ALGÈBRE

Jean-Paul Calvi

0.7

UPS
Université de Toulouse

Première mise en ligne, à la version 0.5.0, le 17 décembre 2009, sur la page

http://www.math.univ-toulouse.fr/∼calvi/

À partir de la version 0.6.0, le texte est déposé sur la page

jeanpaulcalvi.com

Développements

0.7	Révision du chapitre 1
1	Compléments au chapitre 2 (algèbre linéaire sur un corps quelconque, introduction à la cryptographie, introduction à la théorie des codes)

They said 'You have a blue guitar'
You do not play things as they are',
The man replied, 'Things as they are
Are changed upon the blue guitar'

W. Stevens (The man with the blue guitar)

Préface

Le premier chapitre de ce cours est une introduction à la théorie élémentaire des groupes. Il part de la définition pour arriver jusqu'au (premier) théorème d'isomorphisme. Il se termine par l'étude du groupe symétrique. J'ai enseigné ce chapitre pendant plusieurs années à l'université Paul Sabatier où il m'était demandé de la faire dans un volume horaire limité à 12 heures de cours et 12 heures de travaux dirigés. Le second chapitre, portant sur la théorie des anneaux et des corps, se borne à présenter les définitions et les propriétés élémentaires. Je l'ai enseigné dans une version précédente du cours pour laquelle le volume horaire était double. Le contenu est par force très limité et tout ce qui est commencé reste en un certain sens inachevé. Je construit les anneaux $\mathbb{Z}/n\mathbb{Z}$, plus généralement les anneaux quotient, et les anneaux de polynômes à une indéterminée (à coefficients dans un anneau). L'étude s'arrête avant d'aborder la théorie de la divisibilité. La forme actuelle de ce deuxième chapitre est encore très éloignée de celle qu'elle sera en principe dans le futur.

Les connaissances préalables nécessaires indiquées ci-dessous sont limitées et devraient en principe être acquises à l'issue d'une première année d'enseignement supérieur scientifique.

(i) Vocabulaire de la théorie des ensembles : intersection, réunion, complémentaire, inclusion de deux ensembles ; diverses manières d'écrire un ensemble. Produit cartésien d'une famille finie d'ensemble.

(ii) Application, composée des applications, injection, bijection, surjection, bijection réciproque. Caractérisation des bijections d'un ensemble fini dans lui-même.

(iii) Arithmétique élémentaire. Divisibilité, nombres premiers, pgcd, théorème fondamental de l'arithmétique.

(iv) Calcul dans $\mathbb{C}$, forme cartésienne, forme trigonométrique, conjugaison, exponentielle complexe, racines de l'unité.

(v) Algèbre linéaire élémentaire dans $\mathbb{R}^n$, calcul matriciel, déterminant.

(vi) Pour certains exercices, très peu, analyse des fonctions d'une variable réelle telle qu'enseignée généralement en première année d'université.

Les premiers développements projetés, qui devraient à terme conduire à la version 1.0 de ce texte sont indiqués sur la page des mentions légales.

Foix, le 7 juillet 2013,

Jean-Paul Calvi

Renvois. Lorsque le texte renvoie à un objet (théorème, section, exercice, etc) du même chapitre, seul le numéro de l'objet est indiqué. Par contre si le texte renvoie à un objet d'un autre chapitre, le numéro du chapitre apparaît aussi. Ainsi, si au cours chapitre 2, on renvoie au théorème 20 du chapitre 1, on écrira théorème I.20. Pour utiliser les liens, il suffit de sélectionner le second, ici 20.

Table des matières

I

Introduction à la théorie des groupes

§ 1. La structure de groupe

1.1 Introduction

Le lecteur qui initie la lecture de ce texte a déjà un grande familiarité avec de nombreuses techniques de composition d'objets mathématiques. Rapidement après avoir appris à compter avec les entiers naturels ($\mathbb{N}$) il a aussi appris à les *additionner*, puis à les *multiplier*. Il a ensuite appris, dans certains cas, à les *soustraire* et à les *diviser*. Les difficultés liées à la division ont par la suite conduit à l'introduction des nombres rationnels positifs ($\mathbb{Q}^+$), certainement précédée par celle des nombres décimaux ($\mathbb{D}^+$) ; tandis que les difficultés liées à la soustraction ont conduit à l'introduction des nombres négatifs ($\mathbb{Z}$ et $\mathbb{Q}$). On a ensuite mis en évidence l'insuffisance des nombres rationnels, par exemple en montrant que la longueur de la diagonale d'un carré de côté 1 ne peut pas être un nombre rationnel, et le calcul dans $\mathbb{Q}$ a dû être étendu aux nombres réels ($\mathbb{R}$) (sans qu'aucune construction rigoureuse de $\mathbb{R}$ n'ait vraisemblablement été proposée) avant d'arriver à l'ensemble des nombres complexes ($\mathbb{C}$) probablement construit en imposant des règles de calculs sur $\mathbb{R}^2$, peut-être avec la motivation de compléter $\mathbb{R}$ en sorte que tous les polynômes possèdent des racines dans l'extension, ou peut-être simplement — on montre que cela revient au même — en sorte que le seul polynôme X^2+1 y possède une racine. D'autres opérations fondamentales avec des objets qui n'étaient plus facilement perçus comme des nombres ont été introduites dans l'étude des mathématiques élémentaires, la plus importante de toutes étant la loi de composition des applications. Enfin, dès ses débuts à l'université, le lecteur a aussi appris à combiner des ensembles entre eux pour former leur réunion ou leur intersection, à additionner et a multiplier des tableaux de nombres appelés matrices, à effectuer des additions modulo 2π sur les mesures des angles, possiblement sur des entiers modulo n. L'objet de ce premier chapitre,

comme aussi du suivant, est d'étudier les règles de calculs, communes à pratiquement tous les objets mathématiques que le lecteur a rencontré jusqu'ici, et les propriétés générales qui en découlent. Un tel ensemble de règles s'appelle une **structure algébrique**. L'étude de ces structures permettra d'abord de mieux analyser les réflexes de calculs acquis après des années d'expérience. Surtout, le recul que procure le travail dans un cadre plus abstrait facilitera la découverte de nouvelles propriétés d'objets connus depuis longtemps * ; il suggérera, souvent par analogie, l'étude de nouveaux objets.

1.2 Lois internes

Soit E un ensemble non vide. Une application $*$ de $E\times E$ dans E s'appelle une **loi interne** ou parfois une **opération**. Si a et b sont dans E alors l'image du couple (a,b) par $*$ n'est généralement pas notée $*(a,b)$ comme c'est l'usage avec la plupart des applications mais plutôt $a*b$. Nous parlons de loi *interne* (à E) parce qu'avec deux éléments de E nous fabriquons un troisième élément de E. Les opérations de l'algèbre élémentaire $+$ et $\times$ sont des lois internes sur $\mathbb{Z}$. La division est une loi interne sur $\mathbb{Q}^\star$. L'addition et la multiplication des matrices sont des lois internes sur l'ensemble des matrices carrées d'ordre n, $M_n(\mathbb{R})$. L'élément $a*b$ s'appelle le **produit** de a par b ou, s'il faut être précis, le $*$**-produit** de a par b. Chacun des éléments a et b est un **facteur** du $*$-produit $a*b$.

1.3 Associativité et commutativité d'une loi interne

L'associativité est une propriété qui regarde la répétition d'une opération et la commutativité, l'ordre dans lequel elle est effectuée. Soit $*$ une loi interne sur E. Nous dirons que

(i) $*$ est **associative** si quels que soient $a,b,c\in E$, nous avons $(a*b)*c=a*(b*c)$.

(ii) $*$ est **commutative** si quels que soient $a,b\in E$, nous avons $a*b=b*a$.

L'addition dans $\mathbb{Z}$ et la multiplication dans $\mathbb{R}$ sont à la fois commutatives et associatives. La propriété d'associativité est essentielle. Les lois non associatives ont très peu d'intérêt en mathématiques ; cependant il n'est pas difficile d'en construire. Voici un exemple de loi non associative :

$$*:\begin{array}{ccc}\mathbb{Q}^{\star+}\times\mathbb{Q}^{\star+} & \longrightarrow & \mathbb{Q}^{\star+}\\ (x,y) & \longmapsto & \frac{1}{x+y}\end{array}.$$

En effet,

$$(x*y)*z=\frac{1}{\frac{1}{x+y}+z}\quad\text{et}\quad x*(y*z)=\frac{1}{x+\frac{1}{y+z}},$$

*. Ce travail de synthèse n'a rien à voir avec le cheminement historique qui conduit aux fondement de la théorie des groupes et que nous discuterons sommairement à la partie 9.

et les deux quantités en général ne coïncident pas (par exemple pour $x=1$, $y=2$, $z=2$ nous trouvons $(x*y)*r=3/7$ et $x*(y*z)=4/5$). Remarquons que cette loi est commutative et nous verrons par la suite de nombreux exemples de lois associatives qui ne sont pas commutatives. Cela montre que les propriétés d'associativité et de commutativité sont *indépendantes* — l'une peut être vérifiée sans que l'autre le soit.

E. 1. La soustraction dans $\mathbb{Z}$, la division dans $\mathbb{R}^\star$ et l'exponentiation dans $\mathbb{R}^{\star+}$ ($x*y:=x^y$) sont-elles des lois associatives ? Nous verrons plus loin qu'il est plus utile de considérer la soustraction dans $\mathbb{Z}$ et la division dans $\mathbb{R}^\star$ dans leurs rapports respectivement à l'addition et à la multiplication plutôt que comme des lois internes à part entière.[s:1]

s: p. 103

1.4 À quoi servent l'associativité et la commutativité ?

Si nous voulons former des produits avec quatre éléments a, b, c et d en utilisant une loi interne quelconque $*$, il y a à priori cinq possibilités :

$$\begin{array}{c|c|c|c|c} (i) & (ii) & (iii) & (iv) & (v) \\ a*((b*c)*d) & a*(b*(c*d)) & (a*b)*(c*d) & (a*(b*c))*d & ((a*b)*c)*d \end{array}.$$

Or si la loi est associative, chacun de ces cinq calculs produit le même résultat. Montrons par exemple que (i)=(iv). Posant $\square=b*c$,

$$(i)=a*((b*c)*d)=a*(\square*d)\overset{\text{assoc.}}{=}(a*\square)*d=(a*(b*c))*d=(iv).$$

Puisque le résultat est le même quel que soit le placement des parenthèses il est inutile de les employer et nous pourrons simplement écrire, sans introduire de confusion, $a*b*c*d$. Insistons sur le fait que ceci n'est qu'une simplification d'écriture. S'il faut effectuer concrètement le calcul de $a*b*c*d$, nous devrons bien décider d'un **parenthésage**, c'est-à-dire un placement de parenthèses spécifique, parce que les calculs ne peuvent s'effectuer que deux par deux. En utilisant une démonstration par récurrence, la propriété indiquée ci-dessus est étendue au cas d'un produit de n éléments, $n\geq 3$.

THÉORÈME 1. — *Lorsque la loi $*$ sur E est* associative, *nous pouvons écrire les produits sans qu'il soit nécessaire de placer les parenthèses (autrement dit, le résultat ne dépend pas de la manière dont celles-ci sont placées). En particulier, pour $a\in E$ et $n\in\mathbb{N}^\star$, nous pouvons définir*

$$a^n:=\underbrace{a*a*\cdots*a}_{n\text{ fois}}, \tag{1.1}$$

et les relations suivantes sont vraies

$$\begin{cases} a^n*a^m &= a^{n+m}, \quad n,m\in\mathbb{N}^\star \\ (a^n)^m &= a^{nm}, \quad n,m\in\mathbb{N}^\star \end{cases}. \tag{1.2}$$

Enfin, si, en plus d'être associative, la loi $*$ est aussi commutative *les éléments de $a_1*a_2*\cdots*a_n$ peuvent être permutés de manière arbitraire sans modifier le résultat. En*

particulier,

$$(a_1 * a_2 * \cdots * a_n)^m = a_1^m * a_2^m * \cdots * a_n^m, \quad m \in \mathbb{N}. \tag{1.3}$$

Démonstration. Les points non déjà vus se vérifient immédiatement. ■

La notation a^n dont les formules (1.2) montrent tout l'intérêt ont cependant l'inconvénient de faire disparaître la mention à la loi utilisée, ce qui peut créer des confusions quand nous travaillons avec différentes lois sur un même ensemble.

Les notions d'associativité et de commutativité ne sont pas anodines. Un calculateur expérimenté — comme l'est nécessairement tout lecteur de ce cours — établit très rapidement l'égalité $-5+128+15-38=100$, si rapidement même que les transformations qu'il effectue cessent d'être conscientes. Il regroupe probablement les termes comme suit $-5+128+15-38 \to ((-5+15)+128-38) \to (10+128)-38 \to (138-38)$, et chacune de ces transformations utilise la commutativité ou l'associativité de l'addition. Si ces transformations sont évidentes au point d'en devenir inconscientes pour le calculateur expérimenté, il n'y a aucune raison qu'il en soit de même pour un débutant. L'étude des notions d'associativité et de commutativité dans un cadre abstrait permet de *dés-automatiser* leur utilisation quand nous les employons dans l'arithmétique élémentaire et de mieux comprendre les difficultés de ceux que leurs intérêts et leurs dispositions naturelles ne conduiront jamais à lire un cours comme celui-ci.

HISTOIRE 1. — Les notions d'associativité et de commutativité ci-dessus ont été définies par *W. Hamilton* (1788-1856) au moment où il inventa les quaternions, en 1846. Le fait de devoir définir ces propriétés ne pouvait apparaître qu'une fois compris le concept fondamental d'opération (de loi interne). Notons l'apparition relativement récente de ce concept.

1.5 Élément neutre pour une loi interne

Soit $*$ une loi interne sur un ensemble (non vide) E. Nous dirons qu'un élément $e \in E$ est **élément neutre** pour $*$ (ou de $*$) si quel que soit $a \in E$, $a*e = e*a = a$.

Par exemple, 0 est élément neutre de l'addition dans $\mathbb{N}$, 1 est élément neutre de la multiplication dans $\mathbb{R}^\star$. La division dans $\mathbb{R}^\star$ n'admet pas d'élément neutre.

THÉORÈME 2. — *Une loi interne admet au plus un élément neutre.*

Démonstration. Supposons que e et e' soient éléments neutres de $*$. D'un côté $e*e' = e'$ car e est élément neutre et de l'autre $e*e' = e$ car e' est élément neutre ; d'où $e = e'$. ■

1.6 Définition d'un groupe

Un ensemble G muni d'une loi interne $*$ est appelé **groupe** si :

(i) La loi $*$ est associative et admet un élément neutre, souvent noté e — ou, s'il faut préciser, e_G.

(ii) Pour tout $g \in G$, il existe un élément $y \in G$, appelé **élément symétrique** de g tel que $g*y = y*g = e$.

Nous parlons alors du groupe $(G, *)$ ou — lorsqu'il n'y a pas d'ambiguïté sur la loi $*$ — simplement du groupe G. Lorsque la loi $*$ est commutative, nous disons que $(G, *)$ est un **groupe commutatif** ou encore un **groupe abélien** en hommage au mathématicien norvégien Niels Abel (1802-1829) qui se servit du groupe $\mathbf{S}_n$ (voir 1.8) dans ses travaux sur la résolution des équations polynomiales par radicaux. Lorsque G contient un nombre infini d'éléments, G est dit **infini**. Dans le cas contraire, nous disons que G est **fini**. Le cardinal, c'est-à-dire le nombre d'éléments, d'un groupe G, aussi appelé **ordre**, est noté $\text{card}(G)$ ou $o(G)$ ou $|G|$. Dire qu'un groupe est fini est donc équivalent à dire qu'il est d'ordre fini.

E. 2. La loi de composition $\circ$ est une loi interne sur l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ noté $\mathscr{F}(\mathbb{R})$. Soit $f \in \mathscr{F}(\mathbb{R})$ montrer que s'il existe $g \in \mathscr{F}(\mathbb{R})$ telle que $f \circ g = \text{Id}$ alors f est surjective. Trouver un exemple de fonction f pour laquelle une telle fonction g existe mais $g \circ f \neq \text{Id}$. s: p. 103 s:2

1.7 L'élément symétrique

Nous ne pouvons pas parler d'élément symétrique sans disposer au préalable d'un élément neutre. La propriété (ii) de la définition d'un groupe requiert seulement l'existence d'*un* élément symétrique. En réalité, comme l'annonce l'emploi de l'article défini dans le titre de ce paragraphe, un élément symétrique, s'il existe, ne peut être qu'unique. En effet, supposons que y et y' soient éléments symétriques de $g \in G$ de sorte que nous ayons à la fois $g*y = y*g = e$ et $g*y' = y'*g = e$. Nous avons

$$\begin{array}{lll} & (g*y) = e & \\ \Rightarrow & y'*(g*y) = y'*e & \text{(multiplication par } y' \text{ à gauche)} \\ \Rightarrow & (y'*g)*y = y' & \text{(utilise } * \text{ associative et } e \text{ neutre)} \\ \Rightarrow & e*y = y' & \text{(car } y' \text{ est symétrique de } g.) \\ \Rightarrow & y = y' & \text{(car } e \text{ élément neutre).} \end{array}$$

Nous avons montré, en particulier, le théorème suivant.

THÉORÈME 3. — *Dans un groupe tout élément admet toujours un* unique *élément symétrique.*

Cette unicité permet d'attacher une notation particulière à l'élément symétrique. L'unique élément symétrique de g sera noté en général g^{-1} (voir cependant 1.9 ci dessous). Les quelques propriétés qui suivent sont fondamentales et systématiquement employées dans les calculs.

(i) $e^{-1} = e$. L'élément neutre est son propre symétrique.

(ii) Pour tout $g \in G$, $(g^{-1})^{-1} = g$.

(iii) Pour tous $g, g' \in G$, $(g*g')^{-1} = g'^{-1}*g^{-1}$. *Le symétrique d'un produit est le produit* inverse *des symétriques.*

[TH 3]

(iv) Plus généralement, si $g_i \in G$, $i = 1, \ldots, n$, nous avons

$$(g_1 * g_2 * \cdots * g_n)^{-1} = g_n^{-1} * g_{n-1}^{-1} * \cdots * g_1^{-1}. \tag{1.4}$$

En particulier, $(g^n)^{-1} = (g^{-1})^n$, $n \in \mathbb{N}^\star$. Posant

$$g^{-n} := (g^n)^{-1}, \quad n \in \mathbb{N}^\star; \tag{1.5}$$

il est possible de parler de g^m lorsque m est un entier négatif. Si nous convenons encore que $g^0 = e$, la notation g^m prend un sens pour tout $m \in \mathbb{Z}$. Dans ces conditions, les relations suivantes sont valides :

$$g^m * g^{m'} = g^{m+m'} \quad \text{et} \quad (g^m)^{m'} = g^{mm'}, \quad m, m' \in \mathbb{Z}. \tag{1.6}$$

Chacune des propriétés ci-dessus mérite une démonstration. Elles sont très simples. Le lecteur s'entraînera utilement à les rédiger.[s:3] s: p. 103

E. 3. Soit $(G, *)$ un groupe. On définit une loi interne $\bar{*}$ sur G par $a \bar{*} b := a * b^{-1}$ où b désigne le symétrique de b pour la loi $*$. Lorsque $(G, *) = (\mathbb{Z}, +)$, $\bar{*}$ n'est autre que la soustraction et lorsque $(G, *) = (\mathbb{R}^\star, \cdot)$, $\bar{*}$ est la division. Montrer que $(G, \bar{*})$ n'est jamais un groupe.

NOTE 1. — La soustraction ne naît pas de la manière dont elle présentée dans l'exercice. Le résultat de la soustraction de $a - b$ est semble-t-il conçu et en tout cas appris comme l'image de a par l'opération $\boxed{-b}$ qui est l'opérateur réciproque de l'opérateur $\boxed{+b}$ lequel associe au nombre a le nombre $a + b$. Une remarque similaire vaut pour la division.

1.8 Exemples de groupes

(1.8.1) Le cercle unité $(\mathbf{U}, \cdot)$. C'est l'ensemble des nombres complexes de module 1 muni de la *multiplication des nombres complexes* : $\mathbf{U} = \{z \in \mathbb{C} : |z| = 1\}$. Nous avons $z = a + ib \in \mathbf{U} \iff a^2 + b^2 = 1$ et $z \in \mathbf{U} \iff z = e^{i\theta}$ pour un $\theta \in \mathbb{R}$. L'élément neutre de $(\mathbf{U}, \cdot)$ est 1. Le symétrique de z est son conjugué $\bar{z}$. C'est un groupe abélien infini.

(1.8.2) Les entiers relatifs $(\mathbb{Z}, +)$, l'ensemble des entiers relatifs muni de *l'addition (habituelle)*. L'élément neutre est 0, le symétrique d'un élément est son *opposé*. C'est un groupe abélien infini.

(1.8.3) Les racines n-ième de l'unité : $(\mathbf{U}_n, \cdot)$ où $n \in \mathbb{N}^\star$. C'est l'ensemble des nombres complexes satisfaisant $z^n = 1$ muni de la multiplication habituelle des nombres complexes. Nous avons

$$\mathbf{U}_n = \left\{ e^{\frac{2ik\pi}{n}} : k = 0, 1, \ldots, n-1 \right\}.$$

L'élément neutre est 1. $(\mathbf{U}_n, \cdot)$ est un groupe abélien fini, contenant n éléments. Formons la table de $\mathbf{U}_5$. Juste comme les tables d'addition ou de multiplications étudiées à l'école élémentaire, une **table** de groupe (fini) est un tableau qui fait apparaître toutes les opérations possibles entre deux éléments d'un groupe fini G. Si ce groupe contient

n éléments, la table comportera n^2 résultats. Posant $g_j = e^{\frac{2ik\pi}{5}}$ pour $j = 0,1,2,4$ et 4, la table de $(\mathbf{U}_5, \cdot)$ est donnée par

$\swarrow$	g_0	g_1	g_2	g_3	g_4
g_0	g_0	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4	g_0
g_2	g_2	g_3	g_4	g_0	g_1
g_3	g_3	g_4	g_0	g_1	g_2
g_4	g_4	g_0	g_1	g_2	g_3

Dans la première case la flèche est mise pour indiquer le sens de lecture du tableau. Dans ce cas, le groupe étant commutatif nous aurions obtenu le même tableau en inversant la direction de la flèche. La commutativité du groupe apparaît sur le tableau à travers la symétrie par rapport à la diagonale principale. Remarquons aussi que les résultats se répètent à chaque ligne avec un décalage. Ce phénomène est typique des groupes dit cycliques qui sont étudiés dans 4.5 et dont $\mathbf{U}_n$ est un exemple particulier important. Enfin le fait que chaque élément du groupe apparaît une fois et une seule sur chaque ligne et chaque colonne de résultats sera facilement expliqué par qui traitera l'exercice suivant.

E. 4. Soient $G, *$ un groupe et $g \in G$. Montrer que les application $x \in G \to g*x$ et $x \in G \to x*g$ sont des bijections. Que peut-on en déduire sur les lignes et colonnes de la table d'un groupe fini. s:4

s: p. 103

Notons que les règles de simplifications $a*x = a*y \implies x = y$ et $x*a = y*b \implies x = y$ sont toujours valables.

(1.8.4) L'ensemble $(\mathbf{GL}_n(\mathbb{K}), \cdot)$ *des matrices inversibles* à n lignes et n colonnes à coefficients dans $\mathbb{K} = \mathbb{C}, \mathbb{R}$ ou $\mathbb{Q}$, muni de la *multiplication des matrices*. L'élément neutre est la matrice identité. L'élément symétrique est la matrice inverse. Lorsque $n = 2$,

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies M^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Dans le cas général ($n \geq 2$), l'inverse de M est donné par la transposée de la comatrice de M divisée par le déterminant de M,

$$M^{-1} = \frac{1}{\det M} (\mathrm{comat} A)^T, \tag{1.7}$$

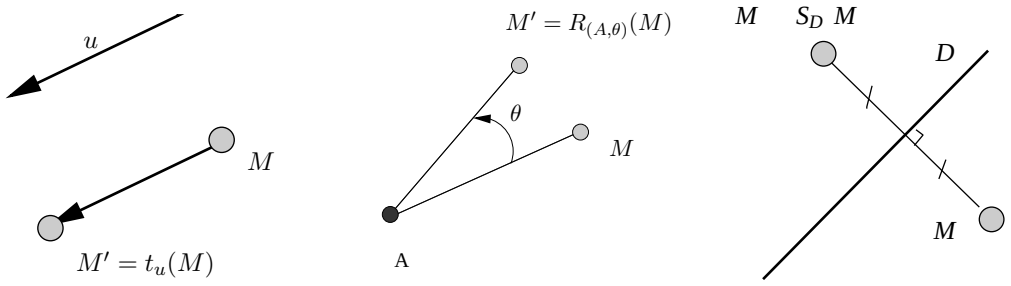
ou $(.)^T$ indique la transposée et comat(M) est la matrices de coefficient (i, j) est donnée par $(-1)^{i+j}$ multiplié par le déterminant de ma matrice obtenue en omettant la i-ème ligne et la j-ième colonne. La formule (1.7) n'a pas d'intérêt pratique pour le calcul de l'inverse mais elle est utile pour résoudre des questions théoriques sur l'inversion de matrices et sur les déterminants.

$\mathbf{GL}_n(\mathbb{K})$ est un groupe non abélien (dès que $n > 1$) infini.

[TH 3]

(1.8.5) Les bijections d'un ensemble dans lui-même : $(\mathbf{S}(\Omega), \circ)$. Ω est un ensemble quelconque non vide et $\mathbf{S}(\Omega)$ est l'ensemble des bijections de Ω sur Ω muni de la loi de *composition des fonctions*. L'élément neutre est l'application identité, le symétrique est la bijection réciproque. C'est un groupe infini lorsque Ω est infini et il a pour cardinal $n!$ lorsque Ω est formé de n éléments. Il est non abélien dès que $\text{card}(\Omega) > 2$. Lorsque $\Omega = \{1, 2, \ldots, n\}$ le groupe est habituellement désigné par $\mathbf{S}_n$. C'est un groupe très important, appelé le **groupe symétrique**. Il sera étudié en détails à la section 8.

