

Lemme 0.10. *Soient $f : A \to B$ un morphisme d'anneaux et A', B' des sous-anneaux de A et B respectivement.*

1) L'image $f(A')$ est un sous-anneau de B.

2) L'image réciproque $f^{-1}(B')$ est un sous-anneau de A.

Démonstration : 1) On sait déjà que $f(A')$ est un sous-groupe additif de B. Par ailleurs, on a $f(1_A) = 1_B$ et $1_A \in A'$ d'où $1_B \in f(A')$. Si x et y sont dans $f(A')$, il existe u et v dans A' tels que $x = f(u)$ et $y = f(v)$, donc $xy = f(u)f(v) = f(uv)$ appartient à $f(A')$.

2) On a vu que $f^{-1}(B')$ est un sous-groupe de A. L'égalité $f(1_A) = 1_B \in B'$, entraîne que $1_A \in f^{-1}(B')$. Si x et y sont dans $f^{-1}(B')$, alors $f(x)$ et $f(y)$ sont dans B', et $f(xy) = f(x)f(y) \in B'$ d'où $xy \in f^{-1}(B')$.

De façon analogue aux morphismes de groupes, on démontre que l'application composée de deux morphismes d'anneaux est un morphisme d'anneaux, et que si un morphisme d'anneaux est une bijection, son application réciproque est aussi un morphisme d'anneaux.

Définition 0.18. *Soient A et B des anneaux. On appelle isomorphisme de A sur B tout morphisme d'anneaux bijectif de A sur B. S'il existe un isomorphisme entre A et B, on dit que A et B sont isomorphes.*

Lemme 0.11. *Soient A et B des anneaux commutatifs, $f : A \to B$ un morphisme d'anneaux et I un idéal de B. Alors, $f^{-1}(I)$ est un idéal de A.*

Démonstration : Considérons des éléments $x \in A$ et $y \in f^{-1}(I)$. L'élément $f(x)f(y)$ est dans I i.e. $f(xy) \in I$, donc $xy \in f^{-1}(I)$. L'assertion en résulte puisque $f^{-1}(I)$ est un sous-groupe additif de A.

Remarque 0.2. L'image d'un idéal par un morphisme n'est pas en général un idéal, comme le montre l'injection $\mathbb{Z} \to \mathbb{Q}$. Cela étant, A et B étant des anneaux commutatifs, si $f : A \to B$ est un morphisme surjectif de A sur B, et I un idéal de A, alors $f(I)$ est un idéal de B.

Définition 0.19. *Soit $f : A \to B$ un morphisme d'anneaux. On appelle noyau de f, et on note* $\mathrm{Ker}(f)$*, l'ensemble des éléments $x \in A$ tels que $f(x) = 0$. Le sous-anneau $f(A)$ de B s'appelle l'image de f.*

Théorème 0.6 (Factorisation des morphismes d'anneaux). *Soient A un anneau commutatif, B un anneau et $f : A \to B$ un morphisme d'anneaux. Alors,* $\mathrm{Ker}(f)$ *est un idéal de A, et l'anneau quotient $A/\mathrm{Ker}(f)$ est isomorphe à $f(A)$, via l'application qui à $x + \mathrm{Ker}(f)$ associe $f(x)$.*

Démonstration : Le fait que $\mathrm{Ker}(f)$ soit un idéal de A résulte directement des définitions. Notons $h : A/\mathrm{Ker}(f) \to f(A)$ l'application définie par

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

Compte tenu du théorème 0.4, on sait que h est bien définie et que c'est un isomorphisme de groupes. Par ailleurs, si $x + \mathrm{Ker}(f)$ et $y + \mathrm{Ker}(f)$ sont dans $A/\mathrm{Ker}(f)$, on a

$$h\big((x + \mathrm{Ker}(f))(y + \mathrm{Ker}(f))\big) = h\big((xy + \mathrm{Ker}(f))\big) = f(xy) = f(x)f(y),$$

qui n'est autre que $h\big((x + \mathrm{Ker}(f))\big)h\big((y + \mathrm{Ker}(f))\big)$. Puisque l'on a

$$h\big(1_A + \mathrm{Ker}(f)\big) = f(1_A) = 1_B,$$

h est donc un morphisme d'anneaux, d'où le résultat.

En illustration de ce qui précède, établissons l'énoncé suivant qui caractérise, à isomorphisme près, les anneaux quotients de $\mathbb{Z}$.

Proposition 0.6. *Soit A un anneau. Les conditions suivantes sont équivalentes :*

1) l'anneau A ne possède pas de sous-anneaux autres que lui-même.

2) Il existe $n \in \mathbb{N}$ tel que A soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration : Pour tout $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'a pas de sous-anneaux autres que lui-même. En effet, si B est un sous-anneau de $\mathbb{Z}/n\mathbb{Z}$, alors $\overline{1}$ est dans B, donc le sous-groupe engendré par $\overline{1}$, i.e. $\mathbb{Z}/n\mathbb{Z}$, est contenu dans B, d'où $B = \mathbb{Z}/n\mathbb{Z}$. En particulier, tout anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$, pour un certain entier n, possède cette propriété. Inversement, supposons la première condition réalisée. Considérons l'application $f : \mathbb{Z} \to A$ définie par $f(n) = n1_A$. C'est un morphisme d'anneaux. Son image est un sous-anneau de A. D'après l'hypothèse faite, on a donc $f(\mathbb{Z}) = A$. Par ailleurs, il existe $n \in \mathbb{N}$ tel que l'on ait $\mathrm{Ker}(f) = n\mathbb{Z}$. Par suite, A est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (th. 0.6).