Anneaux et arithmétique

1 Quelques rappels de théorie élémentaire des groupes

Ce qui suit contient, sans démonstration, le minimum vital en théorie des groupes pour pouvoir aborder l'étude des anneaux. Vous y trouverez quelques considérations sur les usages en matière (d'abus) de notations. Si vous vous ennuyez profondément en parcourant ces lignes, savez retrouver sans coup férir les démonstrations omises, et pouvez aisément rallonger les trop courtes listes d'exemples présentées, il est bien sûr inutile de vous attarder sur ce texte. *Si des passages vous posent difficulté, vous paraissent obscurs voire incompréhensibles, c'est un signal d'alarme et il faut tout faire pour y remédier*; les enseignants sont là pour vous y aider si besoin.

1.1 Lois de composition interne. Associativité, commutativité, élément neutre, symétrique

Définition 1. Soit E un ensemble. Une *loi de composition interne sur E* est une application $E \times E \to E$.

Remarque 1. Soit E un ensemble et $\varphi\colon E \times E \to E$ une loi de composition interne sur E. Si (x, y) est un couple d'éléments de E, un usage répandu en théorie des ensembles est d'utiliser la notation « fonctionnelle » $\varphi(x, y)$ pour désigner l'image de ce couple par l'application φ.

Cependant, dans le contexte des lois de composition interne, on utilise bien plus fréquemment la notation $x \ \varphi \ y$, et c'est naturellement ce que nous ferons dans ce cours. Ainsi, on note $2 + 3$ et non $+(2, 3)$ la somme des entiers 2 et 3. Le nom savant d'une telle notation est *notation infixée*.

Une autre notation moins pratiquée et très semblable à la notation fonctionelle est la notation dite *préfixée* (ou *polonaise*), consistant à noter $\varphi \ x \ y$ l'image de (x, y) par φ. Par exemple on notera $+ \ 2 \ 3$ la somme des entiers 2 et 3. L'un des avantages de ce type de notation est de rendre inutile le parenthésage, indispensable en notation infixée lorsque la loi φ n'est pas associative ou lorsque plusieurs lois sont en jeu. Ainsi les notations $\times \ + \ 4 \ 3 \ 5$ ou $\times \ 5 \ + \ 4 \ 3$ désignent $5 \times (4 + 3)$.

Définition 2. Soit E un ensemble muni d'une loi de composition interne $\star\colon E \times E \to E$.

- La loi $\star$ est dite *associative* si on a

$$\forall (f,g,h) \in E^3, \quad f \star (g \star h) = (f \star g) \star h.$$

- La loi $\star$ est dite *commutative* si on a

$$\forall (f,g) \in E^2, \quad f \star g = g \star f.$$

- Un *élément neutre* pour la loi $\star$ est un élément e de E vérifiant

$$\forall f \in E, \quad f \star e = e \star f = f.$$

Remarque 2. L'associativité permet de se passer de parenthèses dans les « compositions multiples ». Par exemple, si $\star$ est associative, on pourra écrire sans risque de confusion des expressions comme

$$f_1 \star f_2 \star f_3 \star f_4.$$

Cette expression n'a a priori rigoureusement aucun sens car elle peut s'interpréter comme $(f_1 \star f_2) \star (f_3 \star f_4)$ ou $(f_1 \star (f_2 \star (f_3 \star f_4)))$ ou d'autres façons encore. L'associativité nous dit que toutes les façons dont on peut placer des paires de parenthèses de façon à donner un sens rigoureux à l'expression ci-dessus donnent le même résultat.

Proposition 3. *Soit E un ensemble muni d'une loi de composition interne $\star$: $E \times E \to E$. On suppose que $\star$ admet un élément neutre. Alors un tel élément neutre est unique.*

Définition 4. Soit E un ensemble muni d'une loi de composition interne $\star$: $E \times E \to E$ admettant un élément neutre, noté e.

Soit $f \in E$. Un *symétrique* de f pour $\star$ est un élément $g \in E$ vérifiant

$$g \star f = f \star g = e.$$

Proposition 5. *Soit E un ensemble muni d'une loi de composition interne $\star$: $E \times E \to E$ associative et admettant un élément neutre. Soit $f \in E$. Si f admet un symétrique, ce symétrique est unique.*

1.2 Groupes

Définition 6. Un *groupe* est un couple $(G, \star)$ où G est un ensemble et $\star$ une loi de composition interne associative sur G, admettant un élément neutre, et tel que tout élément de G admet un symétrique

Un groupe $(G, \star)$ est dit *commutatif* (ou *abélien*) si la loi $\star$ est commutative.