(1.8.6) L'ensemble des isométries affines du plan euclidien (orienté) P : $(\mathbf{Is}(P), \circ)$. Il est muni de la *composition des fonctions*. C'est un groupe infini non abélien contenant en particulier les translations (de vecteur u, t_u), les rotations (de centre A et d'angle θ, $R_{A,\theta}$), les réflexions ou symétries orthogonales (d'axe D, S_D) * :



$\overrightarrow{MM'} = u$

(Translation de vecteur u)

$AM = AM'$ et $(\overrightarrow{AM}, \overrightarrow{AM'}) = \theta$

(Rotation de centre A et d'angle θ)

D est la médiatrice des points M et M'

(Réflexion d'axe D)

L'élément neutre est l'application identité. Le tableau ci-dessous donnent les symétriques des éléments les plus intéressants de **Is**.

	f	f^{-1}
translation de vecteur u	t_u	t_{-u}
rotation de centre A et d'angle θ	$R_{A,\theta}$	$R_{A,-\theta}$
symétrie orthogonale d'axe D	S_D	S_D

Le cas des symétries orthogonales montre qu'il est tout à fait possible qu'un élément différent du neutre soit égal à son symétrique.

∗. Les seules isométries planes manquantes, sont les réflexions glissées.

(1.8.7) Produit direct de deux groupes. Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. Une loi interne $*$ sur $(G_1 \times G_2)$ est définie par la relation suivante :

$$(g_1, g_2) * (g_1', g_2') = (g_1 *_1 g_1', g_2 *_2 g_2').$$

Alors $(G_1 \times G_2, *)$ est un groupe, appelé le **produit direct** de $(G_1, *_1)$ par $(G_2, *_2)$. Nous avons

$$e_{G_1 \times G_2} = (e_{G_1}, e_{G_2}) \quad \text{et} \quad (g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}).$$

s: p. 103 E. 5. Dresser la table du groupe $\mathbf{U}_2 \times \mathbf{U}_2$. [s:5]

Nous pouvons généraliser la construction en faisant intervenir n groupes au lieu de deux. Lorsque tous les groupes coïncident, nous notons

$$\underbrace{G \times G \times \cdots \times G}_{n \text{ fois}} = G^n$$

et la loi de G^n est généralement (abusivement) notée comme celle de G

$$(g_1, g_2, \ldots, g_n) * (g_1', g_2', \ldots, g_n') = (g_1 * g_1', g_2 * g_2', \ldots, g_n * g_n').$$

Un exemple particulièrement important est le groupe $(\mathbb{Z}^n, +)$ tandis que $(\mathbb{R}^n, +)$ est sans doute déjà familier au lecteur.

E. 6. Soit X un ensemble et $(G, *)$ un groupe. Montrer que l'ensemble des fonctions de X dans G, noté $\mathscr{F}(X, G)$ est un groupe lorsqu'on le munit de la loi $*_X$ définie pour $f, h \in \mathscr{F}(X, G)$ par la relation $(f *_X h)(x) = f(x) * h(x)$, $x \in X$. Expliquer pourquoi cette construction est une généralisation du produit direct $G \times G \times \cdots \times G$? Voir aussi l'exercice 48.

NOTE 2. — Nous parlons de produit direct par opposition à une autre construction plus générale et moins élémentaire obtenue à l'aide de deux groupes qui s'appelle le **produit semi-direct** et qui sera étudiée en exercice.

1.9 Notation additive et notation multiplicative

Très souvent, pour une simple question de commodité d'écriture, toutes les lois sont notées de la même manière, généralement avec un point "$\cdot$" — de sorte que l'on écrit $g \cdot g'$ plutôt que $g * g'$, $g \circ g'$ etc, et, comme nous le faisons couramment avec le produit habituel dans $\mathbb{R}$ ou $\mathbb{C}$, lorsqu'il n'y a pas de confusion possible, le point aussi est omis. Nous écrivons alors gg' plutôt que $g \cdot g'$. Dans ce cas (notation point ou notation vide) nous disons que nous utilisons une **notation multiplicative**. Lorsque le groupe est *abélien*, le loi est plus souvent notée avec un "$+$" : c'est la **notation additive**. Dans ce cas, le symétrique d'un élément g n'est plus noté g^{-1} mais $-g$ et l'écriture de $g + (-g')$ est abrégée en $g - g'$. La notation g^n devient ng et les relations (1.6) sont transformées en accord avec cette nouvelle convention. Ces conventions nécessitent une attention soutenue lorsque plusieurs groupes entrent en jeu et que des *mêmes* notations sont employées

pour désigner des lois *différentes*. S'agissant ici d'un cours d'introduction qui s'adresse par définition à des lecteurs peu expérimentés, nous essaierons, dans cette première partie, de garder des notations différentes pour des lois différentes.

NOTE 3. — Dans le cas d'un groupe *abélien* dans lequel nous utiliserions une notation multiplicative, il ne serait pas interdit d'utiliser la notation x/y pour xy^{-1} puisque, la formule $(x/y)(x'/y') = (xx')/(yy')$ serait valable (voir l'exercice ci-dessous). Cette convention n'est généralement pas employée quand on considère seulement des groupes mais l'idée sera reprise dans l'étude des corps, voir II::2.2.

E. 7. Soit $(G,\cdot)$ un groupe abélien. On note $x/y := xy^{-1}$ Montrer que $(x/y)(x'/y') = (xx')/(yy')$.

E. 8. Relire l'ensemble des formules de cette partie et étudier s'il faut les modifier dans le cas où une notation additive est employée.

1.10 A propos de la définition d'un groupe

Un ensemble G munit d'une loi interne associative est parfois appelé un **semi-groupe**. Si un semi-groupe admet un élément neutre pour sa loi, il devient un **monoïde**. La définition de groupe donnée ici au paragraphe 1.6 est redondante : certaines des propriétés imposées découlent des autres. Ceci fait l'objet de l'exercice 9 ci-dessous.

E. 9. Soit $(G,*)$ un ensemble non vide muni d'une loi interne associative. On suppose qu'il existe dans G un élément e satisfaisant les deux propriétés suivantes :

(i) Pour tout $a \in G$, $e * a = a$;

(ii) pour tout $a \in G$, il existe un élément $a' \in G$ tel que $a' * a = e$.

Montrer que $(G,*)$ est un groupe.

La définition utilisant le nombre d'axiomes minimal est celle qui se déduit de l'exercice : *on appelle groupe un ensemble non vide muni d'une loi interne satisfaisant les deux conditions de l'exercice*. Cette définition minimale est donnée dans le traité d'algèbre de van der Waerden (**?**) qui a eu une une influence considérable sur l'enseignement de l'algèbre moderne, et aussi, par exemple, par Zariski et Samuel (**?**). Ces auteurs, influencés par la philosophie dominante de leur époque, recherchaient la présentation la plus épurée sur le plan logique. L'auteur de ce texte comme aussi **?**, **?** et la plupart des auteurs modernes choisissent au contraire les définitions qui leur semblent les plus naturelles, les plus aisément mémorisables par les lecteurs auxquels ils s'adressent, y compris si ces définitions ne sont pas logiquement minimales, et ils rejettent la construction de définitions plus économiques en exercice, comme il est fait ici. Pour une présentation sommaire de la genèse de la définition d'un groupe abstrait, nous renvoyons à la section 9.

§ 2. SOUS-GROUPES

2.1 Définition et notations

Un sous-groupe est un groupe à l'intérieur d'un groupe et qui utilise la même opération que celui-ci. La définition précise est la suivante. Soient $(G,*)$ un groupe et H un sous-ensemble *non vide* de G. Nous disons que H est un **sous-groupe** de G si les deux conditions suivantes sont vérifiées.

(i) Pour tous $x, y \in H$, $x*y \in H$

(ii) Pour tout $x \in H$, $x^{-1} \in H$

Cela signifie que la restriction de $*$ à $H \times H$ — que nous notons encore $*$ mais qu'il faudrait en toute rigueur désigner par $*_{|H}$ voire $*_{|H\times H}$ — donne une loi interne de H et que $(H,*)$ est alors lui-même un groupe. En d'autres termes un sous-groupe H est un sous-ensemble d'un groupe $(G,*)$ qui est *fermé* pour l'opération $*$ ainsi que par l'application qui a tout élément associe son symétrique.

Le sous-ensemble $\mathbb{N}$ de $\mathbb{Z}$ satisfait la première condition ci-dessus mais pas la seconde.

s: p. 103 E. 10. Trouver un sous-ensemble de $\mathbb{Z}$ qui vérifie la seconde condition mais pas la première. s:6

Les deux conditions (i) et (ii) peuvent être regroupées en une seule.

THÉORÈME 4. — *Soit H un sous-ensemble non vide de G. Pour que H soit un sous-groupe de G il faut et il suffit que*

(iii) quels que soient $x, y \in H$, $x*y^{-1} \in H$.

s: p. 103 *Démonstration.* Il est évident que les conditions (i) et (ii) entraînent (iii)s:7. Montrons que, réciproquement, la seule condition (iii) entraînent à la fois (i) et (ii). Puisque $H \neq \emptyset$, il existe $h \in H$. Appliquons (iii) avec $x = y = h$. Nous obtenons $h*h^{-1} \in H$ donc $e_G \in H$. Appliquons maintenant (iii) avec $x = e_G$. Puisque $e_G * y^{-1} = y^{-1}$, nous obtenons (ii). Enfin, prenant $x, y \in H$, nous avons par (ii) qui vient d'être établi $y^{-1} \in H$ et appliquant (iii) avec y^{-1} à la place de y il vient $x*(y^{-1})^{-1} \in H$ c'est-à-dire $x*y \in G$ qui donne (i). ■

La notation $H \leq G$ est employée pour dire H est sous-groupe de G. Lorsque la possibilité que H soit égal à G est exclue nous écrivons $H < G$.

Insistons sur le fait que pour montrer qu'un sous-ensemble H de G est un sous-groupe de G, il faut d'abord s'assurer qu'il est non vide.

E. 11. La vérification que H est non vide n'est pas anodine. Un étudiant qui l'omettrait pourrait
s: p. 103 arriver à la conclusion que $\{x \in \mathbb{R} \,:\, \exp x = 0\}$ est un sous-groupe de $(\mathbb{R},+)$. Pourquoi ? s:8

Nous avons vu dans la démonstration du théorème 4 qu'un sous-groupe H contient toujours l'élément neutre e_G. L'ensemble réduit à l'élément neutre forme d'ailleurs toujours un sous-groupe. Un sous-groupe H de G qui est différent à la fois de G lui-même et de $\{e_G\}$ s'appelle un sous-groupe **propre**.

E. 12. $(\mathbb{R},+)$ admet-il des sous-groupes finis propres ? [s:9] s: p. 103

2.2 Exemples de sous-groupes

(2.2.1) Sous-groupes de $(\mathbb{C},+)$. Nous avons $\mathbb{Z}<\mathbb{Q}<\mathbb{R}<(\mathbb{C},+)$.

E. 13. Montrer que l'ensemble $\mathbb{D}$ des nombres décimaux est un sous-groupe de $(\mathbb{R},+)$.

Rappelons que $\mathbb{D}=\{n/10^m : (n,m)\in\mathbb{Z}\times\mathbb{N}^\star\}$.

(2.2.2) Sous-groupes de $(\mathbb{Z},+)$. Soit $m\in\mathbb{N}^\star$. Nous avons $m\mathbb{Z}<(\mathbb{Z},+)$ où $m\mathbb{Z}=\{mr : r\in\mathbb{Z}\}$ est l'ensemble des (entiers relatifs) multiples de m. Réciproquement,

THÉORÈME 5. — *Tout sous-groupe G de $(\mathbb{Z},+)$ est de la forme $G=m\mathbb{Z}$ pour un certain $m\in\mathbb{N}$ (dépendant de G).*

Démonstration. Soit G un sous-groupe de $(\mathbb{Z},+)$. Nous devons établir l'existence d'un entier positif m tel que $G=m\mathbb{Z}$. Traitons d'abord le cas où G est réduit à l'élément neutre, i.e. $G=\{0\}$. Dans ce cas nous avons bien évidemment $G=m\mathbb{Z}$ en prenant $m=0$. Supposons maintenant que G ne soit pas réduit à l'élément neutre, il existe alors $g\in G$ avec $g\neq 0$. Puisque $G\leq\mathbb{Z}$, $g\in G \implies -g\in G$ et nous sommes donc sûrs que G contiendra un élément strictement positif, autrement dit $G\cap\mathbb{N}^\star\neq\emptyset$. Prenons alors m comme le plus petit élément de $G\cap\mathbb{N}^\star$. Puisque $m\in G$ et que G est un sous-groupe, $km=m+m+\cdots+m\in G$. Toujours grâce au fait que G soit un sous-groupe, $-m\in G$ puis $-km=(-m)+(-m)+\cdots+(-m)\in G$ si bien que $m\mathbb{Z}\subset G$. Montrons maintenant que $G\subset m\mathbb{Z}$. Prenons g un élément quelconque de G. C'est un entier que nous pouvons diviser par m pour obtenir une expression $g=qm+r$ où r est le reste $(0\leq r<m)$. Comme $qm\in G$, $r=g-qm\in G$. Comme en outre $0\leq r<m$ et m est le plus petit entier (strictement) positif dans G, la seule possibilité est que r soit égal à 0. Retournant à l'expression de g, il vient $g=qm\in m\mathbb{Z}$ d'où nous déduisons $G\subset m\mathbb{Z}$ et finalement, par double inclusion, $G=m\mathbb{Z}$. ■

E. 14. Soient m et n deux entiers positifs. A quelle(s) condition(s) $m\mathbb{Z}$ est-il un sous-groupe de $(n\mathbb{Z},+)$? Déterminer l'ensemble des sous-groupes de $(n\mathbb{Z},+)$.

THÉORÈME 6 (Bézout). — *Soient m et n deux entiers non nuls. Définissons $m\mathbb{Z}+n\mathbb{Z}=\{am+bn : (a,b)\in\mathbb{Z}^2\}$. Nous avons*

$$m\mathbb{Z}+n\mathbb{Z}=\mathrm{pgcd}(m,n)\mathbb{Z} \tag{2.1}$$

où $\mathrm{pgcd}(m,n)$ désigne le plus grand commun diviseur de m et de n.

Démonstration. Montrons d'abord que $m\mathbb{Z}+n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. En effet, c'est un ensemble non vide et si $x=a_1m+b-1n\in m\mathbb{Z}+n\mathbb{Z}$ et $y=a_2m+b_2n\in m\mathbb{Z}+n\mathbb{Z}$ alors $x-y=(a_1-a_2)m+(b_1-b_2)n\in m\mathbb{Z}+n\mathbb{Z}$. D'après le théorème 5, il existe donc $d\in\mathbb{N}$ tel que $m\mathbb{Z}+n\mathbb{Z}=d\mathbb{Z}$. Notons maintenant D le plus grand commun diviseur [*] de m et n. Puisque $m=sD$ et $n=s'D$, nous avons $am+bn=(as+bs')D$ de sorte que tous les éléments de $m\mathbb{Z}+n\mathbb{Z}$ sont multiples de D, autrement dit $m\mathbb{Z}+n\mathbb{Z}\subset D\mathbb{Z}$, ou encore $d\mathbb{Z}\subset D\mathbb{Z}$ qui entraîne que D divise d. D'autre part puisque a et b sont éléments de $m\mathbb{Z}+n\mathbb{Z}=d\mathbb{Z}$, l'entier d divise à la fois m et n, il divise donc D. Les relations $d|D$ et $D|d$ donnent $d=D$ [†], ce qu'il fallait établir. ■

Découle du théorème, l'**identité de Bézout** qui affirme qu'il existe toujours $u,v\in\mathbb{Z}$ tels que

$$mu+nv=\text{pgcd}(m,n). \tag{2.2}$$

Notons aussi que les entiers m et n sont premiers entre eux si et seulement si $m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$. La condition nécessaire et suffisante pour que cette condition soit vérifiée est qu'il existe $u,v\in\mathbb{Z}$ tels que $nu+mv=1$. En effet, si $m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$, l'existence d'un tel couple (u,v) est évidente. Réciproquement, si (u,v) existe alors $m\mathbb{Z}+n\mathbb{Z}$ est un sous-groupe de la forme $k\mathbb{Z}$ qui contient 1. Cela force $k=1$ et $\text{pgcd}(m,n)=1$.

s: p. 103 E. 15. Soient m_i, $i=1,\dots,k$, k entiers non nuls. Que vaut $m_1\mathbb{Z}+m_2\mathbb{Z}+\cdots+m_k\mathbb{Z}$? s:10

Le corollaire suivant est souvent appelé **lemme de Gauss**.

COROLLAIRE 7. — *Soient α,β et γ trois entiers non nuls. Si α divise le produit $\beta\gamma$ et α et β sont premiers entre eux alors α divise γ.*

Démonstration. Puisque α et β sont premiers entre eux, nous avons $\text{pgcd}(\alpha,\beta)=1$ et l'identité de Bézout ci-dessus assure l'existence de deux entiers u et v tels que $u\alpha+v\beta=1$. En multipliant l'égalité par γ, nous obtenons $u\alpha\gamma+v\beta\gamma=\gamma$. Puisque α divise $\beta\gamma$, il divise aussi $u\alpha\gamma+v\beta\gamma$ qui n'est autre que γ. C'est ce qu'il fallait établir. ■

s: p. 103 E. 16. Les entiers (u,v) satisfaisant l'identité de Bézout sont-ils uniques ? s:11

(2.2.3) Sous-groupes de $(\mathbb{C}^\star,\cdot)$. Soit $n\in\mathbb{N}^\star$: $\mathbb{Q}^{\star+}<\mathbb{Q}^\star<\mathbb{R}^\star<(\mathbb{C}^\star,\cdot)$ mais aussi $\mathbf{U}_n<\mathbf{U}<(\mathbb{C}^\star,\cdot)$.

NOTE 4. — Rappelons que, d'une manière générale, lorsque $X=\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $X^\star$ désigne $X/\{0\}$. Dans l'étude des anneaux on utilisera la notation A^* qui représente, en général, un ensemble de nature différente, voir 2.1::II.

∗. Par convention, le plus grand commun diviseur de deux entiers non nuls quelconques est toujours positif.

†. Les relations $d|D$ et $D|d$ en général donnent $d=D$ ou $d=-D$ mais ici les deux nombres sont positifs et le seconde alternative est impossible.

(2.2.4) Soit $n \in \mathbb{N}^\star$,

$$\mathbf{GL}_n(\mathbb{Q}) < \mathbf{GL}_n(\mathbb{R}) < (\mathbf{GL}_n(\mathbb{C}), \cdot).$$

Des sous-groupes beaucoup plus importants seront étudiées dans plusieurs chapitres de ce cours. Quelques exemples sont considérés dans l'exercice 50.

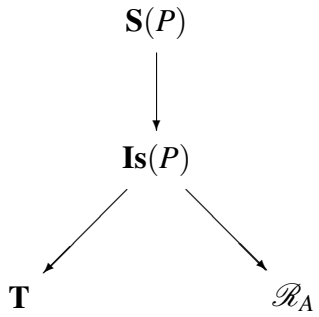
(2.2.5) Sous-groupes des bijections du plan dans lui-même. Nous avons

$$\mathbf{T} < \mathbf{Is}(P) < (\mathbf{S}(P), \circ)$$

où $\mathbf{T}$ l'ensemble des translations du plan euclidien. Pour montrer que $\mathbf{T} < \mathbf{Is}(P)$, il suffit d'observer $t_{\vec{u}} \circ t_{\vec{v}} = t_{\vec{u}+\vec{v}}$.

(2.2.6) Sous-groupes du groupe des isométries du plan euclidien. $\mathscr{R}_A < (\mathbf{Is}(P), \circ)$ où $\mathscr{R}_A$ l'ensemble des rotations de centre A du plan euclidien. Cela provient de la relation $r_{A,\theta} \circ r_{A,\theta'} = r_{A,\theta+\theta'}$.

Les chaînes de sous-groupes sont parfois représentées sous la forme d'un arbre comme celui ci-après qui correspond aux exemples (2.2.5)) et (2.2.6)).



(2.3)

E. 17. Construire un arbre dont le sommet soit $(\mathbb{C}, +)$.

(2.2.7) Si A_1 est un sous-groupe de $(G_1, *)$ et A_2 un sous-groupe de $(G_2, \circ)$ alors $A_1 \times A_2$ est un sous-groupe du produit direct $G_1 \times G_2$.

§ 3. MORPHISMES

3.1 Introduction

L'algèbre élémentaire est pleine d'applications qui se comportent de la manière la plus simple possible dans leurs rapports avec l'une au moins des opérations élémentaires que sont l'addition et la multiplication des nombres réels. Le lecteur sait par exemple que lorsque x et y sont des réels quelconques $(xy)^2 = x^2y^2$, s'ils sont positifs $\sqrt{xy} = \sqrt{x}\sqrt{y}$ ou, dans tous les cas, $|xy| = |x||y|$; il connaît des relations similaires pour les applications $x \mapsto x^\alpha$, d'autres, plus difficiles à mémoriser, comme

$\ln(ab) = \ln(a) + \ln(b)$ ou sa complémentaire $\exp(a+b) = \exp(a)\exp(b)$, ou encore, dans un domaine différent, $\det(AB) = \det A \det B$. Ce type de relation facilite grandement les calculs et c'est pourquoi elle sont enseignées en priorité chaque fois qu'elles existent. Les applications qui les satisfont comme ci-dessus l'élévation au carré, la racine carrée, la valeur absolue, le logarithme, l'exponentielle ou l'application déterminant sur l'ensemble des matrices sont appelés des *morphismes* (une définition précise est donnée plus bas). Le mot est construit sur la racine grecque *morph* qui signifie forme. Les morphismes respectent, en un certain sens, la forme des quantités auxquelles ils s'appliquent. Les mathématiciens professionnels recherchent ces morphismes chaque fois qu'ils ont à travailler avec un ensemble muni d'une loi interne et, dans la plupart des cas, ils sont capables de décider en un clin d'oeil si une application donnée satisfait ou non cette propriété. Les étudiants ont exactement le même intérêt que les professionnels pour les morphismes, simplement ils ont souvent tendance à transformer en des morphismes des applications qui ne le sont pas. Ainsi, par exemple, peuvent-ils écrire au collège [!] $(x+y)^2 = x^2+y^2$ [!] lorsque x et y sont dans $\mathbb{R}$ comme simple extrapolation de la relation $(xy)^2 = x^2y^2$ ou, à l'université [!] $\det(A+B) = \det A + \det B$ [!] lorsque A et B sont des matrices d'ordre ≥ 2, deux relations également insensées. L'objet de cette partie est d'étudier les propriétés des morphismes des lois de groupes et de mettre en évidence leur intérêt dans l'étude des groupes eux-mêmes.

3.2 Definition

Soit $(G,*)$ et $(G',\circ)$ deux groupes et φ une application de G dans G' : $\varphi : G \to G'$. Nous disons que l'application φ est un **morphisme** de groupe (ou simplement un morphisme) lorsqu'elle vérifie

$$\varphi(a*b) = \varphi(a) \circ \varphi(b), \qquad a, b \in G. \tag{3.1}$$

Autrement dit, φ *est un morphisme si l'image d'un quelconque* $*$*-produit est le* $\circ$*-produit des images*.

Il y a une terminologie assez sophistiquée pour décrire divers types de morphismes. D'abord, les morphismes sont aussi appelés **homomorphismes**. L'ensemble des morphismes de G dans G' est noté $\mathsf{Hom}(G,G')$. Lorsque le groupe de départ et le groupe d'arrivée sont les mêmes, le terme **endomorphisme** est employé et l'ensemble des endomorphismes est noté $\mathsf{End}(G)$ de sorte que $\mathsf{End}(G) = \mathsf{Hom}(G,G)$. Un morphisme bijectif est un **isomorphisme**. Enfin, un isomorphisme de G dans lui-même s'appelle un **automorphisme** ; l'ensemble des automorphismes de G est noté $\mathsf{Aut}(G)$ si bien que $\mathsf{Aut}(G) = \mathsf{End}(G) \cap \mathbf{S}(G)$.

s: p. 103 E. 18. L'ensemble $\mathsf{Hom}(G,G')$ peut-il être vide ? [s:12]

s: p. 103 E. 19. Montrer que si $f \in \mathsf{Hom}(G,G')$ et $g \in \mathsf{Hom}(G',G'')$ alors $g \circ f \in \mathsf{Hom}(G,G'')$. [s:13]

NOTE 5. — Sont aussi employés dans la littérature les terme de **monomorphisme** pour désigner un morphisme injectif et celui d'**épimorphisme** pour un morphisme surjectif. Nous ne ferons pas appel à ce

vocabulaire dans ce cours. La préposition *sur* est souvent employée devant l'ensemble d'arrivée lorsque l'application est surjective. Si $f : A \longrightarrow B$ est surjective, f est une surjection de A *sur* B. La même convention vaut pour les bijections qui ne sont que des surjections particulières.

THÉORÈME 8. — *Si $\varphi : G \to G'$ est un isomorphisme alors l'application réciproque $\varphi^{-1} : G' \to G$ (qui existe puisque φ est bijective) est elle-même un isomorphisme.*

Démonstration. Si $x, y \in G'$ alors, puisque φ est bijective, il existe a et b dans G tels que $\varphi(a) = x$ et $\varphi(b) = y$. De plus,

$$x \circ y = \varphi(a) \circ \varphi(b) = \varphi(a * b)$$

car φ est un morphisme. Il suit que

$$\varphi^{-1}(x \circ y) = \varphi^{-1}(\varphi(a * b)) = a * b = \varphi^{-1}(x) * \varphi^{-1}(y). \quad \blacksquare$$

COROLLAIRE 9. — *$\mathsf{Aut}(G)$ est un sous-groupe de $(\mathbf{S}(G), \circ)$.*

Démonstration. $\mathsf{Aut}(G)$ est un sous-ensemble non vide de $\mathbf{S}(G)$ car l'application identité est élément de $\mathsf{Aut}(G)$. De plus si $f, g \in \mathsf{Aut}(G)$ alors $f \circ g$ est encore un morphisme de G de G et aussi une bijection de G sur G comme composée de deux bijections de G sur G. Enfin si $f \in \mathsf{Aut}(G)$ alors $f^{-1} \in \mathsf{Aut}(G)$ par application du théorème précédent (avec $G = G'$). ■

Lorsqu'il existe un isomorphisme entre G et G', nous disons que G et G' sont *isomorphes* et notons $G \simeq G'$.

THÉORÈME 10. — *L'image de l'élément neutre du groupe de départ par un morphisme est l'élément neutre du groupe d'arrivée.* [$\varphi(e_G) = e_{G'}$].

Démonstration. Soit φ un morphisme de $(G, *)$ dans $(G', \circ)$. Nous avons $\varphi(e_G * e_G) = \varphi(e_G) \circ \varphi(e_G)$ et puisque e_G est élément neutre $e_G * e_G = e_G$. Il suit que

$$\begin{aligned} & \varphi(e_G) = \varphi(e_G) \circ \varphi(e_G) \\ \Rightarrow\ & [\varphi(e_G)]^{-1} \circ \varphi(e_G) = [\varphi(e_G)]^{-1} \circ \varphi(e_G) \circ \varphi(e_G) \\ \Rightarrow\ & e_{G'} = e_{G'} \circ \varphi(e_G) \\ \Rightarrow\ & e_{G'} = \varphi(e_G). \end{aligned}$$ ■

THÉORÈME 11. — *Par un morphisme l'image du symétrique d'un élément est le symétrique de l'image de cet élément.* [$\varphi(g^{-1}) = [\varphi(g)]^{-1}$.]

NOTE 6. — Il faut bien prendre garde ici de ne pas confondre $[\varphi(g)]^{-1}$ avec $\varphi^{-1}(g)$. C'est une erreur très commune chez les débutants. La première formule désigne le symétrique de l'élément $\varphi(g) \in G'$ qui existe toujours puisque G' est un groupe. En particulier, $[\varphi(g)]^{-1} \in G'$. La seconde n'a de sens que lorsque φ est une bijection – à moins que, par un abus de notation assez courant, elle ne désigne $\varphi^{-1}(\{g\})$, l'image réciproque par φ du singleton $\{g\}$ – qui n'a de sens de toute manière que si $g \in G'$ et qui désigne alors un sous-ensemble de G.

Démonstration. Soient φ un morphisme de $(G,*)$ dans $(G',\circ)$ et $g \in G$. Nous avons

$$\begin{array}{ll} & g*g^{-1} = e_G = g^{-1}*g \\ \Longrightarrow & \varphi(g*g^{-1}) = \varphi(e_G) = \varphi(g^{-1}*g) \\ \Longrightarrow & \varphi(g)\circ\varphi(g^{-1})) = e_{G'} = \varphi(g^{-1})\circ\varphi(g) \quad \text{(utilise le théorème 10).} \end{array}$$

Cela signifie que $\varphi(g^{-1})$ satisfait aux deux conditions définissant le symétrique de $\varphi(g)$ donc $\varphi(g^{-1}) = [\varphi(g)]^{-1}$. ■

E. 20. Déterminer tous les endomorphismes de $(\mathbb{Z},+)$. Lesquels sont-ils des automorphismes ? Même question lorsque $(\mathbb{Z},+)$ est remplacé par $(\mathbb{Q},+)$.

E. 21. Nous avons vu que $\mathtt{Aut}(G)$ est un sous-groupe de $S(G)$. Est-il possible que $\mathtt{Aut}(G)$ soit égal à $S(G)$?

3.3 Morphismes et images des sous-groupes

THÉORÈME 12. — *Soient φ un morphisme de G dans G' et H un sous-groupe de G alors $\varphi(H)$ est un sous-groupe de G'. En particulier $\varphi(G)$ est un sous-groupe de G'.* [$H \leq G \Rightarrow \varphi(H) \leq G'$.]

Rappelons que $\varphi(H) := \{\varphi(h) : h \in H\}$ et s'appelle l'**image** de H par φ.

Démonstration. Pour montrer que $\varphi(H)$ est un sous-groupe de G' nous devons vérifier (1) qu'il est non vide et (2) pour tous $x,y \in \varphi(G)$ nous avons $x\circ y^{-1} \in \varphi(G)$. Que $\varphi(H)$ soit non vide est clair car, d'après le Théorème 10, $e_G \in H \Rightarrow \varphi(e_G) = e_{G'} \in \varphi(H)$. Quant au second point, si $x, y \in \varphi(H)$ alors $x = \varphi(a)$ et $y = \varphi(b)$ avec $a, b \in H$. Donc

$$\begin{array}{lll} x\circ y^{-1} & = \varphi(a)\circ[\varphi(b)]^{-1} & \\ & = \varphi(a)\circ\varphi(b^{-1}) = \varphi(a*b^{-1}) & \text{(utilise le théorème 11)} \\ & \in \varphi(H) & \text{(car } a,b \in H \text{ et } H \leq G\text{),} \end{array}$$

donc $\varphi(H)$ est bien un sous-groupe de G'. ■

3.4 Le noyau d'un morphisme

Soit φ un morphisme de $(G,*)$ dans $(G',\circ)$. Nous appelons **noyau** de φ et notons $\ker\varphi$ — "ker" est l'abréviation du mot allemand *kernel* qui signifie noyau — l'ensemble

$$\ker\varphi = \{g \in G \ : \ \varphi(g) = e_{G'}\} \tag{3.2}$$

D'après le Théorème 10, nous avons toujours $\varphi(e_G) = e_{G'}$ donc $e_G \in \ker\varphi$ qui n'est ainsi jamais vide.

THÉORÈME 13. — *Le noyau d'un morphisme est un sous-groupe du groupe de départ.* [$\ker\varphi \leq G$].

Démonstration. Puisque $\ker\varphi \neq \emptyset$ il suffit de vérifier que $x, y \in \ker\varphi \Rightarrow x * y^{-1} \in \ker\varphi$. Or

$$\begin{array}{lll} \varphi(x*y^{-1}) & = \varphi(x)\circ\varphi(y^{-1}) & \text{(utilise la définition d'un morphisme)} \\ & = \varphi(x)\circ[\varphi(y)]^{-1} & \text{(utilise le théorème 11.)} \\ & = e_{G'}\circ[e_{G'}]^{-1} & \text{(utilise la définition du noyau.)} \\ & = e_{G'}. & \end{array}$$

Il suit que $x * y^{-1} \in \ker\varphi$ qui est donc bien un sous-groupe. ■

Le noyau vérifie une autre propriété. Si $g \in G$ et $x \in \ker\varphi$ alors $g * x * g^{-1} \in \ker\varphi$. En effet,

$$\begin{array}{lll} \varphi(g*x*g^{-1}) & = \varphi(g)\circ\varphi(x)\circ\varphi(g^{-1}) & \\ & = \varphi(g)\circ\varphi(x)\circ[\varphi(g)]^{-1} & \text{(utilise le théorème 11)} \\ & = \varphi(g)\circ e_{G'}\circ[\varphi(g)]^{-1} & \\ & = \varphi(g)\circ[\varphi(g)]^{-1} & \\ & = e_{G'}. & \end{array}$$

Les groupes vérifiant cette propriété sont dits distingués. Cette notion très utile sera étudiée par la suite.

THÉORÈME 14. — *Pour qu'un morphisme soit injectif il faut et il suffit que son noyau se réduise à l'élément neutre.* [$\varphi : G \overset{\text{morph.}}{\longrightarrow} G'$ injective $\Leftrightarrow \ker\varphi = \{e_G\}$.]

Rappelons qu'une application φ est dite **injective** lorsque deux éléments distincts ont nécessairement deux images distinctes. Autrement dit l'hypothèse $\varphi(x) = \varphi(y)$ doit toujours impliquer $x = y$.

Démonstration. ($\Longrightarrow$) *Nous supposons que φ est injective et montrons que* $\ker\varphi = \{e_G\}$.

Nous savons que $e_G \in \ker\varphi$. Si x est un autre élément de $\ker\varphi$ avec $x \neq e_G$ alors $\varphi(e_G) = e_{G'} = \varphi(x)$ donc x et e_G ont la même image sans être égaux, ce qui contredit l'injectivité de φ.

($\Longleftarrow$) *Nous supposons que* $\ker\varphi = \{e_G\}$ *et montrons que φ est injective.*

Supposons que x et y soient deux éléments de G tels que $\varphi(x) = \varphi(y)$. Nous avons

$$\begin{array}{lll} & \varphi(x)\circ[\varphi(y)]^{-1} = e_{G'} & \\ \Rightarrow & \varphi(x)\circ\varphi(y^{-1}) = e_{G'} & \text{(par le Théorème 11)} \\ \Rightarrow & \varphi(x*y^{-1}) = e_{G'} & \\ \Rightarrow & x*y^{-1} \in \ker\varphi & \\ \Rightarrow & x*y^{-1} = e_G & \text{(car } \ker\varphi = \{e_G\}\text{)} \\ \Rightarrow & x = y & \end{array}$$

L'hypothèse $\varphi(x) = \varphi(y)$ implique donc $x = y$ et φ est bien injective. ■

THÉORÈME 15. — *Soient G et G' deux groupes finis de* même cardinal *et φ un morphisme de G dans G'. Pour que φ soit un isomorphisme il faut et il suffit que* $\ker\varphi$ *soit réduit à l'élément neutre.*

Démonstration. Lorsque G et G' sont des ensembles finis, de même cardinal, dire que $\varphi : G \to G'$ est bijective est équivalent à dire qu'elle est injective. Le théorème est donc une conséquence directe du théorème 14. ■

E. 22. Montrer que pour tout $m \in \mathbb{N}$, l'application ϕ_m définie sur $\mathbf{U}_6$ par $\phi(z) = z^m$ est un endomorphisme. Tous les endomorphismes de $\mathbf{U}_6$ sont-ils de cette forme ? Combien y-en-a-t-il ? Lesquels sont des automorphismes ? Le cas général où $\mathbf{U}_6$ est remplacé par $\mathbf{U}_n$ sera considéré plus loin.

3.5 Morphismes et image-réciproque des sous-groupes

Soit φ un morphisme de $(G,*)$ dans $(G',\circ)$. S'il n'est permis de parler de l'élément $\varphi^{-1}(g)$ que lorsque φ est bijective (et $g \in G'$), nous pouvons toujours considérer l'ensemble $\varphi^{-1}(\{g\})$, qui est formé, par définition, de tous les éléments $x \in G$ tels que $\varphi(x) = g$. Cet ensemble $\varphi^{-1}(\{g\})$ peut-être vide et il est égal à $\{\varphi^{-1}(g)\}$ lorsque (mais pas seulement) φ est bijective. D'un manière générale, si $Y \subset G'$, l'ensemble défini par

$$\varphi^{-1}(Y) = \{x \in G : \varphi(x) \in Y\}$$

est appelé **image-réciproque** ou **pré-image** de Y par φ et il est noté $\varphi^{-1}(Y)$.

Remarquons que $\ker\varphi = \varphi^{-1}(\{e_{G'}\})$.

THÉORÈME 16. — *Soient φ un morphisme de G dans G' et W un sous-groupe de G' alors $\varphi^{-1}(W)$ est un sous-groupe de G qui contient* $\ker\varphi$. [$W \leq G' \Rightarrow \varphi^{-1}(W) \leq G$.]

Démonstration. Puisque W est sous-groupe de G', $e_{G'} \in W$ de sorte que

$$\ker\varphi = \varphi^{-1}(\{e_{G'}\}) \subset \varphi^{-1}(W)$$

qui n'est donc pas vide. Il suffit maintenant de vérifier que $x, y \in \varphi^{-1}(W) \Rightarrow x * y^{-1} \in \varphi^{-1}(W)$. Or

$$\begin{aligned} & \varphi(x*y^{-1}) = \varphi(x)\circ\varphi(y^{-1}) && \text{(définition d'un morphisme)} \\ & \qquad = \varphi(x)\circ[\varphi(y)]^{-1} && \text{(utilise le théorème 11.)} \\ \Rightarrow\quad & \varphi(x*y^{-1}) \in W\circ W \subset W && \text{(car } W \leq G.\text{)} \end{aligned}$$

Donc $x * y^{-1} \in \varphi^{-1}(W)$ qui est bien un sous-groupe. ■

3.6 Exemples de morphismes

(3.6.1) Exponentielle et logarithme L'application

$$\exp : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{\star+},.)\\ x & \longmapsto & \exp x.\end{array}$$

est un isomorphisme, et $\exp^{-1} = \ln$.

(3.6.2) Exponentielle complexe. Est un morphisme l'application

$$E_{\mathbb{C}} : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbf{U},.)\\ x & \longmapsto & \exp ix.\end{array}$$

Nous avons

$$\ker E_{\mathbb{C}} = \{x \in \mathbb{R} : \exp(ix) = 1\} = \{x \in \mathbb{R} : x = 2k\pi,\ k \in \mathbb{Z}\} = 2\pi\mathbb{Z}. \tag{3.3}$$

(3.6.3) Le déterminant.

$$\det : \begin{array}{ccc}\mathbf{GL}_n(\mathbb{K}) & \longrightarrow & (\mathbb{K}^{\star},.)\\ A & \longmapsto & \det A\end{array}$$

Nous avons

$$\ker\det = \{A \in \mathbf{GL}_n(\mathbb{K}) : \det A = 1\} := \mathbf{SL}_n(\mathbb{K}).$$

(3.6.4) Les automorphismes intérieurs. Soit $(G,\cdot)$ un groupe et $x \in G$. L'application

$$\phi_x : \begin{array}{ccc}(G,\cdot) & \longrightarrow & (G,\cdot)\\ g & \longmapsto & x^{-1}\cdot g\cdot x.\end{array}$$

est un automorphisme. Tout automorphisme construit de cette manière s'appelle un **automorphisme intérieur**. L'ensemble des automorphismes intérieurs, noté $\mathsf{Int}(G)$, forme lui-même un groupe lorsqu'il est muni de la loi de composition des applications.

*(3.6.5) L'application **puissance**.* Soit $(G,*)$ un groupe quelconque et $g \in G$. L'application suivante est un morphisme de groupe.

$$p_g : \begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,*)\\ m & \longmapsto & g^m\end{array}.$$

*(3.6.6) **Projection**.* Soit $W = G_1 \times G_2$ le produit direct des groupes $(G_1,*)$ et $(G_2,\circ)$. L'application $\mathbf{proj}_{G_1}$ définie sur W à valeurs dans G_1 par la relation

$$\mathbf{proj}_{G_1}(g_1,g_2) = g_1$$

est une morphisme surjectif dont le noyau est le groupe $\{e_{G_1}\} \times G_2$.

E. 23. Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes. Montrer que les produits directs $G_1 \times G_2$ et $G_2 \times G_1$ sont isomorphes : construire un isomorphisme entre les deux groupes. Pour la définition du produit direct, voir (1.8.7).

§ 4. PARTIES GÉNÉRATRICES D'UN GROUPE

4.1 Introduction

Le groupe $(\mathbb{Z},+)$ possède la propriété remarquable de pouvoir être reconstruit à partir du seul élément 1 : tous les éléments de $\mathbb{Z}$ s'écrivent en additionnant 1 un certain nombre de fois et éventuellement en prenant le symétrique du résultat obtenu, par exemple, $-5=-(1+1+1+1+1)$. Une telle propriété n'est certainement pas vraie pour $(\mathbb{R},+)$. Le produit direct $(\mathbb{Z}^2,+)$ lui peut-être reconstruit à l'aide des deux seuls éléments $(1,0)$ et $(0,1)$ [*] et le groupe $\mathbf{U}_4=\{1,-1,i,-i\}$ à partir de l'élément i puisque $1=i^4$, $-1=i^2$ et $-i=i^3$. Pourquoi certains groupes peuvent-ils être reconstruits à partir d'un nombre fini de leurs éléments, et comment ces reconstructions s'effectuent-elles ? Ce sont deux questions que nous étudions dans cette partie.

4.2 Intersections de sous-groupes

THÉORÈME 17. — *Soient $(G,*)$ un groupe et $\mathscr{F}$ une famille non vide de sous-groupes de G. Si I est l'intersection de tous les éléments de $\mathscr{F}$, autrement dit $I=\bigcap_{H\in\mathscr{F}} H$ alors I est lui-même un sous-groupe de G.*

Notons que $\mathscr{F}$ peut contenir un nombre fini ou infini de sous-groupes.

Démonstration. D'abord I est non vide car e_G est élément de tout sous-groupe F de $\mathscr{F}$ et il appartient donc à I. Soient $x,y\in I$, nous voulons montrer que $x*y^{-1}\in H$. Par définition de I, pour tout $H\in\mathscr{F}$, nous avons $x,y\in H$ et puisque H est un sous-groupe $x*y^{-1}\in H$. Il suit que $x*y^{-1}$ appartient à tous les éléments de $\mathscr{F}$ et donc à I. Cela montre que I est bien un sous groupe. ∎

E. 24. Si m et n sont deux entiers positifs, déterminer le sous-groupe de $\mathbb{Z}$ défini par $m\mathbb{Z}\cap n\mathbb{Z}$.

4.3 Sous-groupe engendré par une partie

Soit $(G,*)$ un groupe et A un sous-ensemble *non vide* de G. Nous appellons **sous-groupe engendré** par A le sous-groupe

$$\langle A\rangle := \bigcap_{H\in\mathscr{S}(A)} H \tag{4.1}$$

où $\mathscr{S}(A)$ est l'ensemble de tous les sous-groupes de G qui contiennent A. Cet ensemble n'est pas vide car il contient G lui-même. En vue du Théorème 17, la formule (4.1) définit bien un sous-groupe de G.

∗. Il suffit d'écrire $(m,n)=(m,0)+(0,n)$ puis exprimer $(m,0)$ à l'aide de $(1,0)$ et $(0,n)$ à l'aide de $(0,1)$.

THÉORÈME 18. — *Le sous-groupe $\langle A\rangle$ est le plus petit sous-groupe de G contenant A.*

Ici l'adjectif 'petit' réfère à la relation d'ordre définie par l'inclusion des ensembles : un ensemble X est plus petit qu'un ensemble Y si $X \subset Y$. De manière précise, le théorème 18 signifie que les deux assertions suivantes sont équivalentes

(E1) $I = \langle A\rangle$.

(E2) I vérifie les deux conditions suivantes

(a) I est un sous-groupe de G contenant A et

(b) Si H est un autre sous-groupe de G contenant A alors $I \subset H$.

Démonstration. D'après la définition, nous avons immédiatement que $\langle A\rangle$ vérifie les deux conditions de (E2). Nous montrons que si I vérifie (a) et (b) alors $I = \langle A\rangle$. A cause de (b), $I \subset \bigcap_{H\in\mathscr{S}(A)} H = \langle A\rangle$. D'autre part, puisque, d'après (a), I est un sous-groupe contenant A, nous avons $I \in \mathscr{S}(A)$ et par conséquent $\bigcap_{H\in\mathscr{S}(A)} H \subset I$ soit $\langle A\rangle \subset I$. Par double inclusion nous en déduisons $I = \langle A\rangle$. ■

Ni la définition, ni cette caractérisation ne permettent de se faire une idée de la nature des éléments de $\langle A\rangle$. Le paragraphe suivant donne une approche *constructive* des sous-groupes engendrés.

4.4 Description des éléments d'un sous-groupe engendré

THÉORÈME 19. — *Soient $(G,*)$ un groupe, A un sous-ensemble non vide de G et $x \in G$. Pour que $x \in \langle A\rangle$ il faut et il suffit qu'il existe $n \in \mathbb{N}^\star$ et des éléments $x_1, x_2, \ldots, x_n$ avec $x_i \in A$ ou $x_i^{-1} \in A$ pour $i = 1, 2, \ldots, n$ tels que $x = x_1 * x_2 * \cdots * x_n$.*

Le théorème affirme l'égalité

$$\langle A\rangle = \{x_1 * x_2 * \cdots * x_n : n \in \mathbb{N}^\star, x_i \text{ ou } x_i^{-1} \in A, i = 1, \ldots, n\}, \tag{4.2}$$

ou encore

$$\langle A\rangle = \{g_1^{\pm 1} * g_2^{\pm 1} * \cdots * g_n^{\pm 1} : n \in \mathbb{N}^\star \text{ et } g_i \in A, i = 1, \ldots, n\}, \tag{4.3}$$

où le symbole $\pm$ signifie que nous pouvons prendre aussi bien g_i que g_i^{-1} de sorte que $g_1^{\pm 1} * g_2^{\pm 1} * \cdots * g_n^{\pm 1}$ désigne 2^n expressions différentes. Il faut bien prendre garde que si ces expressions sont *formellement* différentes, certaines d'entre elles peuvent bien, suivant la nature de G, donner le même résultat. Insistons aussi sur le fait que le nombre de facteurs n, en général, dépend de x.

Démonstration. Appelons I le membre de droite dans (4.2) (ou (4.3)), nous devons montrer que $I = \langle A\rangle$. Pour cela, d'après le Théorème 18, il suffit de vérifier l'assertion (E2) c'est-à-dire

– I est un sous-groupe de G contenant A et
– tout sous-groupe de G contenant A contient aussi I.

Étape 1. I est un sous-groupe de G contenant A.

En considérant les cas où $n = 1$ et $x_1 \in A$ dans (4.2) nous voyons que $A \subset I$. En particulier I est non vide. Montrons que c'est un sous-groupe de G. Pour cela prenons x et y dans I et vérifions que $x * y^{-1} \in I$. Ecrivons

$$\begin{cases} x = x_1 * x_2 * \cdots * x_m & x_i \in A \text{ ou } x_i^{-1} \in A \\ y = y_1 * y_2 * \cdots * y_p & y_i \in A \text{ ou } y_i^{-1} \in A \end{cases} \quad \text{(Attention, en général } m \neq p\text{).}$$

En utilisant la formule 1.4 (p. 9) sur l'inverse d'un produit nous obtenons

$$x * y^{-1} = x_1 * x_2 * \cdots * x_m * y_p^{-1} * \cdots * y_1^{-1}$$

Chacun des $m + p$ facteurs f du produit vérifie $f \in A$ ou $f^{-1} \in A$ de sorte que $x * y^{-1}$ a bien la forme requise (avec $n = m + p$) des éléments de I. Il suit que $x * y^{-1} \in I$ et I est donc bien un sous-groupe de G contenant A.

Étape 2. Si H est un sous-groupe de G contenant A alors $I \subset H$.

Prenons $x \in I$ que nous écrivons comme précédemment $x = x_1 * x_2 * \cdots * x_n$. Etudions le facteur x_i. Il y a deux possibilités :
– Soit $x_i \in A$ et alors $x_i \in H$ puisque $A \subset H$
– Soit $x_i^{-1} \in A$ et alors $x_i^{-1} \in H$ puis, puisque H est un sous-groupe, $x_i = (x_i^{-1})^{-1} \in H$.

Dans les deux cas $x_i \in H$ de sorte que, toujours puisque H est un sous-groupe, $x \in H$ comme produit d'éléments de H. Cela achève la démonstration de la deuxième étape et du théorème. ■

Lorsque une partie (non vide) A vérifie $\langle A \rangle = G$, nous disons que A *engendre* G ou que G est *engendré* par A ou encore que A est une **partie génératrice** de G. Pour bien des questions, il est raisonnable de considérer qu'une bonne connaissance du groupe G est acquise si nous avons pu mettre en évidence une partie génératrice *la plus petite possible* car nous pouvons alors décrire par la formule assez simple (4.2) tous les éléments du groupe. Cette notion peut rappeler au lecteur celle de partie génératrice d'un espace vectoriel. Il y a une différence fondamentale. Nous savons que dans un espace vectoriel de dimension finie, de toute partie génératrice, nous pouvons extraire une partie génératrice minimale (quand nous lui retirons un quelconque de ses éléments elle n'est plus génératrice) et cette partie génératrice minimale n'est autre qu'une base de l'espace vectoriel. En particulier, toutes les parties génératrices minimales possèdent le même nombre d'éléments, ce nombre étant égal à la dimension de l'espace vectoriel. Cette propriété ne demeure pas en général pour les parties génératrices des groupes. Il existe par exemple des parties génératrices minimales de $(\mathbb{Z}, +)$ qui contiennent k

éléments, k étant un entier positif quelconque. De telles parties sont construites dans l'exercice 26.

Les groupes les plus simples sont ceux qui sont engendrés par un singleton. Nous étudions ce cas dans la partie suivante.

4.5 Groupes cycliques et ordre d'un élément

Nous disons qu'un groupe $(G,*)$ est **cyclique** s'il est engendré par un ensemble réduit à un seul élément i.e. $G = \langle\{a\}\rangle$. Nous notons aussi pour alléger l'écriture $G = \langle a\rangle$. D'après la formule (4.2), tout élément de G s'écrit alors

$$x = a^{\pm 1} * a^{\pm 1} * \cdots * a^{\pm 1} = a^m \quad \text{avec } m \in \mathbb{Z}$$

de sorte que

$$G = \{a^m : m \in \mathbb{Z}\}.$$

Il se peut que les éléments dans l'ensemble de droite ne soient pas tous deux à deux distincts. Si $a^{m_1} = a^{m_2}$ avec, disons, $m_1 > m_2$ alors $a^{m_1 - m_2} = e$ et dans ce cas la description de G peut encore être simplifiée. Appelons d le plus petit entier strictement positif tel que $a^d = e$. Notre supposition implique l'existence de cet entier d avec $d \leq m_1 - m_2$. Nous disons que a est d'**ordre** (fini) d et nous écrivons $o(a) = d$. Dans ces conditions,

$$G = \{a^i : i = 0, 1, \ldots, d-1\}.$$

En effet, si m est un entier quelconque, en effectuant une division euclidienne, nous pouvons écrire $m = dq + r$ avec $r \in \{0, 1, \ldots, d-1\}$ d'où

$$a^m = a^{dq+r} = (a^d)^q * a^r = e^q * a^r = a^r$$

de sorte que $\{a^m : m \in \mathbb{Z}\} = \{a^i : i = 0, 1, \ldots, d-1\}$. Notons que l'ensemble $\{a^i : i = 0, 1, \ldots, d-1\}$ ne peut pas être davantage réduit. En effet si $a^i = a^{i'}$ avec $i > i'$ alors $a^{i-i'} = e$ or $0 < i - i' \leq i < d$ et cela contredit le fait que d est le plus petit entier positif vérifiant $a^d = e$. Nous avons démontré le théorème suivant.