Une telle définition sera stérile si l'on ne dispose pas d'un stock conséquent d'exemples « concrets » mobilisables facilement (*cf.* aussi la partie 1.6). Notamment, vous devriez être capable de rallonger de manière significative la liste fort succincte qui suit.

Exemples 3. Soit E un ensemble. On note $\mathfrak{S}_E$ l'ensemble des bijections de E sur lui-même. Alors $(\mathfrak{S}_E, \circ)$ est un groupe. Ce groupe est commutatif si et seulement si E est de cardinal au plus 2.

$(\mathbf{Z}, +)$ est un groupe commutatif.

Remarque 4. Nous y reviendrons en détail plus tard, mais on peut d'ores et déjà signaler que tout anneau commutatif unitaire $(A, +, \times)$ « porte naturellement en lui » deux groupes commutatifs, à savoir $(A, +)$ (le groupe commutatif sous-jacent) et $(A^\times, \times)$ (le groupe des éléments inversibles).

Définition 7. Soit $(G, \star)$ un groupe d'élément neutre e. Un *sous-groupe* de $(G, \star)$ est une partie H de G vérifiant les propriétés suivantes :

- e est dans H ;
- pour tout élément f de H, le symétrique de f appartient aussi à H ;
- pour tout couple (f, g) d'éléments de H, $f \star g$ appartient aussi à H.

Exemple 5. G et $\{e\}$ sont des sous-groupes de $(G, \star)$.

L'un des intérêts de la notion de sous-groupe réside dans la propriété suivante :

Proposition 8. *Soit $(G, \star)$ un groupe et H un sous groupe de G. Alors l'application*

$$\star_H : \begin{array}{ccc} H \times H & \longrightarrow & H \\ (h_1, h_2) & \longmapsto & h_1 \star h_2 \end{array}$$

est bien définie, et $(H, \star_H)$ est un groupe.

Remarque 6. Cette propriété, dont la démonstration peut apparaître (à juste titre !) comme essentiellement vide, est très utile dans la pratique pour montrer que certains ensembles munis d'une certaine loi de composition interne sont bien des groupes sans utiliser la définition 6.

De manière plus précise, soit H un ensemble muni d'une loi de composition interne $\otimes$. Pour montrer que $(H, \otimes)$ est un groupe, il suffit de trouver un groupe « connu » $(G, \star)$ tel que H est (plus généralement, est en bijection avec) un sous-ensemble de G qui est en outre un sous-groupe de $(G, \star)$ tel que les lois $\star_H$ et $\otimes$ coïncident. Dans la pratique, montrer que les conditions de la définition 7 sont vérifiées s'avère très souvent beaucoup moins laborieux que de montrer que les conditions de la définition 6 sont vérifiées, notamment parce que l'on évite ainsi d'avoir à montrer l'associativité de la loi considérée. En outre, il n'est pas rare que l'on puisse même se passer d'utiliser la définition 7 en identifiant H comme le noyau ou l'image d'un morphisme judicieusement choisi entre groupes connus (*cf.* la proposition 20), ce qui s'avère fréquemment encore plus efficace que l'utilisation de la définition 7

Bien sûr, cette technique sera d'autant plus mobilisable que l'on a à sa disposition un stock raisonnable de groupes « connus ».

1.3 Puissances itérées d'un élément d'un groupe

Définition 9. Soit $(G, \star)$ un groupe dont on note e l'élément neutre. Soit $g \in G$. On définit, pour tout $n \in \mathbf{Z}$, un élément $g^{\star n} \in G$ de la façon suivante :

1. pour tout $n \in \mathbf{N}$, on définit par récurrence $g^{\star n}$ en posant $g^{\star 0} = e$ et
$$\forall n \in \mathbf{N}, \quad g^{\star(n+1)} = g \star g^{\star n}.$$
2. Soit h le symétrique de g. Pour $n \in \mathbf{Z} \setminus \mathbf{N}$, on pose $g^{\star n} = h^{\star(-n)}$.