THÉORÈME 20. — *Soit $(G,*)$ un groupe cyclique engendré par a. Il y a deux possibilités.*

- Ou bien *a est d'ordre fini $d \in \mathbb{N}^\star$ et $G = \{a^i : i = 0, 1, \ldots d-1\}$*
- ou bien *a n'est pas d'ordre fini (on dit alors qu'il est d'ordre infini) et $G = \{a^m : m \in \mathbb{Z}\}$.*

Dans chaque cas les éléments des ensembles indiqués sont deux à deux distincts.

Le mot *ordre* a déjà été utilisé pour désigner le cardinal d'un groupe. Ici, nous pouvons remarquer que l'ordre d'un élément est égal à l'ordre (au cardinal) du groupe qu'il engendre, i.e. $o(a) = |\langle a\rangle|$, et cela justifie l'emploi du même mot *ordre* pour désigner deux concepts différents. Notons encore que les groupes cycliques sont toujours abéliens.

NOTE 7. — Beaucoup d'auteurs appellent groupe **monogène** ce que nous avons appelé groupe cyclique infini et garde la dénomination de cyclique au seuls groupes finis.

E. 25. Quelle est la forme de la table d'un groupe cyclique si les éléments sont ordonnés comme suit : $e, a, a^2, \ldots, a^n$?

4.6 Groupes cycliques et fonction puissance

Rappelons que si $(G,*)$ est un groupe et $g \in G$ alors le morphisme p_g défini de $(\mathbb{Z},+)$ dans $(G,*)$ par $p_g(m) = g^m$ est appelé puissance.

(i) Si g est d'ordre infini p_g est injective.

(ii) Si g est d'ordre d $\ker p_g = d\mathbb{Z}$.

Montrons le second point. Si $m \in \ker p_g$ alors $g^m = e$ mais, effectuant une division euclidienne, $m = qd + r$ avec $r \in \{0, 1, \ldots, d-1\}$. Par conséquent $g^m = e \Rightarrow g^{qd+r} = e \Rightarrow (g^d)^q * g^r = e \Rightarrow e^q g^r = e \Rightarrow g^r = e$. La seule possibilité est que $r = 0$ car $r < d$ et d est l'ordre de g c'est-à-dire le plus petit entier positif pour lequel $g^d = e$. Maintenant $r = 0$ donne $m = qd$ i.e. $m \in d\mathbb{Z}$. Cela prouve $\ker p_g \subset d\mathbb{Z}$. Il est facile de vérifier $d\mathbb{Z} \subset \ker p_g$ d'où $\ker p_g = d\mathbb{Z}$.

Du premier point, nous tirons le théorème suivant.

THÉORÈME 21. — *Si* $(G,*)$ *est un groupe cyclique* infini *alors* $(G,*) \simeq (\mathbb{Z},+)$.

Démonstration. Si $G = \langle g \rangle$ alors, par définition p_g est surjectif et puisque nous savons que c'est un morphisme injectif, c'est un isomorphisme. ■

4.7 Exemples de sous-groupes engendrés

(4.7.1) Dans $(\mathbb{Z},+)$.

Exemple 1. Pour tout $m \in \mathbb{Z}$, $\langle m \rangle = m\mathbb{Z}$.

En effet, les éléments de $\langle m \rangle$ sont les entiers x qui s'écrivent $x = \pm m \pm m \pm \cdots \pm m = rm$ avec $r \in \mathbb{Z}$.

Exemple 2. Quels que soient les entiers m et n, $\langle m,n \rangle = \text{pgcd}(m,n)\mathbb{Z}$. En particulier si m et n sont premiers entre eux alors $\langle m,n \rangle = \mathbb{Z}$.

En effet, les élément de $\langle m, n \rangle$ sont les entiers s qui s'écrivent

$$s = \pm \begin{pmatrix} m \\ \text{ou} \\ n \end{pmatrix} + \pm \begin{pmatrix} m \\ \text{ou} \\ n \end{pmatrix} + \cdots + \pm \begin{pmatrix} m \\ \text{ou} \\ n \end{pmatrix} = pm + rn \quad \text{avec } p, r \in \mathbb{Z}.$$

Or le théorème 6 de Bézout dit que lorsque p et r parcourent $\mathbb{Z}$ alors l'entier $pm + rn$ parcourt $\text{pgcd}(m,n)\mathbb{Z}$.

E. 26. Soit $k \in \mathbb{N}^\star$. Nous construisons une partie génératrice pour $(\mathbb{Z},+)$. Soient $r_1, \ldots, r_k$, k nombres premiers deux à deux distincts. On note $l_i = \prod_{j \neq i} r_j$ et $L = \{l_1, l_2, \ldots, l_k\}$. (a) Montrer que les élements de L sont premiers dans leur ensemble. Cela signifie que 1 est leur seul diviseur

commun positif. (b) Montrer en utilisant l'exercice 15 que $\mathbb{Z} = \langle L \rangle$. (c) Montrer que L est une partie génératrice minimale. Autrement dit, vérifier que si $L' \subset L$, $L' \neq L$ alors $\langle L' \rangle \neq \mathbb{Z}$.

(4.7.2) Eléments générateurs du groupe des racines de l'unité. Nous avons

$$\mathbf{U}_n = \langle \exp(2i\pi/n) \rangle.$$

En effet,

$$\mathbf{U}_n = \left\{ \exp \frac{2ik\pi}{n} : k = 0, 1, \ldots, n-1 \right\} = \{\phi^k : k = 0, 1, \ldots, n-1\}$$

où $\phi = \exp \frac{2i\pi}{n}$. En particulier, $o(\phi) = n$. Le groupe $\mathbf{U}_n$ est donc cyclique d'ordre n.

(4.7.3) Parties génératrices de $\mathbf{Is}(P)$. On démontre en géométrie que toute isométrie du plan s'écrit comme la composée d'au plus trois réflexions (symétries orthogonales) de sorte que

$$\mathbf{Is}(P) = \langle s_D : D \text{ droite du plan} \rangle.$$

(4.7.4) Sous-groupe engendré par la réunion de deux sous-groupes dans un groupe abélien.

THÉORÈME 22. — *Soient G un groupe abélien, H et W deux sous-groupes de G.*

$$\langle H \cup W \rangle = HW$$

où $HW := \{hw : h \in H,\ w \in W\}$

E. 27. Si X est une partie génératrice de G_1 et Y une partie génératrice de G_2 alors $X \times Y$ est une partie génératrice de $G_1 \times G_2$.

§ 5. RELATION D'ÉQUIVALENCE DÉFINIE PAR UN SOUS-GROUPE

5.1 Définition

Nous initions dans cette partie l'étude du concept le plus abstrait de ce cours et souvent le plus difficile à appréhender, celui du calcul sur les classes d'équivalence. Il n'est pas possible d'expliquer ici le caractère naturel et la portée de ce calcul mais nous pouvons au moins montrer comment il s'inscrit dans la continuité de pratiques déjà bien maîtrisées par le lecteur. Les étudiants de deuxième année d'université ont déjà l'habitude de manier des inégalités modulo une certaine quantité. Ils savent la signification d'une affirmation comme $\pi/6$ *et* $-11\pi/6$ *sont égaux modulo* 2π qui s'écrit symboliquement sous la forme

$$\pi/6 = -11\pi/6 \quad [2\pi].$$

Au début, l'emploi du signe $=$ peut gêner et il est généralement préférable d'employer une expression et une notation plus précises, $\pi/6$ *et* $-11\pi/6$ *sont congrus modulo* 2π et $\pi/6 \equiv -11\pi/6 \quad [2\pi]$. Cette notation est essentielle pour traduire le fait qu'une rotation de 2π (de centre l'origine) laisse tout point invariant. En d'autres mots, un nombre complexe dont les arguments sont congrus sont alignés. Une notation similaire est employée en arithmétiques. On écrit

$$5 = 11 \quad [6] \qquad \text{ou} \qquad 5 \equiv 11 \quad [6]$$

pour dire que 5 et 11 ont le même reste dans leur division euclidienne par 6. Cette notation permet de mettre en évidence et d'exploiter des propriétés de la divisibilité des nombres entiers et elle est utilisée sous une forme ou une autre depuis l'antiquité. Ces deux deux notations, qui désignent en réalité, une certaine relation d'équivalence, comme nous allons le voir plus bas, sont en réalité construites sur un mode très semblable que nous représentons sur le tableau parallèle ci-après qui va mettre en évidence le rôle que joue un certain sous-groupe dans la définition de ces modulo-égalités.

$\alpha, \beta \in \mathbb{Z}, n \in \mathbb{N}$	$\theta_1, \theta_2 \in \mathbb{R}$
$\alpha \equiv \beta \quad [n]$ α et β ont le même reste dans la division par n $\beta - \alpha$ est un multiple de n $\beta + (-\alpha) \in n\mathbb{Z}$	$\theta_1 \equiv \theta_2 \quad [2\pi]$ θ_1 et θ_2 diffèrent de $2k\pi$, $k \in \mathbb{Z}$ $\theta_1 - \theta_2$ est un multiple de 2π $\theta_1 + (-\theta_2) \in 2\pi\mathbb{Z}$

Ainsi dans le premier cas, nous avons un sous-groupe de $H = n\mathbb{Z}$ du groupe $(\mathbb{Z}, +)$ et la relation $\alpha \equiv \beta \quad [n]$ signifie simplement que $\beta + (-\alpha)$ est un élément de H. Dans le second cas, intervient $H = 2\pi\mathbb{Z}$ qui est un sous-groupe de $(\mathbb{R}, +)$. D'autre part, les conditions $\beta + (-\alpha) \in n\mathbb{Z}$ et $\theta_1 + (-\theta_2) \in 2\pi\mathbb{Z}$ sont de la forme $x^{-1} * y \in H$. Une telle définition s'étend aisément au cas d'un groupe général comme suit.

Soient $(G, *)$ un groupe et H un sous-groupe de G. Nous dirons que deux éléments x et y de G sont en relation R_H et écrivons $x\mathrm{R}_H y$ lorsque $x^{-1} * y \in H$.

E. 28. Dans $(\mathbb{R}, +)$, nous prenons $H = \mathbb{Z}$. Déterminer l'ensemble des réels x tels que $x\mathrm{R}_H x^2$.

THÉORÈME 23. — *La relation* R_H *est une relation d'équivalence sur* G.

Rappelons que dire que R_H est une relation d'équivalence signifie qu'elle satisfait les trois propriétés suivantes.

(i) R_H est **réflexive** $(\forall x \in G,\ x\mathrm{R}_H x)$,

(ii) R_H est **symétrique** $(\forall x, y \in G,\ x\mathrm{R}_H y \Rightarrow y\mathrm{R}_H x)$

(iii) R_H est **transitive** $(\forall x, y, z \in G,\ (x\mathrm{R}_H y \text{ et } y\mathrm{R}_H) \Rightarrow x\mathrm{R}_H z)$.

[TH 23]

Démonstration. Soit $x \in G$. $x \mathrm{R}_H x$ signifie $x^{-1} * x \in H$ or $x^{-1} * x = e_G$ et $e_G \in H$ car $H \leq G$. Cela montre que R_H est réflexive. Ensuite

$$\begin{array}{lll} x \mathrm{R}_H y & \Longrightarrow x^{-1} * y \in H & \text{(par définition de } \mathrm{R}_H\text{)} \\ & \Longrightarrow (x^{-1} * y)^{-1} \in H & \text{(utilise le fait que } H \text{ sous-groupe)} \\ & \Longrightarrow y^{-1} * (x^{-1})^{-1} \in H & \text{(utilise la relation (1.4) p. 9)} \\ & \Longrightarrow y^{-1} * x \in H & \text{(utilise une propriété de l'élément symétrique, voir ii p. 8)} \\ & \Longrightarrow y \mathrm{R}_H x, & \text{(par définition de } \mathrm{R}_H\text{)} \end{array}$$

ce qui montre que R_H est symétrique.

Enfin

$$\begin{array}{lll} \left.\begin{array}{l} x \mathrm{R}_H y \\ y \mathrm{R}_H z \end{array}\right\} & \Longrightarrow \left.\begin{array}{l} x^{-1} * y \in H \\ y^{-1} * z \in H \end{array}\right\} & \text{(par définition de } \mathrm{R}_H\text{)} \\ & \Longrightarrow (x^{-1} * y) * (y^{-1} * z) \in H & \text{(utilise le fait que } H \text{ est un sous-groupe)} \\ & \Longrightarrow x^{-1} * (y * y^{-1}) * z \in H & \text{(utilise l'associativité de la loi } *\text{)} \\ & \Longrightarrow x^{-1} * e_G * z \in H & \text{(utilise la définition de l'élément symétrique)} \\ & \Longrightarrow x^{-1} * z \in H & \text{(utilise la définition de l'élément neutre)} \\ & \Longrightarrow x \mathrm{R}_H z & \text{(par définition de } \mathrm{R}_H\text{)} \end{array}$$

donc R_H est transitive et cela achève la preuve qu'elle est une relation d'équivalence. ■

La **classe d'équivalence** de $x \in G$, notée $\mathbf{cl}(x)$ ou $\overline{x}$ ou $\dot{x}$ est l'ensemble des éléments de G qui sont en relation avec x

$$\mathbf{cl}(x) = \{g \in G : x \,\mathrm{R}_H\, g\}.$$

Il faut toujours bien garder à l'esprit que les classes d'équivalences sont des ensembles.

Si x et x' sont deux éléments de G, il y a seulement deux possibilités

(i) ou bien $x \mathrm{R}_H x'$ auquel cas $\mathbf{cl}(x) = \mathbf{cl}(x')$,

(ii) ou bien $x \neg \mathrm{R}_H x'$ auquel cas $\mathbf{cl}(x) \cap \mathbf{cl}(x') = \emptyset$. Le symbole $\neg$ est employé pour indiquer la négation : $x \neg \mathrm{R}_H x'$ signifie que x n'est pas en relation avec x'.

Autrement dit, deux classes d'équivalence sont des ensemble égaux ou disjoints. En effet, si $x \mathrm{R}_H x'$ et $y \in \mathbf{cl}(x)$ alors

$$\left.\begin{array}{l} x \mathrm{R}_H x' \\ y \mathrm{R}_H x \end{array}\right. \overset{\text{transitivité de } \mathrm{R}_H}{\Longrightarrow} y \mathrm{R}_H x' \Rightarrow y \in \mathbf{cl}(x'),$$

de sorte que $\mathbf{cl}(x) \subset \mathbf{cl}(x')$. Nous montrons de la même manière que $\mathbf{cl}(x') \subset \mathbf{cl}(x)$ d'où $\mathbf{cl}(x) = \mathbf{cl}(x')$.

Réciproquement, si nous supposons que $x \neg \mathrm{R}_H\, x'$ et $\mathbf{cl}(x) \cap \mathbf{cl}(x') \neq \emptyset$ nous obtenons une contradiction puisque

$$y \in \mathbf{cl}(x) \cap \mathbf{cl}(x') \Rightarrow \begin{cases} y\,\mathrm{R}_H\, x \\ y\,\mathrm{R}_H\, x' \end{cases} \overset{\text{transitivité de } \mathrm{R}_H}{\Longrightarrow} x\,\mathrm{R}_H\, x' \quad \text{contradiction !}$$

L'ensemble de toutes les classes d'équivalence est noté G/H et il est appelé le **quotient** de G par H. Lorsque $y \in \mathbf{cl}(x)$, nous disons que y est un **représentant** de $\mathbf{cl}(x)$. L'élément x est un représentant de $\mathbf{cl}(x)$ mais, en général, $\mathbf{cl}(x)$ admet beaucoup d'autres représentants.

Nous utiliserons le fait que G est réunion des classes d'équivalence (distinctes)

$$G = \bigcup_{i \in I} \mathbf{cl}(x_i) \quad \text{avec} \quad \mathbf{cl}(x_i) \cap \mathbf{cl}(x_j) = \emptyset \quad \text{pour} \quad i \neq j. \tag{5.1}$$

Cela signifie que les classes d'équivalence forment une **partition** de G. La formule (5.1) peut être récrite comme

$$G = \bigcup_{A \in G/H} A.$$

5.2 Description des classes d'équivalence

Dans la relation R_H définie ci-dessus nous avons

$$\mathbf{cl}(x) = \{g \in G : x\mathrm{R}_H\, g\} = \{g \in G : x^{-1} * g \in H\} = \{g \in G : g \in x * H\} = x * H$$

où, par définition, $x * H = \{x * h : h \in H\}$. Ces ensembles $x * H$ s'appellent les **classes** (d'équivalence à gauche) définies par le sous-groupe H. La formule (5.1) devient

$$G = \bigcup_{i \in I} (x_i * H) \quad \text{avec } {x_i}^{-1} * x_j \notin H \text{ pour } i \neq j. \tag{5.2}$$

Exemple 3. Lorsque $(G, *) = (\mathbb{Z}, +)$ et $H = 6\mathbb{Z}$,

$$\mathbf{cl}(x) = \overline{x} = x + 6\mathbb{Z} = \{x + 6k : k \in \mathbb{Z}\}.$$

Par exemple,

$$\mathbf{cl}(2) = \mathbf{cl}(8) \qquad \text{car} \quad 2\,\mathrm{R}_H\, 8 \quad (-2) + 8 \in 6\mathbb{Z} \tag{5.3}$$
$$\mathbf{cl}(0) = \mathbf{cl}(-6) \qquad \text{car} \quad 0\,\mathrm{R}_H\, 6 \quad (-0) + (-6) \in 6\mathbb{Z} \tag{5.4}$$
$$\mathbf{cl}(11) = \mathbf{cl}(29) \qquad \text{car} \quad 11\,\mathrm{R}_H\, 29 \quad (-11) + 29 \in 6\mathbb{Z}. \tag{5.5}$$

Ainsi, 8 est un représentant de $\mathbf{cl}(2)$, 11 et 29 sont des représentants de $\mathbf{cl}(5)$. Il est facile de vérifier qu'il y a seulement 6 classes d'équivalences $\mathbf{cl}(0)$, $\mathbf{cl}(1)$, $\mathbf{cl}(2)$, $\mathbf{cl}(3)$, $\mathbf{cl}(4)$, $\mathbf{cl}(5)$ et

$$\mathbb{Z} = \mathbf{cl}(0) \cup \mathbf{cl}(1) \cup \mathbf{cl}(2) \cup \mathbf{cl}(3) \cup \mathbf{cl}(4) \cup \mathbf{cl}(5)$$

où, pour $i = 0, 1, \ldots, 5$. D'une manière générale, si $(G, *) = (\mathbb{Z}, +)$ et $H = m\mathbb{Z}$ ($m \in \mathbb{Z}^*$), il y a m classes d'équivalence

$$\mathbb{Z} = \mathbf{cl}(0) \cup \mathbf{cl}(1) \cup \mathbf{cl}(2) \cdots \cup \mathbf{cl}(m-1)$$

où $\mathbf{cl}(i)$ est l'ensemble des entiers dont le reste dans la division par m est égal à i.

Exemple 4. Lorsque $(G, *) = (\mathbb{R}, +)$ et $H = \mathbb{Z}$,

$$\mathbf{cl}(x) = \{x + k : k \in \mathbb{Z}\} = x + \mathbb{Z}.$$

Par exemple

$$\mathbf{cl}(12/7) = \mathbf{cl}(5/7) \quad \text{car} \quad 12/7 \, \mathrm{R}_H \, 5/7 \quad \text{car} - 12/7 + 5/7 \in \mathbb{Z}.$$

Chaque classe admet un et un seul représentant dans $[0, 1[$. De manière plus précise, l'unique représentant de $x \in \mathbb{R}$ dans $[0, 1[$ est donné par $x - \mathrm{E}(x)$ où E désigne la fonction **partie entière**. Ainsi, $\mathbf{cl}(\pi)$ admet $\pi - 3$ comme représentant. Nous avons donc une bijection entre $\mathbb{R}/\mathbb{Z}$ et $[0, 1[$.

La première application de la relation d'équivalence R_H est données dans le paragraphe suivant. Nous verrons ensuite à la section 6 que, sous réserve que H possède la propriété requise, il possible de définir une loi $\overline{*}$ qui fera de $(G/H, \overline{*})$ un groupe.

5.3 Le théorème de Lagrange

THÉORÈME 24 (Lagrange). — *Soit $(G, *)$ un groupe fini et H un sous-groupe de G. Le cardinal de H divise le cardinal de G, autrement dit $o(H) | o(G)$.*

Démonstration. Considérons la relation d'équivalence R_H qui donne une partition de G de la forme

$$G = \bigcup_{i \in I} \mathbf{cl}(x_i).$$

Ici, puisque G est fini, I et, pour chaque $i \in I$, $\mathbf{cl}(x_i)$ sont aussi des ensembles finis. Nous avons alors

$$\mathrm{card}(G) = \sum_{i \in I} \mathrm{card}(\mathbf{cl}(x_i)) \tag{5.6}$$

car les classes sont des ensembles deux à deux disjoints ($\mathbf{cl}(x_i) \cap \mathbf{cl}(x_j) = \emptyset$ dès que $i \neq j$). Maintenant, nous savons depuis le paragraphe précédent, que $\mathbf{cl}(x_i) = x_i * H$.

Nous allons voir que cela implique que $\text{card}(\mathbf{cl}(x_i)) = \text{card}(H)$. Pour démontrer cette égalité, considèrons l'application

$$\phi : \begin{array}{ccc} H & \to & x_i * H \\ h & \mapsto & x_i * h \end{array}$$

et montrons qu'elle est bijective. La bijectivité impliquera que les ensembles de départ et d'arrivée sont de même cardinal. D'abord, ϕ est surjective par définition de l'ensemble $x_i * H$. Elle est aussi injective. En effet $\phi(h_1) = \phi(h_2) \Rightarrow x_1 * h_1 = x_2 * h_2 \Rightarrow (x_i)^{-1} * (x_i * h_1) = (x_i)^{-1} * (x_i * h_2) \Rightarrow h_1 = h_2$. Reportant $\text{card}(\mathbf{cl}(x_i)) = \text{card}(H)$ dans (5.6) Nous obtenons

$$\text{card}(G) = \sum_{i \in I} \text{card}(H) = \text{card}(H) \times \sum_{i \in I} 1 = \text{card}(H) \times \text{card}(I) \tag{5.7}$$

d'où il résulte $\text{card}(H) \,|\, \text{card}(G)$ i.e. $o(H) \,|\, o(H)$. ■

s: p. 104 E. 29. L'application $h \mapsto x_i * h$ utilisée dans la démonstration est-elle un morphisme ? s:14

Nous avons démontré davantage que ce qu'annonce le théorème. En effet dans (5.7), $\text{card}(I)$ est le nombre de classes d'équivalence c'est-à-dire le cardinal du quotient G/H. La démonstration précédente établissait donc le théorème suivant.

THÉORÈME 25. — *Sous les mêmes hypothèses, nous avons*

$$\text{card}(G) = \text{card}(G/H) \times \text{card}(H). \tag{5.8}$$

Le nombre $\text{card}(G/H)$ s'appelle l'**indice** de H dans G.

THÉORÈME 26. — *Dans un groupe fini, l'ordre de tout élément divise l'ordre du groupe.* $[\forall x \in G, o(x) \mid |G|]$

Démonstration. Nous savons d'après le Théorème 20 (et la remarque qui le suit) que $o(x)$ est égal au cardinal du groupe engendré par x i.e. $o(x) = \text{card}(\langle x \rangle)$. En appliquant le théorème de Lagrange avec $H = \langle x \rangle$, nous obtenons que $o(x) \,|\, o(G)$. ■

COROLLAIRE 27. — *Soit $(G, \cdot)$ un groupe fini. Nous avons*

$$g^{|G|} = e_G, \quad g \in G.$$

Démonstration. En effet, d'après le théorème précédent, il existe un entier k tel que $|G| = k\,o(g)$ de sorte que $e_G = g^{o(g)} \implies e_G = e_G^k = (g^{(o(g)})^k = g^{|G|}$. ■

Exemple 5. Le tableau ci-dessous donne l'ordre de tous les éléments de $\mathbf{U}_8 = \{g_k : k = 0, \ldots, 7\}$ avec $g_k = \exp(2ik\pi/8)$.

ordre	1	2	4	8
éléments	$g_0\ (=1)$	$g_4\ (=-1)$	$g_2 (=i)$ et $g_6 (=-i)$	g_1, g_3, g_5, g_7

Nous apprendrons plus loin comment caractériser tous les éléments d'ordre 8 c'est-à-dire tous les éléments qui engendrent le groupe (voir 7).

s: p. 104 E. 30. Présenter dans un tableau les ordres des éléments de $\mathbf{U}_6$. s:15

5.4 Application à la recherche des sous-groupes

Le théorème de Lagrange et ses corollaires peuvent suffire à déterminer tous les sous-groupes d'un groupe fini de cardinal très petit.

Soit $(G,*)$ un groupe fini contenant p éléments avec p premier (>1). D'après le second corollaire, si $x \in G$ alors $o(x) \,|\, o(G)$ c'est-à-dire ici $o(x) \,|\, p$. Puisque p est premier, nécessairement $o(x) = 1$ ou $o(x) = p$. Dans le premier cas $x = e$ et, dans le second, $\langle x \rangle$ est un sous-groupe de G qui contient le même nombre d'élément que G en sorte que $\langle x \rangle = G$. Nous avons démontré démontré le

THÉORÈME 28. — *Tout groupe d'ordre premier $p > 1$ est cyclique et il est engendré par n'importe lequel de ses éléments différents du neutre.* $[\forall x \in G/\{e\},\ G = \langle x \rangle]$

En particulier, un groupe fini d'ordre premier n'admet aucun sous-groupe propre.

E. 31. Soient p et q deux nombres premiers. Déterminer tous les sous-groupes de $\mathbf{U}_p \times \mathbf{U}_q$.

§ 6. GROUPES QUOTIENTS

6.1 Sous-groupes distingués

Nous savons que les congruences arithmétiques peuvent s'additionner terme a terme. Des relations $15 \equiv 27\ [6]$ et $19 \equiv 37\ [6]$ nous pouvons tirer $34 \equiv 64\ [6]$. Les congruences peuvent aussi se multiplier et ce sont ces deux propriétés qui permettent l'application de la théorie des congruences à tant de problèmes d'arithmétiques [*]. De la même manière, la possibilité d'additionner terme à terme des égalités modulo 2π est essentielle pour calculer les composées de rotation, pour obtenir par exemple qu'une rotation de centre l'origine et d'angle $2\pi/3$ avec une rotation de même centre et d'angle $13\pi/7$ donne une rotation d'angle $11\pi/21$. Puisque nous avons construit la relation R_H par analogie avec les congruences arithmétiques et de mesure d'angle, il est naturel d'espérer la même propriété : la possibilité de $*$-multiplier terme à terme les expressions de la forme $x\mathrm{R}_H y$. Malheureusement, dans le cas général une telle propriété ne demeure pas. Pour qu'elle soit satisfaite, le sous-groupe H, à partir duquel nous construisons la relation R_H doit vérifier la propriété d'être distingué que nous allons définir et étudier à présent. Cette propriété nous permettra ensuite de construire une structure de groupe sur l'ensemble des classes pour parvenir au calcul des classes que nous avons évoqué plus haut.

Soit $(G,*)$ un groupe et H un sous-groupe de G. Nous disons que H est **distingué** dans G (ou **normal** dans G, ou encore **invariant**) s'il vérifie la propriété suivante

$$\forall x \in G \quad x^{-1} * H * x \subset H, \tag{6.1}$$

*. La force de ces deux propriétés apparaîtra dans le chapitre sur la théorie des anneaux dans lequel elles seront efficacement traduites et exploitées.

c'est-à-dire $\forall x \in G, \forall h \in H, x^{-1} * h * x \in H$. L'élément $x^{-1} * h * x$ s'appelle le **conjugué** de h par x. Un sous-groupe H de G est distingué si les conjugués de ses éléments appartiennent encore à H. Certains disent que H est *fermé* pour la conjugaison. En réalité la condition (6.1) est équivalente à

$$\forall x \in G \quad x^{-1} * H * x = H, \tag{6.2}$$

qui est en apparence plus forte. Pour le vérifier, prenons un élément x_0 quelconque de G et appliquons (6.1) avec $x = x_0$ puis avec $x = x_0^{-1}$, il vient

$$x_0^{-1} * H * x_0 \subset H \tag{6.3}$$
$$x_0 * H * x_0^{-1} \subset H. \tag{6.4}$$

En multipliant à droite par x_0^{-1} et à gauche par x_0, la formule (6.4) devient

$$x_0^{-1} * (x_0 * H * x_0^{-1}) * x_0 \subset x_0^{-1} * H * x_0 \Rightarrow H \subset x_0^{-1} * H * x_0. \tag{6.5}$$

De (6.3) et (6.5) nous tirons $x_0^{-1} * H * x_0 = H$. Le même raisonnement étant valide avec n'importe quel $x_0 \in G$, nous obtenons l'égalité (6.2).

La notation $H \triangleleft G$ signifie que H est un sous-groupe distingué de G, différent de G lui-même. Lorsqu'il n'est pas n'exclu que H soit égal à G, nous écrivons $H \trianglelefteq G$

Lorsqu'il n'y a pas de confusion possible sur le groupe G, nous disons simplement que H est distingué. Lorsque H est à la fois sous-groupe de G_1 et de G_2, il faut préciser car H peut être distingué dans G_1 et ne pas l'être dans G_2 comme le montre l'exercice 32.

6.2 Exemples de sous-groupes distingués

(6.2.1) Si $(G,*)$ est abélien alors n'importe lequel de ses sous-groupes est distingué dans G.

E. 32. Montrer que le groupe $\{g^k : k = 0,\dots,n-1\}$ où g est la rotation de centre A et d'angle $2\pi/n$, $g = \mathscr{R}_A(2\pi/n)$, est un sous-groupe distingué du groupe $\mathscr{R}_A$ des rotations de centre A. Montrer par contre que ce n'est pas un sous-groupe distingué du groupe des isométries $\mathbf{Is}(P)$.
s: p. 104 On pourra considérer $t_u \circ g \circ t_{-u}$. [s:16]

(6.2.2) Si φ est un morphisme de $(G,*)$ dans $(T,\circ)$ alors $\ker\varphi$ est un sous-groupe distingué de G. [$\ker\varphi \trianglelefteq G$.]

Démonstration. Prenons $h \in \ker\phi$ et $x \in G$. Nous devons montrer que $x^{-1} * h * x \in \ker\phi$ c'est-à-dire que $\phi(x^{-1} * h * x) = e_T$. Or

$$\begin{aligned} \phi(x^{-1} * h * x) &= \phi(x)^{-1} * \phi(h) * \phi(x) && \text{(utilise le fait que } \phi \text{ est un morphisme et ses conséquences)} \\ &= \phi(x)^{-1} * \phi(h) * \phi(x) && \text{(car } h \in \ker\phi\text{)} \\ &= e_T. \end{aligned}$$

■

(6.2.3) Soit $H = \{\lambda Id : \lambda \in \mathbb{R}^\star\}$ où Id est la matrice identité dans $\mathbf{GL}_n(\mathbb{R})$. Alors $H \trianglelefteq \mathbf{GL}_n(\mathbb{R})$.[s:17] s: p. 104

6.3 Compatibilité de R_H avec la loi de G lorsque $H \trianglelefteq G$.

Soit $(G,*)$ un groupe et $H \trianglelefteq G$. La relation d'équivalence R_H définie par le sous-groupe distingué H a la propriété remarquable d'être **compatible** avec la loi. Cela signifie que, pour $g_1, g_2, r_1, r_2 \in G$,

$$\left.\begin{array}{l} g_1 \,\mathrm{R}_H\, g_2 \\ r_1 \,\mathrm{R}_H\, r_2 \end{array}\right\} \Rightarrow (g_1 * r_1)\ \mathrm{R}_H\ (g_2 * r_2).$$

En effet, $g_1 \,\mathrm{R}_H\, g_2 \Rightarrow g_1^{-1} * g_2 \in H \Rightarrow g_1^{-1} = h * g_2^{-1}$ pour un certain $h \in H$. De même $r_1 \,\mathrm{R}_H\, r_2 \Rightarrow r_1^{-1} = h' * r_2^{-1}$ pour un certain $h' \in H$. Ensuite,

$$\begin{array}{rl} (g_1 * r_1)^{-1} * (g_2 * r_2) & = r_1^{-1} * g_1^{-1} * g_2 * r_2 \\ & = (h' * r_2^{-1}) * (h * g_2^{-1}) * g_2 * r_2 \\ & = h' * r_2^{-1} * h * r_2 \\ & = h' * (\text{un élément de } H) \qquad (\text{car } H \text{ est distingué}). \end{array}$$

Étant le produit de deux éléments du sous-groupe H, $(g_1 * r_1)^{-1} * (g_2 * r_2)$ appartient aussi à H et cela montre que $g_1 * r_1 \,\mathrm{R}_H\, g_2 * r_2$.

Il n'est pas difficile de vérifier que, réciproquement, toutes les relations d'équivalence sur G qui sont compatibles avec la loi de G sont de la forme $\mathsf{R} = \mathsf{R}_H$ avec $H \trianglelefteq G$, voir l'exercice 59.

6.4 Structure du quotient

Soit $(G,*)$ un groupe et H un sous-groupe distingué de G. Rappelons que G/H désigne l'ensemble des classes d'équivalence de R_H. Nous pouvons définir une loi $\overline{*}$ sur G/H comme suit

$$\begin{array}{rccl} \overline{*}\ : & G/H \times G/H & \longrightarrow & G/H \\ & (\mathtt{C}_1\,,\,\mathtt{C}_2) & \longmapsto & \mathbf{cl}\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_1\end{array} * \begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_2\end{array}\right) \end{array} \tag{6.6}$$

Cette définition présente une difficulté évidente. L'élément $\mathtt{C}_1 * \mathtt{C}_2$ doit avoir une valeur et une seule alors que, à priori, la définition ci-dessus lui en attribue $\mathrm{card}(\mathtt{C}_1) \times \mathrm{card}(\mathtt{C}_2)$. Le nombre $\mathrm{card}(\mathtt{C}_1)$ correspond au nombre de choix possibles pour le représentant de $\mathtt{C}_1$ et $\mathrm{card}(\mathtt{C}_2)$ au nombre de choix possibles pour le représentant de $\mathtt{C}_2$. Pour que notre définition soit acceptable — nous disons, **consistante** — nous devons montrer qu'en réalité le choix des représentants n'influe en rien sur la valeur trouvée. Autrement dit, nous devons vérifier que

$$\left.\begin{array}{rcl} x_1, x_1' & \in & \mathtt{C}_1 \\ x_2, x_2' & \in & \mathtt{C}_2 \end{array}\right\} \Rightarrow \mathbf{cl}(x_1 * x_2) = \mathbf{cl}(x_1' * x_2').$$

Il en est bien ainsi. En effet, en utilisant la compatibilité pour la deuxième implication,

$$\left.\begin{array}{l} x_1, x_1' \in \mathtt{C}_1 \\ x_2, x_2' \in \mathtt{C}_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{ll} x_1 \mathsf{R}_H x_1' & \\ x_2 \mathsf{R}_H x_2' & \end{array}\right. \begin{array}{ll} \Rightarrow & (x_1 * x_2)\, \mathsf{R}_H (x_1' * x_2') \\ \Rightarrow & \mathbf{cl}(x_1 * x_2) = \mathbf{cl}(x_1' * x_2'). \end{array}$$

La loi $\overline{*}$ est par conséquent bien définie et c'est une loi interne sur G/H.

Remarquons que nous avons toujours

$$\mathbf{cl}(x_1) \overline{*} \mathbf{cl}(x_2) = \mathbf{cl}(x_1 * x_2), \quad x_2, x_2 \in G. \tag{6.7}$$

C'est une conséquence de la définition dans laquelle $\mathtt{C}_1 = \mathbf{cl}(x_1)$, $\mathtt{C}_2 = \mathbf{cl}(x_2)$ et dans laquelle nous choisissons x_1 comme représentant de $\mathtt{C}_1$ et x_2 comme représentant de $\mathtt{C}_2$. En particulier, *si x_1 est représentant de $\mathtt{C}_1$ et x_2 est représentant de $\mathtt{C}_2$ alors $x_2 * x_2$ est représentant de $\mathtt{C}_1 \overline{*} \mathtt{C}_2$.*

THÉORÈME 29. — *Soit $(G,*)$ un groupe et $H \trianglelefteq G$, $(G/H, \overline{*})$ est un groupe.*

Démonstration. Nous avons déjà vu que $\overline{*}$ est une loi interne. L'associativité provient immédiatement de celle de $*$. En effet, si $\mathtt{C}_1, \mathtt{C}_2$ et $\mathtt{C}_3$ sont trois éléments de G/H de représentants respectifs x_2, x_2 et x_3, nous avons $(\mathtt{C}_1 \overline{*} \mathtt{C}_2) \overline{*} \mathtt{C}_3 = \mathbf{cl}(x_1 * x_2) \overline{*} \mathbf{cl}(x_3) = \mathbf{cl}((x_1 * x_2) * x_3) = \mathbf{cl}(x_1 * (x_2 * x_3)) = \mathbf{cl}(x_1) \overline{*} \mathbf{cl}(x_2 * x_3) = \mathtt{C}_1 \overline{*} (\mathtt{C}_2 \overline{*} \mathtt{C}_3)$.

Montrons que $\mathbf{cl}(e)$ est élément neutre pour $\overline{*}$. Soient $\mathtt{C} \in G/H$ et x un représentant de $\mathtt{C}$. Nous avons

$$\mathtt{C} \overline{*} \mathbf{cl}(e) = \mathbf{cl}(x) \overline{*} \mathbf{cl}(e) = \mathbf{cl}(x * e) = \mathbf{cl}(x) = \mathtt{C}.$$

Nous montrons de même que $\mathbf{cl}(e) \overline{*} \mathtt{C} = \mathtt{C}$ et cela prouve que $\mathbf{cl}(e)$ est élément neutre de $\overline{*}$. Il reste à établir que tout élément de G/H admet un élément symétrique pour $\overline{*}$. Prenons $\mathtt{C}_1 \in G/H$ et x un représentant de $\mathtt{C}_1$ et posons $\mathtt{C}_2 = \mathbf{cl}(x^{-1})$. Nous avons

$$\mathtt{C}_1 \overline{*} \mathtt{C}_2 = \mathbf{cl}(x) \overline{*} \mathbf{cl}(x^{-1}) = \mathbf{cl}(x * x^{-1}) = \mathbf{cl}(e) = \text{neutre de } \overline{*}.$$

On montre de même que $\mathtt{C}_2 \overline{*} \mathtt{C}_1 = \mathbf{cl}(e)$ ce qui prouve que $\mathtt{C}_2$ est élément symétrique de $\mathtt{C}_1$ et cela conclut la démonstration que G/H est un groupe. ■

Nous retiendrons que

$$e_{G/H} = \mathbf{cl}(e_G)$$

et

$$[\mathbf{cl}(x)]^{-1} = \mathbf{cl}(x^{-1}) \qquad (x \in G).$$

De manière générale,

$$\mathbf{cl}(x^m) = [\mathbf{cl}(x)]^m \qquad x \in G,\ m \in \mathbb{Z}.$$

THÉORÈME 30. — *Soit $(G,*)$ un groupe et $H \trianglelefteq G$. L'application s définie par*

$$s : \begin{array}{ccc} (G,*) & \longrightarrow & (G/H, \overline{*}) \\ x & \longmapsto & \mathbf{cl}(x). \end{array}$$

est un morphisme de groupe ; il est surjectif et son noyau est égal à H.

Démonstration. Notons d'abord que s est surjective par définition des classes : toute classe $\mathtt{C} \in G/H$ admet au moins un représentant i.e. $\mathtt{C} = \mathbf{cl}(x) = s(x)$. Montrons que s est un morphisme. Pour $x, y \in G$, $s(x*y) = \mathbf{cl}(x*y) = \mathbf{cl}(x) * \mathbf{cl}(y) = s(x) * s(y)$. Enfin, $x \in \ker s \iff s(x) = e_{G/H} = \mathbf{cl}(e) \iff \mathbf{cl}(x) = \mathbf{cl}(e) \iff e \,\mathsf{R}_H\, x \iff x \in H$ et cela prouve $\ker s = H$. ■

Le morphisme s s'appelle la **surjection canonique** (ou **projection canonique**) de G sur G/H. Elle est souvent notée s_H.

6.5 Le groupe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^\star$. Puisque $(\mathbb{Z}, +)$ est un groupe commutatif tous ses sous-groupes sont distingués et $n\mathbb{Z} < \mathbb{Z}$. Le groupe $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ est un groupe commutatif d'ordre n

$$\mathbb{Z}/n\mathbb{Z} = \{\mathbf{cl}(0), \mathbf{cl}(l), ..., \mathbf{cl}(n-l)\}.$$

Nous écrirons $\mathbf{cl}(i) = \overline{i}$. Pour simplifier nous écrirons souvent $\mathbb{Z}_n$ à la place $\mathbb{Z}/n\mathbb{Z}$. Formons par exemple la table de $\mathbb{Z}_5$.

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$

(Calculs bruts)

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

(Calculs simplifiés)

Les termes neutres ($\overline{0}$) permettent d'identifier les symétriques de chaque élément. Par exemple, le symétrique de $\overline{1}$ est $\overline{4}$ i.e. $= \overline{4} = \overline{-1}$.

La relation $-\overline{1} = \overline{-1}$ est un cas particulier de la relation $[\mathbf{cl}(x)]^{-1} = \mathbf{cl}(x^{-1})$. D'une manière générale dans $\mathbb{Z}_n$, nous avons toujours $-\overline{k} = \overline{-k}$, et nous pouvons intervertir les symboles $-$ et $\bar{\cdot}$.

Le groupe $(\mathbb{Z}_n, \overline{+})$ est cyclique, engendré par l'élément $\overline{1}$. En effet

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{1}+\overline{1}, \ldots, \underbrace{\overline{1+\cdots+1}}_{n-1 \text{ fois}}) = \langle \overline{1} \rangle .$$

En général, un élément quelconque (non nul) n'engendre pas $\mathbb{Z}_n$. Par exemple, dans $\mathbb{Z}_6$, $\langle\overline{3}\rangle = \{\overline{0},\overline{3}\}$ et $\langle\overline{2}\rangle = \{\overline{0},\overline{2},\overline{4}\}$. Le théorème suivant donne une condition nécessaire et suffisante pour qu'un élément donné engendre $\mathbb{Z}_n$.

THÉORÈME 31. — *Soit $n>1$ et $a\in\mathbb{N}$. Pour que $\overline{a}=\mathbf{cl}(a)$ engendre $\mathbb{Z}_n$ (i.e. $\mathbb{Z}_n=\langle\overline{a}\rangle$) il faut et il suffit que a et n soient premiers entre eux.*

Le lecteur attentif aura remarqué une imprécision dans cet énoncé. En effet, nous cherchons une condition sur $\overline{a}$ mais donnons une réponse faisant intervenir a, c'est-à-dire un représentant de la classe $\overline{a}$ plutôt que la classe elle-même. Pour que l'énoncé soit cohérent il faut que cette condition ne dépendent pas du représentant choisi de $\overline{a}$, autrement dit qu'elle soit vraie pour tous les entiers μ de la forme $\mu=a+kn$ (ou bien pour aucun entier de cette même forme). C'est évidemment le cas puisque $a+kn$ sera premier avec n si et seulement si a est premier avec n.

E. 33. Modifier la formulation du théorème en sorte que la remarque précédente ne soit plus nécessaire. s: p. 105 s:1

Démonstration du théorème 31.

Étape 1. Nous montrons que la condition est nécessaire.

Supposons que $\mathbb{Z}_n$ soit engendré par $\overline{a}$. Puisque

$$n=\mathrm{card}(\mathbb{Z}_n)=\mathrm{card}(\langle\overline{a}\rangle),$$

nous avons $o(\overline{a})=n$ et

$$\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{a},\overline{a}+\overline{a},\ldots,\underbrace{\overline{a}+\overline{a}+\cdots+\overline{a}}_{n-1\text{ fois}}\}=\{\overline{0},\overline{a},\overline{2a},\ldots,\overline{(n-1)a}\}.$$

Il existe donc $i\in\{1,\ldots,n-l\}$ tel que $\overline{ia}=\overline{1}$ (le cas $i=0$ ne peut jamais se produire), soit encore $ia=1+kn$ avec $k\in\mathbb{Z}$ ce qui implique que $ia-kn=1$ et, par le théorème 6 de Bézout, que a et n sont premiers entre eux.

Étape 2. Nous montrons que la condition est suffisante

Réciproquement, si a et n sont premiers entre eux alors, toujours par le théorème 6 de Bézout, il existe des entiers u et v dans $\mathbb{Z}$ tels que $au+nv=1$. En effectuant une division euclidienne de u par n, nous obtenons une écriture $u=qn+r$ avec $r\in\{0,\ldots,n-1\}$ et la relation $au+nv=1$ devient

$$a(qn+r)+nv=1 \iff ar+(aq+v)n=1$$

qui implique $\overline{ar}=\overline{1}$ puis

$$\underbrace{\overline{a}+\overline{a}+\cdots+\overline{a}}_{r\text{ fois}}=\overline{1} \implies \overline{1}\subset\langle\overline{a}\rangle \implies \langle\overline{1}\rangle\subset\langle\overline{a}\rangle$$

et donc puisque $\langle\overline{1}\rangle=\mathbb{Z}_n$, nous avons $\mathbb{Z}_n\subset\langle\overline{a}\rangle$. Comme l'inclusion inverse est évidente nous en déduisons $\mathbb{Z}_n=\langle\overline{a}\rangle$. ■

6.6 Théorème d'isomorphisme

THÉORÈME 32. — *Soient G_1 et G_2 deux groupes*[*] *et ϕ un homomorphisme de G_1 dans G_2. Il existe un* isomorphisme γ *de $G_1/\ker\phi$ sur $\phi(G_1)$ tel que $\phi = \gamma \circ s$ où s est la surjection canonique de G_1 sur $G_1/\ker\phi$. Nous avons donc*

$$G_1/\ker\phi \simeq \phi(G_1).$$

Le théorème dit essentiellement que les projections canoniques permettent de *factoriser* les morphismes de groupes par la projection canonique et un isomorphisme. La figure 1 schématise cette propriété.

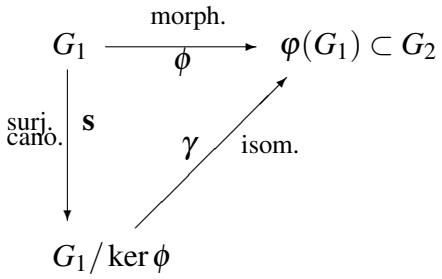


FIGURE 1 – Schéma du théorème d'isomorphisme $\phi = \gamma \circ \mathbf{s}$

Démonstration. Nous définirons γ comme suit

$$\gamma : \begin{array}{ccc} G_1/\ker\phi & \longrightarrow & \phi(G_1) \subset G_2 \\ \mathtt{C} & \longmapsto & \phi\left(\begin{array}{l}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}\end{array}\right). \end{array}$$

Vérifions d'abord que cette définition est consistante c'est-à-dire que nous pouvons effectivement utiliser n'importe quel représentant de $\mathtt{C}$ sans modifier le résultat. Prenons deux représentants x_l et x_2 de $\mathtt{C}$. Nous avons $x_1 \,\mathsf{R}_{\ker\phi}\, x_2$ i.e. $x_1^{-1} * x_2 \in \ker\phi \implies x_2 = x_1 * h$ avec $h \in \ker\phi$ d'où $\phi(x_2) = \phi(x_1 * h) = \phi(x_1) * \phi(h) = \phi(x_1)$ car $h \in \ker\phi$. Deux représentants quelconques de $\mathtt{C}$ donnent le même résultat et notre définition de s est consistante. L'application γ vérifie $\gamma(\mathbf{cl}(x)) = \phi(x)$ car x est représentant de $\mathbf{cl}(x)$. Ceci montre que tous les éléments de $\phi(G_1)$ (et seulement ceux-là) sont dans l'ensemble image de γ qui est par conséquent une surjection de $G_1/\ker\phi$ sur $\phi(G_1)$.