Proposition 10. Règles de calcul des puissances
Soit $(G, \star)$ un groupe dont on note e l'élément neutre. Soit $g \in G$.
On a $g^{\star 0} = e$ et $g^{\star 1} = g$; $g^{\star(-1)}$ est le symétrique de g.
On a
$$\forall (n, m) \in \mathbf{Z}^2, \quad g^{\star(m+n)} = g^{\star m} \star g^{\star n} = g^{\star n} \star g^{\star m}$$
$$\forall (n, m) \in \mathbf{Z}^2, \quad (g^{\star m})^{\star n} = g^{\star m\, n}$$
Soit h un autre élément de G. On suppose que g et h commutent, c'est-à-dire $g \star h = h \star g$. Alors on a
$$\forall n \in \mathbf{Z}, \quad (g \star h)^{\star n} = g^{\star n} \star h^{\star n} = h^{\star n} \star g^{\star n}$$

1.4 Notations : abus usuels, notations multiplicative et additive

En toute rigueur, un groupe, en tant qu'objet mathématique, est un *couple* $(G, \star)$, où G est un ensemble et $\star$ une loi de composition interne sur G. Très souvent la loi de composition interne n'est pas explicitement indiquée. On rencontre par exemple fréquemment des expressions du type « Soit G un groupe… » ou « Considérons le groupe $\mathfrak{S}_E$ des permutations de E… ». C'est en toute rigueur un abus de notation, qu'on peut exprimer de manière savante en disant qu'on « identifie un groupe à l'ensemble sous-jacent ». Cet abus est très largement toléré et pratiqué, et il en sera naturellement de même dans ce cours. J'ai pris soin jusqu'ici dans ce texte de ne *pas* pratiquer cet abus, mais je le ferai désormais, quoique non systématiquement. La plupart du temps, les problèmes créés par ce type d'abus sont minimes [1], soit parce que la loi de composition interne utilisée est « évidente » (par exemple, pour $\mathfrak{S}_E$, il s'agit a priori de la composition), soit parce que l'on va adopter (parfois implicitement) une des deux notations « génériques » [2] traditionnelles

1. Ou plutôt *devraient* être minimes. La pratique montre que ça n'est pas toujours le cas. N'hésitez pas à solliciter les enseignants en cas de doute ! Le moindre abus de notation est potentiellement dangereux au niveau pédagogique. D'un autre côté, la lourdeur notationnelle induite par le refus de pratiquer certains abus peut être considérée comme un frein à la pédagogie. Il me semble cependant clair que pratiquer un abus sans avoir pleinement conscience qu'il s'agit bien d'un abus et pourquoi expose fatalement à des confusions plus ou moins graves à plus ou moins brève échéance.
2. ce qui au passage constitue un autre abus de notation…

pour exprimer la loi de composition interne d'un groupe, à savoir la *notation multiplicative* ou la *notation additive*. Le tableau ci-dessous en donne les principales caractéristiques.

On insiste très lourdement sur le fait que la notation additive est STRICTEMENT réservée à des groupes *commutatifs*. Cette règle est *absolument inviolable*, car les risques de confusion causés par son non-respect sont extrêmement élevés. Par ailleurs le fait qu'un groupe soit commutatif n'entraîne pas systématiquement que l'on emploie la notation additive pour ce groupe. Cependant, ce sera *toujours* le cas pour le groupe commutatif sous-jacent à un anneau, sauf exceptions absolument rarissimes. Et ce ne sera *jamais* le cas pour le groupe (commutatif) des éléments inversibles d'un anneau.

La notation multiplicative s'emploie a priori pour n'importe quel type de groupe. L'usage veut en général que lorsque l'on ne précise pas explicitement la notation employée, on sous-entend que l'on utilise la notation multiplicative, au moins lorsque l'on travaille avec un groupe non nécessairement commutatif. Dans le doute, il est utile de préciser. On pourra écrire par exemple « Soit G un groupe noté multiplicativement… ».

Notation spécifique	Notation multiplicative	Notation additive
$g \perp h$	$g.h$ ou gh	$g + h$
$g^{\perp n}$, $n \in \mathbf{Z}$	g^n	$n \cdot g$ ou $n\,g$
élément neutre, e	1 ou e	0
« symétrique de g », $g^{\perp(-1)}$	« inverse de g », g^{-1}	« opposé de g », $-g$

Par « notation spécifique », on entend que l'on a choisi un symbole particulier pour désigner la loi du groupe sur lequel on travaille. Dans les exemples donnés par le tableau, ce symbole est $\perp$; jusqu'ici on avait utilisé $\star$; a priori n'importe quel symbole qui n'a pas déjà une signification mathématique dans le contexte où l'on se trouve convient ; si on travaille avec un groupe de permutations il est asez naturel d'utiliser le symbole $\circ$.

La frontière est parfois un peu floue entre notations spécifique et multiplicative. Par exemple, même quand la loi de groupe est désignée par un symbole spécifique, disons $\perp$ pour fixer les idées, les puissances itérées $g^{\perp n}$ sont très souvent notées simplement g^n. Ainsi la formule de calcul des puissances

$$\forall n \in \mathbf{Z}, \forall m \in \mathbf{Z}, \quad g^{\perp n} \perp g^{\perp m} = g^{\perp(m+n)}$$

s'écrira plus simplement

$$\forall n \in \mathbf{Z}, \forall m \in \mathbf{Z}, \quad g^n \perp g^m = g^{m+n}.$$

On prendra bien garde en revanche à ne JAMAIS mélanger la notation additive avec l'une des deux autres notations. Sinon, c'est le désastre assuré…

1.5 Morphismes de groupes ; noyaux et images

Un morphisme de groupes est une application d'un groupe vers un autre qui « respecte la structure de groupe ». Cette notion est l'analogue de celle d'application linéaire en théorie des espaces vectoriels (qui est souvent le premier exemple de morphisme de structures algébriques rencontré dans la scolarité). Moralement, exhiber un morphisme entre deux groupes nous dit qu'il existe un certain lien entre les structures de groupes mises en jeu, à condition que le morphisme ne soit en un sens pas trop « trivial ».

C'est intéressant par exemple quand l'un des groupes est « bien connu » et pas l'autre : cela amène une meilleure compréhension du groupe « moins bien connu ». Le lien est le plus étroit possible lorsque l'application est bijective : on a alors ce qu'on appelle un isomorphisme entre les deux groupes. Cela signifie moralement que les deux groupes sont « les mêmes », bien que les descriptions initiales de ces groupes diffèrent.

Définition 11. Soit $(G, \star)$ et $(H, \otimes)$ des groupes. Soit $\varphi \colon G \to H$ une application. On dit que φ est un *morphisme de groupes* si on a pour tout $(g, h) \in G^2$ la relation

$$\forall g_1 \in G, \forall g_2 \in G, \quad \varphi(g_1 \star g_2) = \varphi(g_1) \otimes \varphi(g_2).$$

Remarque 7. Si G et H sont notés multiplicativement, la relation s'écrit

$$\forall g_1 \in G, \forall g_2 \in G, \quad \varphi(g_1\, g_2) = \varphi(g_1)\varphi(g_2).$$

Si G et H sont commutatifs et notés additivement, la relation s'écrit

$$\forall g_1 \in G, \forall g_2 \in G, \quad \varphi(g_1 + g_2) = \varphi(g_1) + \varphi(g_2).$$

Exemples 8.

- Si G est un groupe, l'application identique Id_G de G est un morphisme de G dans lui-même.
- Si G et H sont des groupes, l'application $G \to H$ constante égale à l'élément neutre de H est un morphisme de groupes. En particulier il existe toujours au moins un morphisme d'un groupe dans un autre. La situation sera très différente pour les morphismes d'anneaux.
- L'application induite par l'inclusion d'un sous-groupe dans un groupe est un morphisme de groupes.
- L'exponentielle de $\mathbf{R}$ dans $\mathbf{R}^\times$ ou de $\mathbf{C}$ dans $\mathbf{C}^\times$ sont des morphismes de groupes.
- L'application $\mathbf{R} \to [0, 1[$ qui à un réel associe sa partie fractionnaire est un morphisme de groupes pour la loi de groupe sur $[0, 1[$ qui associe à $(x, y) \in [0, 1[^2$ la partie fractionnaire de $x + y$.