Montrons que γ est un morphisme. Prenons $\mathtt{C}_1$ et $\mathtt{C}_2$ deux éléments de $G_1/\ker\phi$ et x_1 un représentant de $\mathtt{C}_1$, x_2 un représentant de $\mathtt{C}_2$. Nous avons

∗. Les lois (différentes) des groupes G_1 et G_2 seront ici représentées par le même symbole $*$.

$$\begin{aligned}
\gamma(\mathtt{C}_1 \overline{*} \mathtt{C}_2) &= \phi\left(\begin{array}{l}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_1 \overline{*} \mathtt{C}_2\end{array}\right) \\
&= \phi(x_1 * x_2) && \text{(car } x_1 * x_2 \text{ est un représentant de } \mathtt{C}_1 \overline{*} \mathtt{C}_2\text{)} \\
&= \phi(x_1) * \phi(x_2) \\
&= \gamma(\mathbf{cl}(x_1)) * \gamma(\mathbf{cl}(x_2)) \\
&= \gamma(\mathtt{C}_1) \overline{*} \gamma(\mathtt{C}_2)
\end{aligned}$$

$$\begin{aligned}
\mathtt{C} \in \ker\gamma &\Longrightarrow \gamma(\mathtt{C}) = e_{G_2} \\
&\Longrightarrow \phi(x) = e_{G_2} && \text{(où } x \text{ est un représentant quelconque de } \mathtt{C}\text{)} \\
&\Longrightarrow x \in \ker\phi \\
&\Longrightarrow e_{G_1} \mathrel{R_{\ker\phi}} x \\
&\Longrightarrow \mathbf{cl}(x) = \mathbf{cl}(e_{G_1}) \\
&\Longrightarrow \mathtt{C} = \text{neutre de } G_1/\ker\phi.
\end{aligned}$$

Ceci montre que $\ker\gamma = \{e_{G/\ker\phi}\}$ donc que γ est injective. Nous avons ainsi établi que γ est un isomorphisme de $G/\ker\phi$ sur $\phi(G_1)$. Il reste à vérifier que $\phi = \gamma \circ s$. C'est immédiat car, pour $x \in G_1$, $\gamma(s(x)) = \gamma(\mathbf{cl}(x)) = \phi(x)$. ■

6.7 Exemples d'application du théorème d'isomorphisme

(6.7.1) Considérons le morphisme

$$\exp : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbf{U},\cdot)\\ x & \longmapsto & \exp(ix)\end{array}$$

Nous avons vu (3.6) que $\ker\exp = 2\pi\mathbb{Z} = \{2k\pi : k \in \mathbb{Z}\}$. De plus exp est surjective car tout nombre complexe z de $\mathbf{U}$ s'écrit $z = \exp i\theta$ avec $\theta \in \mathbb{R}$. (Cette propriété est loin d'être évidente. Elle se démontre en analyse par une étude fine de la série définissant la fonction exponentielle.) Nous avons donc $\exp(\mathbb{R}) = \mathbf{U}$. Le théorème d'isomorphisme donne $\mathbb{R}/2\pi\mathbb{Z} \simeq \exp(\mathbb{R})$, soit

$$\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbf{U}.$$

s: p. 104 E. 34. Soit $a \in \mathbb{R}^{\star+}$. Montrer que $\mathbb{R}/a\mathbb{Z} \simeq \mathbf{U}$. [s:18]

(6.7.2) Considérons le morphisme

$$\det : \begin{array}{ccc}(\mathbf{GL}_n(\mathbb{K}),\cdot) & \longrightarrow & (\mathbb{K}^\star,\cdot)\\ A & \longmapsto & \det A\end{array}$$

Nous avons vu (3.6) que $\ker\det = \mathbf{SL}_n(\mathbb{K})$ et det est surjectif — $\forall\lambda \in \mathbb{K}^\star$, $\exists A \in \mathbf{GL}_n(\mathbb{K})$ tel que $\det(A) = \lambda$ (prendre A avec $A_{11} = \lambda$ puis tous les autres éléments de la diagonale

égaux à 1, puis tous les éléments restant nuls) — donc $\det(\mathbf{GL}_n(\mathbb{K})) = \mathbb{K}^\star$. Le théorème d'isomorphisme donne

$$\mathbf{GL}_n(\mathbb{K})/\ker\det \simeq \det(\mathbf{GL}_n(\mathbb{K})),$$

c'est-à-dire

$$\mathbf{GL}_n(\mathbb{K})/\mathbf{SL}_n(\mathbb{K}) \simeq \mathbb{K}^\star.$$

(6.7.3) Soit $(G,*)$ un groupe cyclique d'ordre n i.e. $G = \langle a\rangle$ avec $o(a) = n$ de sorte que $G = \{e, a, a^2, ..., a^{n-1}\}$. Considérons le morphisme

$$p_a : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & a^m. \end{array}$$

Nous savons que p_a est surjectif (parce que a est générateur de G) et avons déjà vu dans (3.6) que $\ker p_a = n\mathbb{Z}$ de sorte que le théorème d'isomorphisme donne $\mathbb{Z}/\ker p_a \simeq p_a(G)$ soit

$$\mathbb{Z}/n\mathbb{Z} \simeq G.$$

Nous avons démontré le théorème suivant

THÉORÈME 33. — *Tout groupe cyclique fini d'ordre n est isomorphe à $(\mathbb{Z}_n, \overline{+})$.*

En particulier $\mathbf{U}_n \simeq \mathbb{Z}_n$. Nous disons qu'*à isomorphisme près*, il existe un seul groupe cyclique d'ordre $n \geq 1$ donné. Tous les théorème valables pour $\mathbb{Z}_n$ ont un pendant immédiat pour n'importe quel sous-groupe cyclique.Cela sera expliqué en détail dans la section suivante.

E. 35. Soit G_2 et G_2 deux groupes isomorphes et ϕ un isomorphisme de G_1 sur G_2. On suppose que $H \trianglelefteq G_1$. Montrer que $\phi(H) \trianglelefteq G_2$ et

$$G_1/H \simeq G_2/\phi(H).$$

§ 7. LES GROUPES ISOMORPHES

Lorsque $(G,*)$ et $(W,\cdot)$ sont deux groupes isomorphes, toutes les propriétés de groupe que possède le premier à un pendant immédiat chez l'autre. Le tableau ci-dessus donne quelques unes de ces correspondances.

Sur G	Sur W	Description de la correspondance induite par l'isomorphisme $\Psi : G \to W$
$z * g^{-1} = x * y$	$\Psi(z) \cdot \Psi(g)^{-1} = \Psi(x) \cdot \Psi(y)$	Une relation liant n éléments dans un groupe implique une relation liant les images de ces n éléments dans l'autre groupe. (Dans l'exemple ci-contre $n = 4$.)
$o(x) = n$	$o(\Psi(x)) = n$	L'ordre d'un élément du premier groupe est égal à l'ordre de son image dans le second groupe.
$H < G$	$\Psi(H) < \Psi(G)$	Un ensemble est sous-groupe du premier groupe si son image dans le second est un sous-groupe.
$G = \langle X \rangle$	$W = \langle \Psi(X) \rangle$	A toute partie génératrice du premier groupe correspond une partie génératrice du second groupe.
$\mathsf{Aut}(G)$	$\mathsf{Aut}(W) = \{\Psi \circ f \circ \Psi^{-1} : f \in \mathsf{Aut}(G)\}$	Chaque automorphisme du second groupe se déduit d'un automorphisme du premier par conjugaison par Ψ et nous avons $\mathsf{Aut}(G) \simeq \mathsf{Aut}(W)$.
$\mathsf{End}(G)$	$\mathsf{End}(W) = \{\Psi \circ f \circ \Psi^{-1} : f \in \mathsf{End}(G)\}$	Chaque endomorphisme du second groupe se déduit d'un endomorphisme du premier par conjugaison par Ψ et nous avons $\mathsf{End}(G) \simeq \mathsf{End}(W)$.

Deux groupes isomorphes sont comme deux exemplaires d'un même livre. Nous pouvons déduire le contenu du premier de celui du second et vice versa. Voyons un exemple. Nous avons établi plus haut que pour qu'un élément $\overline{k}$ soit un générateur du groupe cyclique $(\mathbb{Z}_n, \overline{+})$, il faut et il suffit que k soit premier avec n. Nous savons aussi que tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$. En particulier, le groupe $\mathbf{U}_n$ est isomorphe à $\mathbb{Z}_n$, un isomorphisme étant donné par $\Psi : \phi^k \in \mathbf{U}_n \to \overline{k} \in \mathbb{Z}_n$ où $\phi = \exp(2i\pi/n)$. Il suit que l'élément $\exp(2i\pi k/n)$ sera un générateur de $\mathbf{U}_n$ si et seulement si $\overline{k}$ est un générateur de $\mathbb{Z}_n$ c'est-à-dire si et seulement si k est premier avec n. Deux groupes isomorphes contiennent exactement la même information (pour ce qui concerne toutes les questions liées à la structure de groupe) et si nous limitons à considérer cette information, nous pouvons les confondre. Nombre d'énoncés de la théorie des groupes ont la forme suivante : *à isomorphisme près, il existe un unique groupe d'ordre p premier* ou encore *à isomorphisme près, il existe seulement deux groupe d'ordre* 4. Les mathématiciens construisent une bibliothèque de groupes et chaque fois qu'un nouveau groupe apparaît, ils cherchent à établir s'il est isomorphe à un groupe déjà connu ou s'exprime, par un produit direct ou une méthode plus sophistiquée, à partir d'autres groupes faisant déjà partie de la bibliothèque. Les éléments les plus simples de cette

bibliothèque sont donnés par les théorèmes 21 et 33 qui fournissent une caractérisation, ou comme on dit souvent en mathématiques, une **classification**, complète des groupes cycliques : à isomorphisme près, il existe un seul groupe cyclique (monogène infini) et un seul groupe d'ordre n, $n \in \mathbb{N}^\star$. Pour ce qui concerne les groupes finis abélien, la classification est connue depuis longtemps (elle sera étudiée plus loin) : tout groupe abélien fini est un produit direct de groupes cycliques et par conséquent isomorphe à un produit direct de groupes $\mathbb{Z}_n$. La question est beaucoup plus compliquée pour les groupes non abéliens.

E. 36. Montrer que si deux groupes sont isomorphes alors il existe une bijection entre l'ensemble formé d'une part des sous-groupes du premier groupe et celui formé des sous-groupes du second.

§ 8. LE GROUPE SYMÉTRIQUE

8.1 Définitions

Soit $\Omega(n) = \{1, 2, \ldots, n\}$. Une bijection de $\Omega(n)$ sur $\Omega(n)$ s'appelle une **permutation**. L'ensemble des permutations de $\Omega(n)$ est noté $\mathbf{S}_n$. Un élément f de $\mathbf{S}_n$ est souvent représenté sous la forme d'un tableau à 2 lignes et n colonnes :

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$$

où la seconde ligne donne les images des éléments correspondant sur la première ligne. $\mathbf{S}_n$ est muni de la loi de composition des applications que nous notons cependant ici par un point $(\cdot)$ plutôt que par $\circ$. Ainsi, si

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \quad \text{et} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 6 & 4 \end{pmatrix}$$

alors nous avons

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 6 & 4 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 & 5 & 6 & 4, \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 & 6 & 5 & 4 \end{matrix}$$

de sorte que

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 5 & 4 \end{pmatrix}.$$

Il faut prendre garde que, comme pour toutes les compositions de fonctions, on commence par l'application sur la droite.

E. 37. Calculer $g \cdot f$.

La loi $\cdot$ admet évidemment l'application identité, que nous noterons ici e plutôt que Id, comme élément neutre et la fonction réciproque de f est l'élément symétrique de f. Par exemple,

$$\text{si } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \text{ alors } f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}.$$

A partir de là, nous vérifions facilement le

THÉORÈME 34. — *$(\mathbf{S}_n, \cdot)$ est un groupe d'ordre $n!$. Il est non commutatif dès que $n > 2$. $(\mathbf{S}_n, \cdot)$ s'appelle le n-ième* ***groupe symétrique***

Pour la non-commutativité lorsque $n \geq 3$, nous pouvons prendre f qui envoie 1 sur 2, 2 sur 3, 3 sur 1 et laisse tous les autres éléments fixes, puis g qui envoie 1 sur 2, 2 sur 1 et laisse tous les autres éléments fixes. Puisque $(f \cdot g)(1) = 3$ et $(g \cdot f)(1) = 1$, nous avons $f \cdot g \neq g \cdot f$.

E. 38. Soient $m > n \geq 1$. Trouvez un morphisme injectif de $\mathbf{S}_n$ dans $\mathbf{S}_m$. En déduire que $\mathbf{S}_n$ est isomorphe à un sous-groupe de $\mathbf{S}_m$ que l'on précisera.

8.2 Cycles

Soit $f \in \mathbf{S}_n$. S'il existe $k \in \{2, \dots n\}$ et $a_1, a_2, \dots, a_k$ dans $\Omega(n)$ tels que

$$\begin{cases} f(a_i) = a_{i+1} & i = 1, \dots, k-1 \\ f(a_k) = a_1 & \\ f(b) = b & b \notin \{a_1, \dots, a_k\} \end{cases},$$

autrement dit, si f est de la forme

$$\begin{pmatrix} \boxed{\text{Id}} & a_1 & \boxed{\text{Id}} & a_2 & \boxed{\text{Id}} & \dots & \boxed{\text{Id}} & a_{k-1} & \boxed{\text{Id}} & a_k \\ & a_2 & & a_3 & & & & a_k & & a_1 \end{pmatrix}$$

alors nous disons que f est un **cycle**, ou, plus précisément un **k-cycle** ou encore un cycle de **longueur** k et nous notons

$$f = (a_1\, a_2 \dots a_k).$$

Les 2-cycles sont appelés **transpositions**.

E. 39. (a) Donner l'écriture sous la forme d'un tableau à deux lignes du cycle $(341) \in \mathbf{S}_6$. (b) Vérifier que la permutation suivante est un cycle et donner son écriture,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 1 & 6 & 6 & 8 & 1 & 2 & 9 \end{pmatrix}.$$

L'ensemble $\{a_1,\dots,a_k\}$ s'appelle le **support** du cycle $(a_1\dots a_k)$. La notation employée pour un cycle comporte une petite perte d'information. Elle ne permet pas de savoir sur quel $\Omega(n)$ nous travaillons. Le cycle (142) peut désigner un élément de $\mathbf{S}_4$ mais aussi bien un élément de tout $\mathbf{S}_n$ pour $n \geq 4$. Il faut aussi prendre garde qu'un même cycle possède plusieurs écritures. Ainsi dans $\mathbf{S}_3$, $(123) = (231) = (312)$. Plus généralement, le cycle $(a_1 a_2 \dots a_k)$ admet $k-1$ autres écritures. Remarquons enfin que cela n'a pas de sens de parler de cycle de longueur un.

E. 40. Dans $\mathbf{S}_5$, calculer, en donnant le résultat sous la forme d'un tableau à deux lignes, $(2431)\cdot(1534)$ puis $(12)\cdot(345)$ puis $(345)\cdot(12)$.

E. 41. Démontrer les propriétés suivantes.

a) Soient $n \geq 2$ et $a_1, a_2 \in \Omega(n)$,

$$(a_1\, a_2) = (1\, a_1)\cdot(1\, a_2)\cdot(1\, a_1).$$

b) Soient $n \geq k$ et a_i, $i = 1,\dots k$, k éléments distincts de $\Omega(n)$,

$$(a_1\, a_2\, a_3\, \dots\, a_k) = (a_1\, a_2)\cdot(a_2\, a_3)\,\dots\,(a_{k-1}\, a_k).$$

THÉORÈME 35. — *Si deux cycles ont des supports disjoints alors ils commutent l'un avec l'autre. De manière précise, si* $\{a_1,\dots,a_k\}\cap\{b_1,\dots,b_r\} = \emptyset$ *alors*

$$(a_1\, a_2\, \dots\, a_k)\cdot(b_1\, b_2\, \dots\, b_r) = (b_1\, b_2\, \dots\, b_r)\cdot(a_1\, a_2\, \dots\, a_k).$$

THÉORÈME 36. — *Si* $f \in \mathbf{S}_n$ *est un* k*-cycle alors* f *est d'ordre* k*.*

Rappelons que dire que f est d'ordre k signifie $f^k = e$ et $f^j \neq e$ pour $j = 1,\dots,k-1$.

Démonstration. Supposons que $f = (a_1 a_2 \dots a_k)$, alors $f(a_1) = a_2$ et

$$f^2(a_1) = f(f(a_1)) = f(a_2) = a_3,$$

et en continuant nous arrivons à $f^{k-1}(a_1) = a_k$ qui montre que $f^j \neq e$ pour $1 < j < k$, par contre $f^k(a_1) = a_1$ et nous vérifions immédiatement le même résultat pour tous les a_i, $f^k(a_i) = a_i$, $i = 1,\dots,k$. Comme pour tout $b \in \Omega(n)\setminus\{a_1,\dots,a_k\}$, nous avons $f(b) = b$ et donc $f^k(b) = b$ il suit que pour tout $i \in \Omega(n)$, $f^k(i) = i$ et cela montre $f^k = e$. ■

8.3 Décomposition en produit de cycles

Les cycles sont des permutations relativement simples dont nous allons voir qu'elles permettent de décrire toutes les permutations. Voyons d'abord un exemple. Prenons

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 5 & 6 & 1 & 4 & 8 & 9 & 7 \end{pmatrix}.$$

Puisque $f(1) = 3$, nous pouvons ré-écrire le tableau comme suit

$$f = \begin{pmatrix} 1 & 2 & f(1) & 4 & 5 & 6 & 7 & 8 & 9 \\ f(1) & 2 & 5 & 6 & 1 & 4 & 8 & 9 & 7 \end{pmatrix}.$$

En notant que $f^2(1) = f(3) = 5$, nous pouvons écrire

$$f = \begin{pmatrix} 1 & 2 & f(1) & 4 & f^2(1) & 6 & 7 & 8 & 9 \\ f(1) & 2 & f^2(1) & 6 & 1 & 4 & 8 & 9 & 7 \end{pmatrix}.$$

Maintenant $f^2(1) = f(f^2(1)) = f(5) = 1$ et nous ne pouvons plus continuer la modification du tableau. Nous pouvons cependant faire apparaître des puissances de f avec d'autres éléments que 1. En le faisant nous arrivons à

$$f = \begin{pmatrix} 1 & 2 & f(1) & 4 & f^2(1) & f(4) & 7 & f(7) & f^2(7) \\ f(1) & 2 & f^2(1) & f(4) & 1 & 4 & f(7) & f^2(7) & 7 \end{pmatrix},$$

et à partir de là nous vérifions facilement que

$$f = \Big(1 f(1) f^2(1)\Big)\ \Big(4 f(4)\Big)\ \Big(7 f(7) f^2(7)\Big) = (135)\ (46)\ (789).$$

E. 42. Effectuer la transformation précédente dans le cas où

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 8 & 2 & 4 & 3 & 5 & 1 & 9 & 7 \end{pmatrix}.$$

On comprend aisément que la transformation faite sur l'exemple précédent peut être conduite pour n'importe quelle permutation (et dans n'importe quel $\mathbf{S}_n$) de sorte que toute permutation peut être écrite comme un produit d'un certain nombre de cycles. La question se pose, par contre, de savoir si une telle décomposition est unique. Dans l'exemple précédent, à cause du théorème 35, d'autres écritures peuvent proposées en modifiant l'ordre des cycles. Par exemple

$$\begin{aligned} f &= (46)(135)(789) = (789)(46)(135) && (8.1)\\ &= (789)(46)(135) = (135)(789)(46) && (8.2)\\ &= (46)(789)(35). && (8.3) \end{aligned}$$

A cette réserve près, la décomposition est unique.

THÉORÈME 37. — *Toute permutation se décompose en un produit de cycles disjoints. Cette décomposition est unique à l'ordre près des facteurs.*

Démonstration (idée). Pour l'existence, nous employons la méthode décrite sur l'exemple ci-dessus. Pour montrer l'unicité à l'ordre près, nous commençons par établir que les supports des cycles qui interviennent dans la décomposition sont complètement

déterminés par la permutation. Étant donnée $f \in \mathbf{S}_n$, considérons la relation R_f définie par

$$i \mathsf{R}_f j \iff \text{il existe } k \in \mathbb{Z} \text{ tel que } j = f^k(i).$$

C'est une relation d'équivalence et si $(a_1 \dots a_k)$ apparaît dans une décomposition de f, c'est-à-dire $f = (\cdots)\dots(a_1 \dots a_k)\dots(\cdots)$ alors $\{a_1, \dots, a_k\}$ est une classe d'équivalence de R_f. Comme la relation R_f est complètement et uniquement déterminée par f il en est de même de ses classes d'équivalence. Une fois connue la classe $\{a_1, \dots, a_k\}$ il n'y a qu'une seule manière possible de former un cycle puisque les éléments doivent être écrits dans un ordre tel que le suivant est l'image du précédent par f. ■

La démonstration du résultat suivant est laissée en exercice.

THÉORÈME 38. — *L'ordre d'une permutation est égal au plus petit commun multiple des longueurs des cycles qui la composent.*

8.4 Signature

Notons $\Omega(n,2)$ l'ensemble des paires de $\Omega(n)$ c'est-à-dire l'ensemble des parties a deux éléments,

$$\Omega(n,2) = \{\{i,j\} \ : \ 1 \leq i < j \leq n\}.$$

Cet ensemble contient $\binom{n}{2} = n(n-1)/2$ éléments. Étant donnée $f \in \mathbf{S}_n$, nous définissons $\bar{f}$ sur $\Omega(n,2)$ par $\bar{f}(\{i,j\}) = \{f(i), f(j)\}$. Puisque $f(i)$ est distinct de $f(j)$ si $i \neq j$, $\bar{f}$ est une application de $\Omega(n,2)$ dans lui-même.

THÉORÈME 39. — *Si $f \in \mathbf{S}_n$ alors $\bar{f}$ est une bijection de $\Omega(n,2)$ dans lui-même. Si g est un autre élément de $\mathbf{S}_n$ alors $\overline{f \cdot g} = \bar{f} \cdot \bar{g}$.*

Démonstration. Puisque l'ensemble de départ est égal à l'ensemble d'arrivée et qu'il est de cardinal fini, il suffit de montrer que $\bar{f}$ est injective. Supposons que $\bar{f}(\{i,j\}) = \bar{f}(\{i',j'\})$ alors $(\{f(i), f(j)\}) = \{f(i'), f(j')\}$ d'où

$$\begin{cases} f(i) = f(i') \text{ et } f(j) = f(j') \\ \text{ou} \\ f(i) = f(j') \text{ et } f(j) = f(i') \end{cases} \implies \begin{cases} i = i' \text{ et } j = j' \\ \text{ou} \\ i = j' \text{ et } j = i' \end{cases},$$

et dans les deux cas nous avons $\{i,j\} = \{i',j'\}$. Le second point se vérifie immédiatement. ■

E. 43. L'application $f \in \mathbf{S}_n \to \overline{f}(\Omega_n(2))$ est un morphisme de groupe.

Maintenant, pour toute paire $x \in \Omega(n,2)$ nous posons

$$d(x) = |\text{différence des deux éléments de } x|.$$

Grâce à la valeur absolue cette quantité ne dépend que des éléments de x et non pas de l'ordre dans lequel ils sont écrits. Notons que $d(x)$ est toujours un entier positif.

Le théorème précédent nous permet d'écrire

$$\prod_{x\in\Omega(n,2)} d(x) = \prod_{x\in\Omega(n,2)} d(\bar{f}(x)).$$

En traduisant cette formule avec $x = \{i, j\}$ nous obtenons le théorème suivant.

THÉORÈME 40. — *Soit $f \in \mathbf{S}_n$, $n \geq 2$. Nous avons*

$$\prod_{\{i,j\}\in\Omega(n,2)} |f(i) - f(j)| = \prod_{\{i,j\}\in\Omega(n,2)} |i - j|.$$

Soit $f \in \mathbf{S}_n$. Nous définissons $\varepsilon(f)$ par la relation

$$\varepsilon(f) = \prod_{\{i,j\}\in\Omega(n,2)} \frac{f(j) - f(i)}{j - i}. \tag{8.4}$$

Nous déduisons du théorème précédent que $|\varepsilon(f)| = 1$ donc $\varepsilon(f) \in \{-1, 1\}$. Le nombre $\varepsilon(f)$ s'appelle la **signature** de f.

Si nous appelons **inversion** de f, toute paire $\{i, j\}$ pour laquelle $f(i) - f(j)/(i - j) < 0$ alors nous tirons de la définition le résultat suivant.

THÉORÈME 41. — *Soit $f \in \mathbf{S}_n$. Nous avons*

$$\varepsilon(f) = (-1)^{\text{nombre d'inversion de } f}.$$

Démonstration. Puisque la signature $\varepsilon(f)$ appartient toujours à $\{-1, 1\}$ nous pouvons la déterminer en étudiant le signe des facteurs qui apparaissent dans sa définition (8.4). ■

8.5 Propriétés de la signature

THÉORÈME 42. — *Soient $k > 1$ et $f = (1\,k)$ alors $\varepsilon(f) = -1$.*

Démonstration. D'après le théorème précédent, il suffit de vérifier que le nombre d'inversion de $(1k)$ est impair. Comptons donc les paires $\{i, j\}$ pour lesquelles $(f(i) - f(j))/(i - j)$ est négatif. Il y a le cas où $i = 1$ et $2 \leq j \leq k - 1$ car alors $(f(i) - f(j))/(i - j) = (f(1) - f(k))/(1 - k) = k - j)/(1 - k) < 0$. Il y aussi le cas $i = 1$ et $j = k$ et ce sont les seules paires pour lesquelles un des deux éléments est égal à 1. Il reste enfin les paires $\{i, k\}$ où $2 \leq i \leq k - 1$. Au total on a donc $(k - 2) + 1 + (k - 2) = 2k - 3$ qui est bien un nombre impair. ■

THÉORÈME 43. — *L'application* $\varepsilon : (\mathbf{S}_n, \cdot) \to (\{-1,1\}, \cdot)$ *est un morphisme de groupe. Autrement dit,*

$$\varepsilon(f \cdot g) = \varepsilon(f) \cdot \varepsilon(g), \quad f, g \in \mathbf{S}_n.$$

Démonstration. Nous avons

$$\varepsilon(f) = \prod_{\{i,j\}} \frac{f(i) - f(j)}{i - j} \tag{8.5}$$

$$= \prod_{\bar{g}(\{i,j\})} \frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \qquad \text{(Th. 39)} \tag{8.6}$$

$$= \prod_{\{i,j\}} \frac{f(g(i)) - f(g(j))}{i - j} \cdot \frac{i - j}{g(i) - g(j)} \tag{8.7}$$

$$= \varepsilon(f \cdot g) \cdot 1/\varepsilon(g) \qquad \text{(en séparant les deux } \prod\text{).} \quad \blacksquare$$

Ce thèorème conduit à une méthode rapide pour le calcul de la signature de n'importe quel cycle, et donc, grâce à la décomposition en cycles disjoints, de n'importe quelle permutation.

THÉORÈME 44. — *La signature d'une transposition quelconque est égale à* -1.

Démonstration. Soit $(a_1 a_2)$ une transposition. Nous avons vu que

$$(a_1 a_2) = (1 a_1)(1 a_2)(1 a_1).$$

En utilisant le théorème 42 et le fait que ε est un morphisme on a

$$\varepsilon((a_1 a_2) = \varepsilon((1 a_1))\varepsilon((1 a_2))\varepsilon((1 a_3)) = (-1)^3 = -1. \quad \blacksquare$$

THÉORÈME 45. — *La signature d'un cycle de longueur* k *est égale à* $(-1)^{k-1}$.