Proposition 12. *Soit $(G, \star)$ et $(H, \otimes)$ des groupes, d'éléments neutres respectifs e_G et e_H, et $\varphi : G \to H$ un morphisme de groupes. Alors « le neutre est envoyé sur le neutre, l'image du symétrique est le symétrique de l'image ». Plus formellement :*

1. *on a* $\varphi(e_G) = e_H$ *;*
2. *soit* $g \in G$ *et* g' *le symétrique de* g *; alors* $\varphi(g')$ *est le symétrique de* $\varphi(g)$*.*

Définition 13. Soit G et H des groupes. Un *isomorphisme de groupes* entre G et H est un morphisme de groupes $\varphi\colon G \to H$ tel qu'il existe un morphisme de groupes $\psi\colon G \to H$ tel que $\varphi \circ \psi = \mathrm{Id}_H$ et $\psi \circ \varphi = \mathrm{Id}_G$.

Deux groupes sont dits *isomorphes* s'il existe un isomorphisme de l'un sur l'autre.

Définition 14. Soit G un groupe. Un *automorphisme* (de groupes) de G est un isomorphisme de G sur lui-même. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Proposition 15.
- *Soit* φ *un morphisme de groupes bijectif. Alors l'application réciproque de* φ *est encore un morphisme de groupes.*
- *La composée de deux morphismes de groupes en est un.*

Corollaire 16. *Soit* G *et* H *des groupes. Un morphisme de groupes* $\varphi\colon G \to H$ *est un isomorphisme si et seulement s'il est bijectif.*

Corollaire 17. *Soit* G *un groupe. Alors* $\mathrm{Aut}(G)$ *est un sous-groupe du groupe* $\mathfrak{S}_G$*. En particulier* $\mathrm{Aut}(G)$ *est un groupe pour la composition.*

Proposition 18. *Soit* $\varphi : (G, \star) \to (H, \otimes)$ *un morphisme de groupes. On a*

$$\forall g \in G, \quad \forall n \in \mathbf{Z}, \quad \varphi(g^{\star n}) = \varphi(g)^{\otimes n}.$$

Définition 19. Soit $(G, \star)$ et $(H, \otimes)$ des groupes, $\varphi : G \to H$ un morphisme de groupes et e_H l'élément neutre de H.
- Le *noyau* de φ, noté $\mathrm{Ker}(\varphi)$ est le sous-ensemble de G défini par

  $$\mathrm{Ker}(\varphi) = \{g \in G, \quad \varphi(g) = e_H\}.$$

  En d'autres termes, $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{e_H\})$.
- L'*image* de φ est l'image directe $\varphi(G)$ de G par l'application φ ; on la note parfois $\mathrm{Im}(\varphi)$.

Proposition 20. *Soit* $(G, \star)$ *et* $(H, \otimes)$ *des groupes,* e_G *l'élément neutre de* G *et* $\varphi : G \to H$ *un morphisme de groupes.*
- *Soit* K *un sous-groupe de* H *; alors* $\varphi^{-1}(K)$ *est un sous-groupe de* G*. En particulier* $\mathrm{Ker}(\varphi)$ *est un sous-groupe de* G*.*
- *Soit* F *un sous-groupe de* G *; alors* $\varphi(F)$ *est un sous-groupe de* H*. En particulier, si* φ *est injectif, tout sous-groupe de* G *est isomorphe à un sous-groupe de* H*.*
- *Le morphisme* φ *est injectif si et seulement si* $\mathrm{Ker}(\varphi) = \{e_G\}$*.*

Remarque 9. Ainsi plus le noyau est « petit », plus le morphisme est « proche » d'être injectif, et plus G est « proche » d'être (isomorphe à) un sous-groupe de H.

Remarque 10. Cette proposition fournit dans de nombreux cas un moyen pratique de montrer qu'une certaine partie d'un groupe en est un sous-groupe (et donc est elle-même un groupe pour la loi induite) : il suffit en effet de montrer que c'est le noyau ou l'image d'un certain morphisme entre groupe « connus » ; *cf.* la remarque 6.

1.6 Tout groupe est isomorphe à un groupe de permutations d'un ensemble

Attention, on n'a pas écrit « au groupe de permutations d'un ensemble ». Par « à un groupe de permutations d'un ensemble » on sous-entend « à un sous-groupe du groupe des permutations d'un ensemble ».

Théorème 21. Théorème de Cayley

Soit G un groupe. Alors il existe un ensemble E tel que G est isomorphe à un sous-groupe de $\mathfrak{S}_E$.

Remarque 11. En fait le théorème est plus précis puisqu'il affirme que G est isomorphe à un sous-groupe de $\mathfrak{S}_G$. Pour montrer cela, on peut par exemple montrer que l'application

$$\begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_G \\ g & \longmapsto & (h \mapsto gh) \end{array}$$

est bien définie et est un morphisme de groupes injectif.