Démonstration. Le raisonnement est similaire à celui de la démonstration précédente en utilisant la relation

$$(a_1\, a_2\, a_3 \ldots a_k) = (a_1\, a_2) \cdot (a_2\, a_3) \ldots (a_{k-1}\, a_k). \quad \blacksquare$$

THÉORÈME 46. — *L'ensemble* $A_n := \{f \in \mathbf{S}_n : \varepsilon(f) = 1\}$ *est un sous-groupe distingué de* $\mathbf{S}_n$ *; il est appelé* n*-ième* ***groupe alterné*** *; il contient* $n!/2$ *éléments.*

§ 9. HISTOIRE

Nombre des techniques étudiées dans ce chapitre furent d'abord découvertes dans le cas particulier du groupe des permutations (alors appelées substitutions) d'un ensemble

fini et, singulièrement, du groupe $\mathbf{S}_5$. Un des problèmes qui occupaient le plus les algébristes à la fin de la Renaissance était celui d'exprimer les racines des polynômes sous la forme de radicaux de quantités dépendant des coefficients du polynôme, les radicaux pouvant être imbriqués les uns dans les autres. Il s'agissait d'étendre aux équations de degré supérieur la formule $s = (-b \pm \sqrt{\Delta})/(2a)$ qui donne les racines d'un trinôme du second degré, que nous apprenons au lycée et qui était connue depuis l'antiquité. Les algébristes italiens de la fin de la renaissance, dont le plus célèbre est Gerolamo Cardano (1501-1576), parvinrent à résoudre de manière satisfaisante ce problème dans le cas des équations de degré 3 et 4. Plus de deux cent ans passèrent sans que le degré supérieur puisse être traité. En 1770, l'italien Joseph Louis Lagrange (1736-1813), un des plus grands mathématiciens de son temps, observa que la possibilité d'exprimer les solutions des équations polynomiales de degré ≤ 4 étaient liées à des propriétés des permutations des racines. L'intérêt qu'il porta à ces permutations le font considérer, peut-être abusivement, comme un précurseur de la théorie des groupes. C'est un autre mathématicien italien Paolo Ruffini [*] (1765-1822) qui établit les premiers théorèmes typiques de la théorie des groupes. Il démontra presque complètement, avant Niels Abel (1802-1829) et Evariste Galois (1811-1832), l'impossibilité d'exprimer en général au moyen de radicaux les racines des polynômes de degré 5. Il introduisit par exemple la notion d'*ordre d'une permutation*, obtint la décomposition en produit de cycles et des résultats fins comme par exemple le fait que si G est un sous-groupe de $\mathbf{S}_5$ dont l'ordre est divisible par 5 alors G contient un élément d'ordre 5. Ces travaux seront largement généralisés par Cauchy (1789-1857) qui portera l'étude de $\mathbf{S}_n$ bien au delà de ce qui est présenté dans ce chapitre. Ce qui est dit jusqu'à présent ne concerne que les groupes de permutations. Cayley (1821-1895) travaille en 1854 avec un concept de groupe abstrait encore assez confus mais il réussit en utilisant des raisonnements typiques de l'actuelle théorie élémentaire des groupes à décrire les groupes possibles d'ordre 6. Kronecker (1823-1891) donne en 1870 une définition plus précise motivée par des questions de théorie des nombres reprise par Weber (1882). Cette définition est encore insuffisante comme le montre l'exercice ci-dessous. La définition moderne est finalement présentée en 1895 dans un livre du même Weber.

E. 44 (Definition de Kronecker). Soit $(G,\cdot)$ un ensemble fini muni d'une loi interne associative et commutative. On dit que G est un K-groupe si pour tous a,b et c dans G on a $ab = ac \implies b = c$. Montrer que G est un K-groupe si et seulement si G est un groupe. Montrer que cette propriété ne serait pas vraie si on omettait l'hypothèse que G est fini.

§ 10. EXERCICES ET PROBLÈMES COMPLÉMENTAIRES

45. Soit $(G,*)$ un groupe. On définit une loi interne $\triangle$ sur G par $a \triangle b := b * a$, $(G,\circ)$ est-il un groupe ?

∗. J J O'Connor and E F Robertson, history.mcs.st-andrews.ac.uk/Biographies/Ruffini.html

46. Soient $(G,*)$ un groupe et f une bijection de G dans G ($f \in \mathbf{S}(G)$. On définit une nouvelle loi $\bullet$ par $a \bullet b = f^{-1}(f(a) * f(b))$. Montrer que $(G,\bullet)$ est un groupe. Est-il isomorphe à $((G,*)$?

47. On note **Aff** l'ensemble des applications affines non constantes de $\mathbb{R}$ dans $\mathbb{R}$, autrement dit,

$$\mathbf{Aff} = \left\{ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax+b \end{array} : a \in \mathbb{R}^\star, b \in \mathbb{R} \right\}.$$

Montrer **Aff** est un sous-groupe de $\mathbf{S}(\mathbb{R})$. Est-il commutatif ?

48. Soient $(G,*)$ et $(W,\perp)$ deux groupes et X un ensemble non vide. On suppose que f est un morphisme de G dans H. Construire un morphisme entre $\mathscr{F}(X,G)$ et $\mathscr{F}(X,W)$. Voir l'exercice 6 pour la définition de $\mathscr{F}(X,G)$.

49. Montrer que s'il existe une bijection f entre deux ensembles Ω et Ω' alors les groupes $\mathbf{S}(\Omega)$ et $\mathbf{S}(\Omega')$ sont isomorphes. (Voir 1.8 (1.8.5) pour la définition de $\mathbf{S}(\Omega)$.)

50 (Sous-groupes remarquables de $\mathbf{GL}_n$). Dans la liste des ensembles ci-dessous déterminer qui est sous-groupe (et sous-groupe distingué) de qui ? Tracer l'arbre correspondants (voir la figure 2.3 17)

(i) $\mathbf{GL}_n(\mathbb{K})$, $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

(ii) $\mathbf{SL}_n(\mathbb{K}) := \{M \in \mathbf{M}_n(\mathbb{K}) : \det M = 1\}$, $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

(iii) $\mathbf{SL}_n(\mathbb{Z}) := \{M \in \mathbf{SL}_n(\mathbb{Q}) :$ tous les coefficients de M sont dans $\mathbb{Z}\}$

(iv) $\mathbf{O}_n(\mathbb{R}) := \{A \in \mathbf{M}_n(\mathbb{R}) : {}^tA.A = I\}$

(v) $\mathbf{O}_n^+(\mathbb{R}) := \{A \in \mathbf{O}_n(\mathbb{R}) : \det A > 0\}$

(vi) $\mathbf{T}_n(\mathbb{K}) := \{M \in \mathbf{GL}_n(\mathbb{K}) : M$ est triangulaire supérieure$\}$, $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

(vii) $\mathbf{UT}_n(\mathbb{K}) := \{M \in \mathbf{T}_n(\mathbb{K}) : M$ a des 1 sur la diagonale$\}$, $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

51. Déterminer tous les morphismes continus de $(\mathbb{R},+)$ dans $(\mathbb{R}^\star,\cdot)$, puis tous les morphismes continus de $(\mathbb{R}^{+\star},\cdot)$ dans lui-même. Un morphisme continu est un morphisme de groupe qui est aussi une application continue $\mathbb{R}$ dans $\mathbb{R}$ dans le sens que l'on étudie dans le cours d'analyse.

52 (Groupes diédraux de petits ordres).

A) Etude du *groupe diédral* $\mathbf{D}_3$.

Dans le plan euclidien P on place les points M_j, $j = 0,1,2$ d'affixe respectif $z_i = \exp(2ij\pi/3)$. Ce sont les sommets d'un triangle équilatéral, voir la figure 2. On note $T = \{M_0, M_1, M_2\}$ et on appelle $\mathbf{D}_3$ l'ensemble des isométries du plan qui conservent T :

$$\mathbf{D}_3 := \{f \in \mathbf{Is}(P) : f(T) = T\}.$$

1) Montrer que $\mathbf{D}_3$ est un sous-groupe de $(\mathbf{Is}(P),\circ)$.
2) Montrer que $\mathbf{D}_3$ est formé de 6 éléments. Donner deux éléments a et b tels que $\mathbf{D}_3 = \langle a,b\rangle$.
3) Faire une table de $\mathbf{D}_3$.

B) Etude du *groupe diédral* $\mathbf{D}_4$

On considère maintenant les points N_j, $j = 0,1,2,3$ d'affixe respectif $z_i = \exp(2ij\pi/4)$. Ce sont les sommets d'un carré, voir la figure 2. On note $C = \{N_0, N_1, N_2, N_3\}$ et on appelle $\mathbf{D}_4$ l'ensemble des isométries du plan qui conservent C :

$$\mathbf{D}_4 := \{f \in \mathbf{Is}(P) : f(C) = C\}.$$

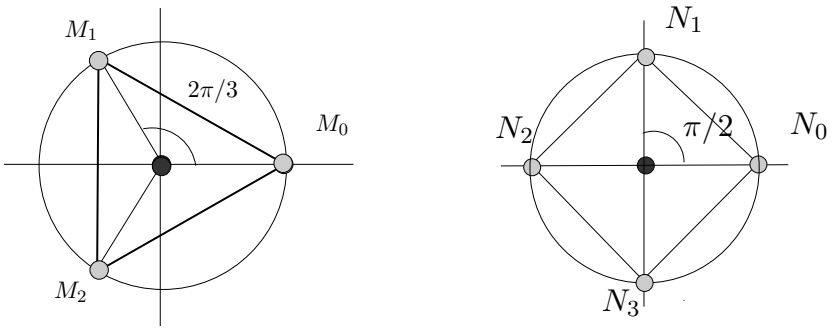


FIGURE 2 – Les figures T et C

1) Montrer que $\mathbf{D}_4$ est un sous-groupe de $(\mathbf{Is}(P), \circ)$.
2) Montrer que $\mathbf{D}_4$ est formé de 8 éléments. Donner deux éléments a et b tels que $\mathbf{D}_4 = \langle a, b \rangle$.
3) Faire une table de $\mathbf{D}_4$.

C) Les $\mathbf{S}_3$ et $\mathbf{D}_3$ sont-ils isomorphes ? Même question avec $\mathbf{S}_4$ et $\mathbf{D}_4$.

NOTE 8. — Plus généralement, si P_n désigne le polygone régulier à n sommets, d'affixes respectifs $z_j = \exp(2ij\pi/n)$, $j = 0, \ldots, n-1$, on appelle $\mathbf{D}_n$ le sous-groupe de $\mathbf{Is}(P)$ formé des isométries qui laissent P_n *globalement* invariant. $\mathbf{D}_n$ contient $2n$ éléments, il est engendré par une rotation a d'ordre n et une réflexion b vérifiant $abab = e$. (e est l'isométrie identique.)

53. Soient $(G, \cdot)$ un groupe et x, y deux éléments distincts de G, chacun différent de l'élément neutre. Montrer que si $x^2 = e$, $y^2 = e$ et $x \cdot y = y \cdot x$ alors $H = \{e, x, y, xy\}$ est un sous-groupe de G. Montrer que ce sous-groupe est isomorphe à $\mathbf{U}_2 \times \mathbf{U}_2$.

54. Montrer que si G est un groupe d'ordre 4 alors G est isomorphe à $\mathbf{U}_4$ ou à $\mathbf{U}_2 \times \mathbf{U}_2$.

55. Déterminer tous les sous-groupes de $\mathbf{U}_2 \times \mathbf{U}_4$.

56 (Centre d'un groupe). Soit $(G, *)$ un groupe. On définit le sous-ensemble $Z(G)$ par

$$Z(G) = \{u \in G : g * u = u * g \text{ pour tout } g \in G\}$$

Autrement dit, u est un élément de $Z(G)$ s'il commute avec *tous* les éléments de G.

A) Montrer que $Z(G)$ est un sous-groupe distingué de G. On l'appelle **centre** de G. A quelle(s) condition(s) a-t-on G=Z(G) ?

B) Dans cette partie, on cherche $Z(\mathbf{GL}_2(\mathbb{R}))$.

1) Soit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathbf{GL}_2(\mathbb{R})).$$

En utilisant le fait que A commute avec les matrices J et K données par

$$I = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

montrer qu'nous avons nécessairement $a = d$ et $b = 0 = c$.

2) En déduire $Z(\mathbf{GL}_2(\mathbb{R}))$.

C) Déterminer les centres des groupes diédraux $\mathbf{D}_3$ et $\mathbf{D}_4$ (voir exercice 52).

D) Montrer que si ϕ est un isomorphisme de $(G,*)$ sur $(G',\circ)$ alors $\phi(Z(G)) = Z(G')$.

NOTE 9. — Déterminer, par exemple en utilisant une récurrence, le centre de $\mathbf{GL}_n(\mathbb{R})$.

THÉORÈME 47. — *Le centre de* $\mathbf{GL}_n(\mathbb{R})$, $n \geq 2$, *est formé des matrice de la forme* λI, $\lambda \in \mathbb{R}$.

57. Soient $(G,\cdot)$ un groupe et H un sous-groupe de G. A-t-on nécessairement $Z(H) = Z(G) \cap H$?

58. Montrer que si m et n sont deux entiers (positifs) premiers entre eux alors $\mathbf{U}_{nm} \simeq \mathbf{U}_n \times \mathbf{U}_m$. Le résultat demeure-t-il si m et n ne sont plus supposés premiers entre eux ?

59. Soit $(G,*)$ un groupe. On suppose que R est une relation d'équivalence sur G qui soit compatible avec la loi $*$, autrement dit $a\,\mathrm{R}\,b$ et $a'\,\mathrm{R}\,b'$ entraîne $a'*a\,\mathrm{R}\,b'*b$. Montrer qu'il existe un sous-groupe distingué H de G tel que $\mathrm{R} = \mathrm{R}_H$.

INDI.. — On pourra considérer l'ensembles des éléments qui sont en relation avec e_G.

60. Soit p un nombre premier. On définit l'ensemble $\mathbb{Q}_p$ par

$$\mathbb{Q}_p := \left\{ \frac{m}{p^n} \,:\, m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Un élément de $\mathbb{Q}_p$ s'appelle une **fraction p-aire**.

1) Montrer que $\mathbb{Q}_p$ est un sous-groupe de $(\mathbb{Q},+)$.

2) Montrer que si p et p' sont deux nombres premiers distincts alors il n'existe pas d'isomorphisme entre $\mathbb{Q}_p$ et $\mathbb{Q}_{p'}$.

61. Soit p un nombre premier.

1) L'ensemble $\mathbb{C}_{p^\infty}$ est défini par

$$\mathbb{C}_{p^\infty} := \cup_{n=1}^{\infty} \mathbf{U}_{p^n}.$$

2) Montrer que $\mathbb{C}_{p^\infty}$ est un sous-groupe infini de $(\mathbf{U},.)$ dont tous les éléments sont d'ordre fini.

3) Est-il vrai que tous les sous-groupes de $\mathbb{C}_{p^\infty}$ sont finis ?

62 ($\leftarrow$ 60 & 61). Soit p un nombre premier.

(i) Trouver un homomorphisme entre $\mathbb{Q}_p$ et $\mathbb{C}_{p^\infty}$.

(ii) Montrer que $\mathbb{Q}_p/\mathbb{Z} \simeq \mathbb{C}_{p^\infty}$

63. Soit $(G,*)$ un sous-groupe.

(a) Montrer que l'intersection d'une famille quelconque H_i de sous-groupes distingués de G est encore un sous-groupe distingué.

(b) En déduire la définition du sous-groupe *distingué* engendré par un sous-ensemble non vide S de G. Ce sous-groupe est note $\langle S \rangle_D$.

(c) Montrer que

$$\langle S \rangle_D = \left\langle \bigcup_{g \in G} g^{-1} * S * g \right\rangle.$$

64 (← 50). Montrer que pour tout $n \geq 2$ nous avons $\mathbf{T}_n(\mathbb{K})/\mathbf{UT}_n(\mathbb{K}) \simeq (\mathbb{K}^\star)^n$

65. Montrer qu'il y a une bijection entre les sous-groupes de G qui contiennent H et les sous-groupes de G/H.

66 (Le groupe affine). Soit $n > 1$ et $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. On dit que $f : \mathbb{K}^n \to \mathbb{K}^n$ est une application affine de $\mathbb{K}^n$ s'il existe un isomorphisme linéaire g de $\mathbb{K}^n$ et un vecteur b de $\mathbb{K}^n$ tels que $f(x) = g(x) + b$ pour tout $x \in \mathbb{K}^n$. L'ensemble des ces applications est noté $\mathbf{Aff}_n(\mathbb{K})$. Il est muni de la loi de composition des applications. Montrer que $(\mathbf{Aff}_n(\mathbb{K}), \circ)$ est un groupe et $\mathbf{GL}_n(\mathbb{K})$ est isomorphes à un des ses quotients (autrement dit il existe $H \leq \mathbf{Aff}_n(\mathbb{K})$ tel que $\mathbf{GL}_n(\mathbb{K}) \simeq \mathbf{Aff}_n(\mathbb{K})/H$).

67. Soit $(G, .)$ un groupe. On suppose que $a \in G$ est un élément d'ordre 2 et b un élément d'ordre 3 tels que $ab = ba$. Ecrire la liste des éléments de $\langle a, b\rangle$ et montrer que $\langle a, b\rangle = \langle ab\rangle$. Généraliser au cas ou 2 est remplacé par s et 3 par t avec s et t premiers entre eux.

68. Soient s et t deux nombres premiers. Montrer que si G est un groupe commutatif d'ordre st alors G est isomorphe à $\mathbf{U}_s \times \mathbf{U}_t$.

69. Dans le groupe $\mathbf{GL}_2(\mathbb{R})$ on considère les éléments a et b définis par

$$a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Montrer que a est d'ordre 3 et b d'ordre 4 mais montrer que $\langle a, b\rangle$ contient une infinité d'éléments.

70 (Recherche des générateurs de $\mathbf{GL}_2(\mathbb{K})$, $\mathbb{K} = \mathbb{R}, \mathbb{Q}$ ou $\mathbb{C}$.). Pour $\alpha \in \mathbb{K}$ et $\beta \in \mathbb{K}^\star$ on définit les matrices

$$t_{12}(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \; t_{21}(\alpha) = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \; d_{11} = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \; d_{22}(\beta) = \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}$$

1) si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ calculer $t_{ij}(\alpha)A$ et $At_{ij}(\alpha)$.

2) Montrer que si $d \neq 0$ alors

$$t_{12}\left(\frac{-b}{d}\right).A.t_{21}\left(\frac{-c}{d}\right) = \begin{pmatrix} a - \frac{bc}{d} & 0 \\ 0 & d \end{pmatrix}.$$

En déduire que

$$A \in \langle t_{ij}(\alpha), d_{ii}(\beta) : (\alpha, \beta) \in \mathbb{K} \times \mathbb{K}^\star \rangle$$

3) Montrer, en se ramenant au cas $d \neq 0$ que les $t_{ij}(\alpha), d_{ii}(\beta) : (\alpha, \beta) \in \mathbb{K} \times \mathbb{K}^\star$ forment un ensemble générateur de $\mathbf{GL}_2(\mathbb{K})$.

II

Introduction à la théorie des anneaux et des corps

§ 1. La structure d'anneau

1.1 Définitions

La plupart des propriétés des nombres entiers font intervenir à la fois l'addition et la multiplication. Il en est de même des extensions successives de $\mathbb{Z}$ que sont $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Aussi est-il naturel de considérer une structure qui fasse intervenir deux lois internes liées entre elles par les mêmes type de règles que celles de l'arithmétique élémentaire. C'est la structure d'anneau que nous allons maintenant introduire. Les démonstrations des propriétés élémentaires sont très semblables à celles données dans le cas des groupes.

Un ensemble non vide A muni de deux lois internes — que nous noterons toujours, pour simplifier, $+$ et $\cdot$ — est un **anneau** si

(i) $(A,+)$ est un groupe commutatif,

(ii) la loi $\cdot$ est associative et elle est **distributive** (à droite et à gauche) par rapport à la loi $+$, c'est-à-dire,

$$\begin{aligned} x\cdot(y+z) &= (x\cdot y)+(x\cdot z), \quad x,y,z\in A \quad \text{(distributivité à gauche)},\\ (y+z)\cdot x &= (y\cdot x)+(z\cdot x), \quad x,y,z\in A \quad \text{(distributivité à droite)}. \end{aligned}$$

Nous parlons alors de l'anneau $(A,+,\cdot)$ ou — s'il n'y a pas de doute possible sur les lois que nous utilisons — simplement de l'anneau A. La loi $+$ est appelée **l'addition** de A et la loi $\cdot$ est appelée le **produit** ou la **multiplication** de A. L'élément neutre de $(A,+)$ est toujours noté 0 — ou, s'il faut être précis, 0_A — et le symétrique de $x\in A$ pour la loi $+$ est noté $-x$ et parfois appelé l'**opposé** de x. Rappelons que la notation $y-x$ signifie alors $y+(-x)$ (voir 1.9::I).

Citons immédiatement quelques exemples sur lesquels nous pourrons illustrer les propriétés introduites plus avant. Le plus important de tous les anneaux est $(\mathbb{Z},+,\cdot)$. Le lecteur est déjà familier avec l'anneau $(M_n(\mathbb{K}),+,\cdot)$ ($\mathbb{K}=\mathbb{Q},\mathbb{R},\mathbb{C}$) formé des matrices carrées à coefficients dans $\mathbb{K}$ avec l'addition et la multiplication habituelle des matrices. La plupart des familles fondamentales de fonctions étudiées en analyse forment aussi des anneaux. Par exemple, si I est un intervalle de $\mathbb{R}$, l'ensemble $\mathcal{C}(I)$ des fonctions continues sur I devient un anneau lorsqu'il est muni de l'addition et de la multiplication habituelle des fonctions. Les anneaux les plus importants, après $\mathbb{Z}$, sont les anneaux de polynômes, une partie entière sera consacrée à leur définition et à leurs propriétés fondamentales.

1.2 Calcul dans les anneaux

La distributivité s'étend immédiatement en utilisant une démonstration par récurrence à un nombre quelconque de sommants. Ainsi, la distributivité à gauche donne par exemple $x\cdot(a_1+a_2+\cdots+a_n)=x\cdot a_1+x\cdot a_2+\cdots+x\cdot a_n$. En utilisant à la fois la distributivité à gauche et à droite, nous obtenons le développement

$$(b_1+\cdots+b_m)\cdot(a_1+a_2+\cdots+a_n)=\sum_{(i,j)\in\Omega(m)\times\Omega(n)} b_i\cdot a_j \tag{1.1}$$

où $\sum_{x\in X} a_x$ désigne la l'addition de tous les éléments a_x lorsque x parcourt X et $\Omega(n)=\{1,2,\ldots,n\}$. La distributivité est le seul axiome qui lie les deux opérations de l'anneau. En réalité, dans l'arithmétique élémentaire des entiers naturels, la multiplication n'est pas indépendante de l'addition puisque le résultat de la multiplication d'un nombre n par m est obtenu, par définition, en additionnant m fois le nombre n (ou encore, puisque l'on démontre que cela revient au même, m fois le nombre n). Puisque toutes les lois usuelles sur $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ sont définies en étendant la loi correspondante sur l'ensemble qui le précède, il est clair que la multiplication usuelle des nombres complexes trouve son origine dans l'addition des entiers naturels et la distributivité du produit par rapport à la multiplication n'est qu'un reflet lointain du lien qui lie la définition de la multiplication à celle de l'addition des entiers. La remarque vaut semble-t-il, pour pratiquement toutes, sinon toutes, les lois d'anneaux qui ont quelque utilité en mathématiques. Cependant, comme nous allons le voir, l'oubli de ce lien, ou plutôt sa réduction à la seule propriété de distributivité, éclaire plutôt qu'il n'obscurcit l'étude des propriétés de A en rapport à ces deux lois. Signalons qu'il existe un anneau, sans intérêt, dans lequel le lien est limité (mais évident). C'est celui pour lequel le produit est défini par $x\cdot y=0_A$ pour tous $x,y\in A$. Un tel anneau est dit à **multiplication nulle**.

NOTE 10. — L'addition et le produit étant associatifs, conformément à ce qui est indiqué dans le théorème I::1 il est inutile d'employer des parenthèses dans les expressions qui font intervenir uniquement le produit ou uniquement l'addition. Il en va différemment pour les expressions faisant intervenir à la fois le produit et l'addition. Ainsi par exemple, $a\cdot b+c$ doit-il être compris comme $(a\cdot b)+c$ ou bien $a\cdot(b+c)$? On convient généralement que les multiplications sont prioritaires (effectuées en premier) de

sorte que c'est la première valeur, $(a\cdot b)+c$, qui est attribuée à $a\cdot b+c$. L'emploi de parenthèses reste nécessaire si nous voulons considérer $(a+b)\cdot c$. Pour éviter toute confusion, il est préférable de maintenir les parenthèses dans tous les cas où elles ne deviennent pas par trop encombrantes.

THÉORÈME 1. — *Dans tout anneau $(A,+,\cdot)$, nous avons*

(i) $a\cdot 0=0=0\cdot a, \quad a\in A.$

(ii) $(-a)\cdot b=a\cdot(-b)=-(ab), \quad a,b\in A.$

A cause de la première propriété, le neutre de la loi $+$ est parfois appelé un élément **absorbant**.

Démonstration. (i) Soit $a\in A$. On $a+0=a \implies a\cdot(a+0)=a\cdot a \implies a\cdot a+a\cdot 0=a\cdot a \implies a\cdot 0=0$. Pour la deuxième implication nous avons utilisé la propriété de distributivité. Nous montrons de même que $0\cdot a=0$ en partant de $0+a=a$.

(ii) Soient $a,b\in A$. On a $(a-a)\cdot b=0\cdot b=0$ ou encore $(a+(-a))\cdot b=0$ qui donne en utilisant la distributivité $a\cdot b+(-a)\cdot b=0 \implies (-a)\cdot b=-(a\cdot b)$. Nous montrons de la même manière que $a\cdot(-b)=-(a\cdot b)$. ∎

Le théorème entraîne la règle de **simplification des signes** dans un anneau. Dans tout anneau $(A,+,\cdot)$, nous avons

$$(-a)\cdot(-b)=a\cdot b. \tag{1.2}$$

En effet, en appliquant le point (ii) du théorème avec $-b$ à la place de b, nous obtenons $(-a)\cdot(-b)=a\cdot(-(-b))=a\cdot b$.