Remarque 12. Le théorème de Cayley permet en un sens de « désacraliser » la définition « abstraite » 6 et ouvre la voie à une introduction sans doute plus « motivée » de la théorie des groupes.

L'idée est que dans de nombreux contextes on ressent assez naturellement le besoin de travailler avec un certain sous-ensemble de l'ensemble des permutations d'un ensemble E, notamment lorsque E est muni de structures supplémentaires. Par exemple si E est muni d'une structure d'espace vectoriel sur un corps, on ne souhaite travailler qu'avec les permutations de E qui sont des applications linéaires. Galois avait remarqué qu'on pouvait obtenir des renseignements intéressants sur l'ensemble E des racines d'un polynôme à coefficients rationnels en étudiant l'ensemble des permutations de E vérifiant une certaine propriété « algébrique » [3].

Par ailleurs, on se rend facilement compte que pour travailler de manière raisonnable avec un sous-ensemble S de l'ensemble de permutations d'un ensemble, certaines conditions

3. Plus précisément, il s'agit de l'ensemble des permutations des racines telles que toute relation algébrique à coefficients dans $\mathbf{Q}$ satisfaite par les racines reste encore vérifiée après application de la permutation ; cette ensemble de permutations est précisément ce que l'on appelle le groupe de Galois de l'équation ; *cf.* par exemple la section *Permutation group approach to Galois theory* de la page Wikipedia *Galois theory* pour des exemples concrets.

naturelles se dégagent : l'ensemble S doit être non vide, stable par composition et passage à l'inverse. C'est le cas pour les deux exemples précités, et dans d'innombrables autres situations d'origine géométrique, arithmétique ou autres.

Ainsi on pourra définir un « groupe de permutations » comme étant une partie non vide de l'ensemble des permutations d'un ensemble, stable par composition et passage à l'inverse. Le théorème de Cayley dit qu'un groupe « abstrait » n'est jamais rien d'autre, à isomorphisme près, qu'un groupe de permutations, et en particulier la définition d'un groupe « abstrait » ne tombe pas du ciel.

Il est à noter qu'identifier un groupe « abstrait » à un groupe de permutation ne sera pas toujours considéré, loin de là, comme la meilleure façon d'appréhender ce groupe. Qui ressentirait le besoin systématique de considérer le groupe additif $\mathbf{Z}$ des entiers relatifs comme un sous-groupe de $\mathfrak{S}_{\mathbf{Z}}$ ou de tout autre groupe de permutations ? Ceci justifie notamment l'intérêt de la définition « abstraite », même si le théorème de Cayley montre que l'on pourrait s'en passer.

1.7 Groupe quotient

On se limite ici au cas du quotient d'un groupe commutatif par un sous-groupe. Naturellement, la notion plus générale de quotient d'un groupe par un sous-groupe distingué est aussi très utile, mais nous nous en servirons très peu dans le contexte de ce cours.

Théorème 22. *Soit G un groupe commutatif, H un sous-groupe de G. Il existe un groupe commutatif K et un morphisme de groupes surjectif $\pi\colon G \to K$ de noyau H.*

Le couple (K, π) est unique à isomorphisme unique près.

Remarque 13. La dernière assertion signifie concrètement ce qui suit : soit (K_i, π_i), $i \in \{1, 2\}$, deux couples où K_i est un groupe commutatif et $\pi_i\colon G \to K$ un morphisme surjectif de noyau H. Alors il existe un *unique* isomorphisme de groupes $\varphi\colon K_1 \to K_2$ tel que $\varphi \circ \pi_1 = \pi_2$

Le groupe K de l'énoncé est appelé *groupe quotient* (de G par H) et noté G/H. Le morphisme π est appelé *morphisme quotient*. L'énoncé d'unicité nous permet moralement de parler « du » groupe quotient de G par H et « du » morphisme quotient.

Remarque 14. La démonstration usuelle de l'*existence* d'un couple (K, π) vérifiant les propriétés de l'énoncé consiste à prendre pour ensemble sous-jacent à K l'ensemble quotient de G pour la relation d'équivalence $\mathcal{R}$ sur G définie (en notation additive) par

$$\forall x \in G, \quad \forall y \in G, \quad x \mathcal{R} y \iff x - y \in H$$

Soit alors $\pi\colon \begin{array}{ccc} G & \longrightarrow & K \\ x & \longmapsto & \overline{x} \end{array}$ l'application qui à $x \in G$ associe sa $\mathcal{R}$-classe d'équivalence. Pour $x, y \in G$, on pose alors $\overline{x} + \overline{y} := \overline{x + y}$. On vérifie que ceci est bien défini, qu'on obtient ainsi une loi de composition interne sur K qui en fait un groupe, et que π est alors un morphisme de groupes de noyau H.

Tout ceci est plus laborieux qu'autre chose. Peut-être encore pire, la connaissance de cette construction n'aide pas nécessairement à comprendre comment « fonctionne » la notion de quotient [4]. Vous pouvez faire par exemple le parallèle avec les constructions de l'ensemble des nombres réels : savoir qu'un nombre réel peut en toute rigueur être construit comme (disons) une classe d'équivalence de suites de Cauchy à valeurs dans $\mathbf{Q}$ n'aide sans doute pas à mieux manipuler les nombres réels.

La démonstration de l'unicité à isomorphisme unique près est totalement indépendante de la démonstration de l'existence et est déjà bien plus représentative d'une « bonne » façon d'appréhender les quotients.

Exemple 15. L'application $\mathbf{R} \to [0,1[$ qui à un réel associe sa partie fractionnaire (*cf.* exemples 8) est le morphisme quotient de $\mathbf{R}$ par $\mathbf{Z}$.

Il en est de même de l'application $\mathbf{R} \to \mathbf{U}$ qui à $t \in \mathbf{R}$ associe $\exp(2\,i\,\pi\,t)$, où $\mathbf{U}$ désigne le groupes des nombres complexes de module 1.

Théorème 23. Propriété universelle du groupe quotient *Soit G un groupe commutatif, H un sous-groupe de G, $\pi\colon G \to G/H$ le morphisme quotient.*

- *Soit K un groupe et $\varphi\colon G \to K$ un morphisme de groupes dont le noyau contient H. Alors il existe un unique morphisme $\psi\colon G/H \to K$ tel que $\psi \circ \pi = \varphi$*
- *Soit K un groupe et $\theta\colon G \to K$ un morphisme de groupes vérifiant la propriété suivante : pour tout groupe L et tout morphisme de groupes $\varphi\colon G \to L$ dont le noyau contient H il existe un unique morphisme $\psi\colon K \to L$ tel que $\psi \circ \theta = \varphi$. Alors K est le groupe quotient de G par H et θ est le morphisme quotient.*

La première assertion du théorème est souvent appelée « théorème de factorisation ». Ce théorème est un outil de base fondamental pour travailler avec des groupes quotient, notamment pour constuire des morphismes de source un groupe quotient. On l'exprime souvent dans la version informelle suivante : « se donner un morphisme de G/H vers K, c'est se donner un morphisme de G vers K dont le noyau contient H ».

Dans la pratique, la version plus précise suivante du théorème de factorisation (qui découle facilement de la version ci-dessus) est utile.

Théorème 24. *Soit G un groupe commutatif, H un sous-groupe de G, $\pi\colon G \to G/H$ le morphisme quotient. Soit K un groupe et $\varphi\colon G \to K$ un morphisme de groupes dont le noyau contient H. Alors il existe un unique morphisme $\psi\colon G/H \to K$ tel que $\psi \circ \pi = \varphi$. En outre :*

- *ψ est surjective si et seulement si φ est surjective ;*
- *ψ est injective si et seulement si $\mathrm{Ker}(\varphi) = H$.*

En particulier, si φ est surjective de noyau H, il existe un unique isomorphisme $\psi\colon G/H \xrightarrow{\sim} K$ tel que $\varphi = \psi \circ \pi$.

4. L'expérience de l'auteur de ces lignes est que la connaissance de cette construction peut même parfois avoir tendance à obscurcir considérablement l'appréhension de la notion de quotient.

Remarque 16. La dernière assertion est en fait l'unicité à isomorphisme unique près du théorème 22.

1.8 Ordre d'un élément d'un groupe. Théorème de Lagrange. Groupes cycliques.

Définition 25. Un groupe est dit *monogène* s'il est engendré par un élément. En d'autres termes, un groupe G est monogène s'il contient un élément g tel que le sous-groupe engendré par g est le groupe G lui-même.

Remarque. Un groupe G noté multiplicativement est monogène si et seulement s'il contient un élément g tel qu'on ait

$$G = \{g^n, \quad n \in \mathbf{Z}\}.$$

Les règles de calcul des puissances montrent alors qu'un groupe monogène est nécessairement commutatif.

Définition 26. Soit G un groupe. Un élément g de G est *d'ordre fini* si le sous-groupe de G engendré par g est fini. L'*ordre* de g est alors le cardinal du sous-groupe engendré par g.

Rappelons qu'en théorie des groupes, le cardinal d'un groupe fini est appelé son *ordre*. Même si les deux notions ne sont pas sans rapport, il ne faut pas confondre les notions d'ordre d'un groupe fini et d'ordre d'un élément !

Proposition 27. *Soit G un groupe noté multiplicativement. Un élément g de G est d'ordre fini si et seulement s'il existe un entier* STRICTEMENT *positif n tel que $g^n = e$. L'ordre de g est alors le plus petit entier strictement positif n vérifiant $g^n = e$.*

Remarque. Si G est noté additivement (rappelons que cela n'est possible que si G est commutatif) la condition ci-dessus s'écrit : il existe un entier STRICTEMENT positif tel que $n.g = 0$.

Exemple. Dans n'importe quel groupe, l'élément neutre e est d'ordre fini et son ordre est 1. On l'appellera l'élément d'ordre fini trivial.

Tout élément d'un groupe fini est d'ordre fini.

$(\mathbf{Z}, +)$ et $(\mathbf{R}, +)$ n'ont aucun élément d'ordre fini non trivial.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est un élément d'ordre 2 du groupe $\mathrm{GL}_2(\mathbf{R})$.

Soit n un entier strictement positif et $m \in \mathbf{Z}$. L'ordre de $[m]_n$ dans le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ est $\frac{n}{\mathrm{pgcd}(n,m)}$.

Proposition 28. *Soit G un groupe noté multiplicativement. Soit g un élément de G, et n un entier* STRICTEMENT *positif. Sont équivalents :*

1. *on a $g^n = e$;*

2. *g est d'ordre fini et son ordre* DIVISE *n.*

Définition 29. Un groupe est dit cyclique s'il est engendré par un élément d'ordre fini.

Un groupe cyclique est donc en particulier fini.

Exemple 17. $(\mathbf{Z}, +)$ est monogène, non cyclique.

Pour tout entier n strictement positif, $\mathbf{Z}/n\mathbf{Z}$ est cyclique.

Tout élément d'un groupe fini engendre un groupe cyclique.

Théorème 30. *Soit G un groupe cyclique et n son ordre. Alors G est isomorphe à $(\mathbf{Z}/n\mathbf{Z}, +)$.*

Il est à noter que les applications des groupes cycliques à la cryptographie sont notamment basées sur le fait qu'on peut construire des groupes cycliques d'un certain ordre n pour lesquels on ne sait pas exhiber efficacement un isomorphisme explicite de G sur $\mathbf{Z}/n\mathbf{Z}$, c'est-à-dire une correspondance explicite entre les éléments de G et les éléments de $\mathbf{Z}/n\mathbf{Z}$ qui soit un morphisme de groupes.

Théorème 31. *Soit G un groupe cyclique engendré par $g \in G$ et n son ordre. Alors les générateurs de G sont les éléments de l'ensemble*

$$\{g^m\}_{\substack{1 \leqslant m \leqslant n \\ \mathrm{pgcd}(m,n)=1}}$$

En particulier G possède exactement $\varphi(n)$ générateurs.

Théorème 32 (Théorème de Lagrange)**.** *Soit G un groupe fini. L'ordre de tout sous-groupe de G divise l'ordre de G.*

En particulier l'ordre de tout élément de G divise l'ordre de G.

En général, si G est un groupe fini et d est un diviseur de l'ordre de G, il n'est pas vrai qu'il existe nécessairement un élément de G d'ordre d, ni un sous-groupe de G de cardinal d.

Théorème 33. *Soit G un groupe cyclique et n son ordre.*

Tout sous-groupe de G est cyclique.

Soit d un diviseur de n. Alors il existe un unique sous-groupe de G d'ordre d. Ce sous-groupe est constitué de l'ensemble des éléments de G dont l'ordre divise d.