Si a et b commutent pour le produit, c'est-à-dire $a\cdot b=b\cdot a$, alors certaines identités remarquables de l'arithmétique élémentaire demeurent vraies. Par exemple,

$$\begin{aligned}(a+b)^2=(a+b)\cdot(a+b)&=(a+b)\cdot a+(a+b)\cdot b\\&=a\cdot a+b\cdot a+a\cdot b+b\cdot b=a^2+2(a\cdot b)+b^2,\end{aligned} \tag{1.3}$$

où nous avons utilisé la distributivité dans les seconde et troisième égalité et l'hypothèse de commutation dans la dernière. Nous établissons facilement, par récurrence, la formule du **binôme de Newton** dans les anneaux

THÉORÈME 2. — *Si $a\cdot b=b\cdot a$ alors*

$$(a+b)^n=\sum_{j=0}^{n}\binom{n}{j}a^j\cdot b^{n-j}. \tag{1.4}$$

L'hypothèse de commutation est essentielle. Rappelons aussi que $k=\binom{n}{j}$ étant un entier, l'écriture $\binom{n}{j}a^j\cdot b^{n-j}$ désigne $(a^j\cdot b^{n-j})+\cdots+(a^j\cdot b^{n-j})$ (k fois).

E. 71. Démontrer le théorème 2.

1.3 Différents types d'anneaux

Soit $(A,+,\cdot)$ un anneau. Si le produit est une loi commutative, nous disons que $(A,+,\cdot)$ est un **anneau commutatif**. Si cette même loi admet un élément neutre, alors appelé **unité** de A, — qui sera alors toujours noté 1, ou, s'il faut préciser, 1_A — nous disons que $(A,+,\cdot)$ est **unitaire**. L'anneau $(\mathbb{Z},+,\cdot)$ est commutatif et unitaire d'unité 1, $(M_n(\mathbb{K}),+,\cdot)$ est unitaire, d'unité la matrice identité mais il n'est pas commutatif. Enfin $(A,+,\cdot)$ est **intègre** lorsque un produit $a\cdot b$ ne peut pas être nul sans qu'au moins un des facteurs a ou b le soit. Autrement dit $(A,+,\cdot)$ est intègre si $a\cdot b=0_A \implies a=0_A$ ou $b=0_A$. Cette propriété est très importante car elle permet de simplifier par des facteurs communs non nuls. $(\mathbb{Z},+,\cdot)$ est intègre, $(M_n(\mathbb{K}),+,\cdot)$ n'est pas intègre dès lors que $n\geq 2$.

$$\text{Si } (A,+,\cdot) \text{ est intègre alors } \left\{\begin{array}{ccc} a\cdot x & = & a\cdot y \\ a & \neq & 0_A \end{array}\right\} \implies x=y. \tag{1.5}$$

En effet $a\cdot x=a\cdot y \implies a\cdot x-a\cdot y=0_A \implies a\cdot(x-y)=0_A$. Donc, puisque A est intègre un des deux facteur est nul. Comme $a\neq 0_A$, il ne peut s'agir que du facteur $x-y$ et $x-y=0_A$ donne $x=y$. Naturellement, nous pouvons tirer la même conclusion si le facteur commun a dans (1.5) se trouve à *droite* de x et y. Lorsque nous écrivons $x=y$ à partir de $a\cdot x=a\cdot y$, nous disons que nous avons simplifié par le terme non nul a.

Une autre manière de dire que l'anneau $(A,+,\cdot)$ est intègre c'est de dire que les applications $x\in A\to a\cdot x\in A$ et $x\in A\to x\cdot a$ sont injectives dès lors que a n'est pas égal à 0_A.

Lorsque 0_A peut s'écrire $0_A=a\cdot b$ avec a et b non nuls — c'est-à-dire différents de 0_A — nous disons que a et b sont des **diviseur de zéro**. Un anneau intègre est donc un anneau qui n'admet aucun diviseur de zéro.

E. 72. Trouver lorsque $n=2$ des matrices a,b,c et d telles que $a\cdot b\neq b\cdot a$. En déduire des contrexemples à la commutativité de $M_n(\mathbb{K})$ pour $n>1$ quelconque.

s: p. 105 E. 73. Montrer que toute matrice non inversible est un diviseur de zéro dans $(M_n(\mathbb{R}),+,\cdot)$. [s:2]

NOTE 11. — Les anneaux non commutatifs sont difficiles à étudier et la plupart des anneaux qui ont un intérêt immédiat sont intègres et unitaires. Certains auteurs appellent anneau ce qui est pour nous un anneau unitaire.

1.4 Sous-anneaux

Soit $(A,+,\cdot)$ un anneau et B un sous-ensemble *non vide* de A, B est un **sous-anneau** de A si

(i) $a,b\in B \implies a-b\in B$,

(ii) $a,b\in B \implies a\cdot b\in B$.

Cela signifie que les restrictions des lois $+$ et $\cdot$ à B sont des lois internes sur B et que, muni des ces restrictions, B est lui-même un anneau. Remarquons la première des

deux conditions ci-dessus dit exactement que B est un sous-groupe de $(B,+)$.

Comme dans le cas des groupes, *l'intersection d'une famille quelconque non vide de sous-anneaux de A est encore un sous-anneau de A* (exercice). En reprenant l'idée utilisée en théorie des groupes (I::4.2), étant donnée une partie non vide X de A, nous définissons le sous-anneau de A engendré par X comme l'intersection de tous les sous-anneaux de A qui contiennent X. C'est le plus petit sous-anneau de A contenant X. Cette notion est, dans la théorie des anneaux, d'une importance limitée contrairement à ce qui passe dans la théorie des groupes et dans celle des corps que nous verrons plus loin.

E. 74. Soit $(A,+,\cdot)$ un anneau et X un sous-ensemble non vide de A. Peut-on décrire les éléments du sous-anneau de A engendré par X comme nous l'avons au théorème I::19 dans le cas des groupes. [s:3]

s: p. 105

1.5 Exemples

(1.5.1) $(\mathbb{Z},+,\cdot)$ *est un sous-anneau de* $(\mathbb{Q},+,\cdot)$ lui-même sous-anneau de $(\mathbb{C},+,\cdot)$. Pour tout $n\in\mathbb{N}$, $n\mathbb{Z}$ est sous-anneau (*non* unitaire) de $(\mathbb{Z},+,\cdot)$. Ce sont d'ailleurs les seuls sous-anneaux de $\mathbb{Z}$ puisqu'un sous-anneau est, en particulier un sous-groupe de $(\mathbb{Z},+)$ et nous avons vu au théorème I::5 que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.

E. 75. Soit $m\in\mathbb{N}^\star$. Définissons $\mathbb{Q}_r := \{a/m^r : (a,r)\in\mathbb{Z}\times\mathbb{N}\}$. (1) Montrer que $\mathbb{Q}_r$ est un sous-anneau de $(\mathbb{Q},+,\cdot)$. (2) Montrer que le sous anneau de $(\mathbb{Q},+,\cdot)$ engendré par $X=\mathbb{Z}\cup\{1/m\}$ n'est autre que l'anneau $\mathbb{Q}_r$.

(1.5.2) Soit $(A,+,\cdot)$ un anneau et X un ensemble quelconque non vide. L'ensemble des applications de X dans A, noté $\mathscr{F}(X,A)$, est un anneau lorsqu'il est muni de l'addition et du produit des applications

$$(f+g)(x) := f(x)+g(x),\quad x\in A, \tag{1.6}$$
$$(f\cdot g)(x) := f(x)\cdot g(x),\quad x\in A. \tag{1.7}$$

Lorsque X est égal à A, cet anneau est noté $\mathscr{F}(A)$. Si I est un intervalle de $\mathbb{R}$, l'ensemble $\mathsf{C}(I)$ des fonctions continues sur I est un sous-anneau de $\mathscr{F}(I,\mathbb{R})$. Il faut prendre garde que dans les relations (1.6) et (1.7) les symboles $+$ et $\cdot$ dans les termes de droite ne représentent pas les mêmes lois que le symbole $+$ et $\cdot$ dans les termes de gauche[s:4].

s: p. 105

(1.5.3) Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux. Le produit cartésien $A\times B$ devient un anneau avec les lois $(a,b)+(a',b') := (a+a',b+b')$ et $(a,b)\cdot(a',b') = (a\cdot a',b\cdot b')$. Ici, nous utilisons trois fois les mêmes symboles ('$+$' et '$\cdot$') pour désigner trois lois différentes. Si A et B sont unitaires $A\times B$ l'est aussi, d'unité $(1_A,1_B)$. Par contre $A\times B$ n'est jamais un anneau intègre, à moins que l'un des deux anneau ne soit réduit à l'élément nul.

E. 76. Montrer que si $(\mathscr{F}(X,A),+,\cdot)$ est intègre si et seulement si A est intègre et X est réduit à un seul élément.

E. 77. Soit $d \in \mathbb{N}^\star$. On note $\mathsf{C}^d(I)$ l'ensemble des fonction d-fois dérivables sur I dont la dérivée d-ième est continue. Montrer que $\mathsf{C}^d(I)$ est un sous-anneau de $\mathsf{C}(I)$. Est-il intègre ?

1.6 Morphismes d'anneaux

Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux et f une application de A dans B. Nous disons que f est un **morphisme d'anneau** si

(i) $f(a+a') = f(a)+f(a')$, $a,a' \in A$;

(ii) $f(a\cdot a') = f(a)\cdot f(a')$, $a,a' \in A$.

Autrement dit, f doit respecter les deux lois de l'anneau. Cependant, lorsque A et B sont *unitaires*, nous rajoutons la condition

(iii) $f(1_A) = 1_B$.

Comme dans le cas des groupes, on utilise les terminologies d'homomorphisme, d'isomorphisme (morphisme bijectif), d'automorphisme (isomorphisme d'un anneau sur lui-même). Les morphismes sont en particulier des morphismes de groupes (de $(A,+)$ dans $(B,+)$) et les résultats sur les morphismes de groupes s'appliquent. Ainsi, nous avons toujours toujours $f(0_A) = 0_B$ (théorème I::10) et pour tout $n \in \mathbb{Z}$, $f(na) = nf(a)$. En particulier $f(-a) = -f(a)$. *Pour qu'un morphisme d'anneau soit injectif, il faut et il suffit que son noyau soit réduit au neutre* 0_A où le noyau $\ker f$ est défini, rappelons-le, par $\ker f := \{a \in A : f(a) = 0_B\}$.

E. 78. L'ensemble image d'un morphisme d'anneau est un sous-anneau de l'anneau d'arrivée.

E. 79. Déterminer tous les morphismes d'anneau de $(\mathbb{Z},+,\cdot)$ dans lui-même.

E. 80. Soit $X \in \mathbf{GL}_n(\mathbb{K})$. Montrer que l'application ϕ_X définie de $M_n(\mathbb{K})$ dans lui-même par la relation $\phi_X(A) = XAX^{-1}$ est un automorphisme de $(M_n(\mathbb{K}),+,\cdot)$.

§ 2. ELÉMENTS INVERSIBLES D'UN ANNEAU UNITAIRE. CORPS

2.1 Le groupe des éléments inversibles

Soit $(A,+,\cdot)$ un anneau unitaire d'unité 1. Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que

$$a\cdot b = b\cdot a = 1. \tag{2.1}$$

Cet élément b, s'il existe, est unique (voir I::1.7), c'est l'élément symétrique de a pour la loi produit. Nous le notons a^{-1} et l'appelons l'inverse de a. L'anneau unitaire A compte toujours au moins un élément inversible, l'unité 1 elle-même, pour lequel $1^{-1} = 1$. Nous désignerons par A^* ou $\mathrm{U}(A)$ l'ensemble des éléments inversible de l'anneau A. Puisque $(a^{-1})^{-1} = a$, si $a \in A^*$ alors $a^{-1} \in A^*$.

D'autre part, puisque pour tout $a \in A$, $a\cdot 0_A = 0_A$, l'élément 0_A n'est jamais inversible, à moins que $0_A = 1_A$. Mais, dans ce cas, pour tout $a \in A$, $a = a\cdot 1_A = a\cdot 0_A = 0_A\cdot$.

Autrement dit, A est réduit à un seul élément 0_A et les lois $+$ et $\cdot$ sont définies par $0_A + 0_A = 0_A$ et $0_A \cdot 0_A = 0_A$. Cet anneau trivial n'a évidemment aucun intérêt.

NOTE 12. — Beaucoup de théorèmes de la théorie des anneaux ne s'appliquent pas à cet anneau particulier. Des mathématiciens lui ont donné le nom de **nullring** pour pouvoir facilement l'exclure des énoncés. Nous avons montré que *dans tout anneau unitaire différent du nullring,* $1_A \neq 0_A$. Un anneau à multiplication nulle, s'il est différent du nullring, n'est jamais unitaire.

THÉORÈME 3. — *L'ensemble A^* des éléments inversibles d'un anneau unitaire $(A,+,\cdot)$ muni de la multiplication de A forme un groupe.*

Démonstration. Montrons que le produit de l'anneau (rigoureusement, la restriction du produit) est une loi interne sur A^*. Pour cela, nous devons vérifier que si $a \in A^*$ et $b \in A^*$ alors $a \cdot b \in A^*$, autrement dit $a \cdot b$ est inversible. C'est bien le cas et l'inverse est $b^{-1} \cdot a^{-1}$ car $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1_A = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b)$. Ensuite $\cdot$ est une loi associative sur A^* (car elle est déjà associative sur A) ; elle admet un élément neutre (l'unité 1) et tout élément possède un élément symétrique pour $\cdot$, c'est la définition de A^*. Cela montre que $(A^*,\cdot)$ est un groupe. ■

Ce théorème nous permettra d'utiliser les ressources du chapitre I pour étudier la structure du groupe des éléments inversibles d'un anneau pour obtenir des résultats assez profonds.

Exemple 1. Le tableau suivant indique le groupe des éléments inversibles de quelques anneaux.

A	$A^* = \mathrm{U}(A)$
$\mathbb{Z}$	$\{-1,+1\}$
$\mathbb{Q}$	$\mathbb{Q} \setminus \{0\}$
$M_n(\mathbb{R})$	$\mathbf{GL}_n(\mathbb{R})$
$\mathscr{F}(X,\mathbb{R})$	$\{f \in \mathscr{F}(X,\mathbb{R}) : \forall x \in X\ f(x) \neq 0\}$

E. 81. Soient A et B deux anneaux unitaires. Montrer que $\mathrm{U}(A \times B) = \mathrm{U}(A) \times \mathrm{U}(B)$.

E. 82. Soient A et B deux anneaux unitaires et f un morphisme de A dans B. Montrer que si $a \in A^*$ alors $f(a) \in B^*$ et $f(a^{-1}) = [f(a)]^{-1}$.

2.2 Définition d'un corps

Un anneau unitaire $(F,+,\cdot)$ dans lequel $1_F \neq 0_F$ et pour lequel $F^* = F/\{0_F\}$ s'appelle un **corps**. Autrement dit, un corps est un anneau unitaire (non trivial) dans lequel tous les éléments non nuls sont inversibles. Les corps ne sont donc que des anneaux unitaires particuliers. Un corps est toujours un anneau intègre. En effet, dans un corps, les conditions $x \cdot y = 0$ et $x \neq 0$, $y \neq 0$ sont contradictoires : puisque $x \neq 0$, il est inversible et alors $x \cdot y = 0 \implies x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0 \implies y = 0$.

Les deux corps les plus importants de l'analyse sont $(\mathbb{R},+,\cdot)$ et $(\mathbb{C},+,\cdot)$. L'algèbre, par contre, utilise quantité d'autres familles de corps, à commencer par $(\mathbb{Q},+,\cdot)$, dont nous étudierons par la suite quelques représentants.

THÉORÈME 4. — *Si F_1 et F_2 sont deux corps et si f est un morphisme (d'anneaux unitaires) entre F_1 et F_2 alors f est nécessairement injective.*

Rappelons que la définition de morphisme d'anneaux unitaires requiert que l'image de l'unité de l'anneau de départ soit l'unité de l'anneau d'arrivée, ici $f(1_{F_1}) = 1_{F_2}$.

Démonstration. En effet, s'il existe $x \in \ker f$ avec $x \neq 0$ nous avons $f(x) = 0_{F_2} \implies f(x)\cdot f(x^{-1}) = 0_{F_2} \implies f(x\cdot x^{-1}) = 0_{F_2} \implies f(1_{F_1}) = 0_{F_2} \implies 1_{F_2} = 0_{F_2}$ et cela contredit la fait que F_2 est un corps. ■

Exemple 2. L'application qui à un nombre complexe $z = x+iy$ fait correspondre son conjugué $\bar{z} = x+iy$ est un automorphisme de $(\mathbb{C},+,\cdot)$.

E. 83. Déterminer l'ensemble de tous les automorphismes de $(\mathbb{C},+,\cdot)$ qui coïncident avec l'identité sur $\mathbb{R}$.

Il existe des corps non commutatifs (c'est-à-dire pour lesquels le produit n'est pas une loi commutative). Le plus célèbre est le corps des quaternions. Dans ce chapitre nous considérerons seulement des corps commutatifs.

Dans un *corps commutatif* il est commode* d'écrire a/b ou $\frac{a}{b}$ à la place de $a\cdot b^{-1}$. Nous disposons alors des règles de calcul suivantes, formellement identiques à celle de l'arithmétique élémentaire,

$$\frac{a}{b}\cdot\frac{c}{d} = \frac{a\cdot b}{b\cdot d} \quad \text{et} \quad \frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd}. \tag{2.2}$$

Démontrons la seconde formule.

$$\begin{aligned}\frac{a}{b}\cdot\frac{c}{d} &= a\cdot b^{-1}+c\cdot d^{-1}\\ &= (a\cdot d)\cdot d^{-1}\cdot b^{-1}+(c\cdot b)\cdot b^{-1}\cdot d^{-1}\\ &= (a\cdot d)\cdot(b\cdot d)^{-1}+(c\cdot b)\cdot(d\cdot b)^{-l}\\ &= (a\cdot d+b\cdot c)\cdot(b\cdot d)^{-1} \quad \text{(car le produit est commutatif)}\\ &= \frac{a\cdot b+b\cdot c}{b\cdot d}.\end{aligned}$$

2.3 Sous-corps et sous-corps engendrés

Une partie non vide L de F est un **sous-corps** de F si

(i) $x,y\in L \implies x-y\in F, \quad x,y\in L$;

∗. Voir aussi la note I::3, p. 13.

(ii) $x,y \in L \implies x\cdot y \in F, \quad x,y \in L$;

(iii) $x \in L\setminus\{0\} \implies x^{-1} \in L$,

où les deux premières conditions donnent simplement que L est un sous-anneau de L tandis que la dernière dit que l'inverse de tout élément non nul de L (qui existe puisque F est un corps) se trouve lui aussi dans L. Il est facile de vérifier (voir 2.1::I) que ces trois conditions sont équivalentes aux deux suivantes :

(iv) $x,y \in L \implies x-y \in F$,

(v) $x,y \in L\setminus\{0\} \implies x\cdot y^{-1} \in F$.

Remarquons que $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ qui, à son tour est un sous-corps, de $\mathbb{C}$. Un sous-corps L de F contient toujours 0_F et 1_F et plus généralement $n1_F$ pour tout $n \in \mathbb{Z}$.

Une famille quelconque non vide de sous-corps de F est encore un sous-corps de F. Si X est un sous-ensemble de F, nous désignons par (X) le sous-corps obtenu en prenant l'intersection de tous les sous-corps de F qui contiennent X. Le sous-corps de $\mathbb{R}$ engendré par $\mathbb{Z}$ n'est autre que $\mathbb{Q}$, autrement dit $(\mathbb{Z}) = \mathbb{Q}$.

2.4 Exemples de sous-corps : les corps quadratiques

Soit θ un nombre rationnel positif qui ne soit pas le carré d'un rationnel c'est-à-dire $\sqrt{\theta} \neq \mathbb{Q}$. Posons

$$\mathbb{Q}(\sqrt{\theta}) := \{x+y\sqrt{\theta} : x,y \in \mathbb{Q}\}, \quad \text{et} \tag{2.3}$$

$$\mathbb{Q}(i\sqrt{\theta}) := \{x+iy\sqrt{\theta} : x,y \in \mathbb{Q}\}. \tag{2.4}$$

THÉORÈME 5. — *$\mathbb{Q}(\sqrt{\theta})$ est un sous-corps de $\mathbb{R}$ et $\mathbb{Q}(i\sqrt{\theta})$ est un sous-corps de $\mathbb{C}$. Le premier est le sous-corps de $\mathbb{R}$ engendré par $\sqrt{\theta}$, $(\{\sqrt{\theta}\}) = \mathbb{Q}(\sqrt{\theta})$ tandis que le second est le sous-corps de $\mathbb{C}$ engendré par $(i\sqrt{\theta})$, $(\{i\sqrt{\theta}\}) = \mathbb{Q}(i\sqrt{\theta})$.*

Les corps $\mathbb{Q}(\sqrt{\theta})$ et $\mathbb{Q}(i\sqrt{\theta})$ s'appellent des **corps quadratiques**.

Nous nous contenterons de démontrer les assertions dans le cas de $\mathbb{Q}(\sqrt{\theta})$.

LEMME 1. — *Si x et y sont deux rationnels et $\alpha = x+\sqrt{\theta}y$ alors $\alpha = 0$ (si et) seulement si $x = y = 0$.*

Démonstration. En effet $\alpha = 0 \implies x+\sqrt{\theta}y = 0 \implies (x+\sqrt{\theta}y)(x-\sqrt{\theta}y) = 0 \implies x^2-\theta y^2 = 0$. Si $y = 0$ alors il vient immédiatement $x = 0$. Sinon, si $y \neq 0$ alors $\theta = (x/y)^2 \implies \sqrt{\theta} = (x/y)$ ce qui contredit l'hypothèse sur θ. ∎

Démonstration du théorème 5. $\mathbb{Q}(\sqrt{\theta})$ étant évidement un sous-ensemble non vide de $\mathbb{R}$, pour établir que c'est un sous-corps, nous devons montrer que si $\theta = x+y\sqrt{\theta}$ et $\beta = x'+y'\sqrt{\theta}$ sont deux éléments quelconques de $\mathbb{Q}(\sqrt{\theta})$, alors $\theta-\beta \in \mathbb{Q}(\sqrt{\theta})$ puis

$\theta\cdot\beta^{-1}\in\mathbb{Q}(\sqrt{\theta})$ dès que $\beta\neq 0$ (c'est-à-dire, d'après le lemme, $x'\neq 0$ ou $y'\neq 0$). Le premier point est évident. Nous omettons sa vérification. Pour le second, nous avons

$$\theta\cdot\beta^{-1}=\frac{x+y\sqrt{\theta}}{x'+y'\sqrt{\theta}}=\frac{(x+y\sqrt{\theta})(x'-y'\sqrt{\theta})}{x'^2+dy'^2}=\frac{xx'-\theta yy'}{x'^2+dy'^2}+\sqrt{\theta}\frac{x'y-xy'}{x'^2+dy'^2}.$$

Nous obtenons une expression de la forme $\square_1+\sqrt{\theta}\square_2$ avec $\square_i$ des rationnels pour $i=1,2$ de sorte que $\theta\cdot\beta^{-1}$ est bien un élément de $\mathbb{Q}(\sqrt{\theta})$. Ceci achève la démonstration que $\mathbb{Q}(\sqrt{\theta})$ est un sous-corps de $\mathbb{R}$. Il reste à établir que $\mathbb{Q}(\sqrt{\theta})$ est le plus petit sous-corps de $\mathbb{R}$ contenant $\sqrt{\theta}$. Nous avons vu qu'un sous-corps de $\mathbb{R}$ contient nécessairement $n=n\cdot 1$, $n\in\mathbb{Z}$ donc aussi $1/s$, $s\in\mathbb{N}^\star$ et donc aussi tout élément de la forme n/s. cela montre que le sous-corps engendré par $\sqrt{\theta}$ contient $\mathbb{Q}$ et aussi évidemment $\sqrt{\theta}$ donc tout élément de la forme $x+y\sqrt{\theta}$, $x,y\in\mathbb{Q}$. Cela montre que $(\sqrt{\theta})$ contient $\mathbb{Q}(\sqrt{\theta})$. Puisque $\mathbb{Q}(\sqrt{\theta})$ est lui-même un sous-corps de $\mathbb{R}$ contenant $\sqrt{\theta}$, nous avons aussi $(\theta)\subset\mathbb{Q}(\sqrt{\theta})$ et l'égalité $(\sqrt{\theta})=\mathbb{Q}(\sqrt{\theta})$ se déduit de la double inclusion. ■

Les corps quadratiques sont les exemples les plus simples de sous-corps de $\mathbb{C}$ construits à partir d'une racine d'un polynôme à coefficients dans $\mathbb{Q}$ — ici le polynôme $x^2-\theta$ pour $\mathbb{Q}(\sqrt{\theta})$ et $x^2+\theta$ pour $\mathbb{Q}(i\sqrt{\theta})$ — que nous rencontrerons plus avant.

E. 84. Déterminer tous les automorphismes du corps $\mathbb{Q}(\sqrt{d},+,\cdot)$.

§ 3. L'ANNEAU $\mathbb{Z}_n$

3.1 Construction

Soit $n\in\mathbb{N}$, $n\geq 2$. Nous avons vu dans 6.5::I que nous pouvons munir $\mathbb{Z}_n$ d'une loi de groupe abélien cyclique jusqu'ici notée $\overline{+}$ pour laquelle $\overline{r}\overline{+}\overline{s}=\overline{r+s}$. Pour simplifier les notations, cette loi $\overline{+}$ sera maintenant notée $+$, confondant ainsi les notation des lois d'addition dans $\mathbb{Z}$ et $\mathbb{Z}_n$. Nous voulons maintenant construire une loi produit pour définir une structure d'anneau sur $\mathbb{Z}_n$. Il est bien naturel de vouloir suivre la même idée que pour la construction de l'addition en proposant de définir la loi $\cdot$ comme suit :

$$\begin{array}{rccl}\cdot\ : & \mathbb{Z}_n\times\mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (\mathtt{C}_1\,,\,\mathtt{C}_2) & \longmapsto & \mathbf{cl}\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_1\end{array}\cdot\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_2\end{array}\right)\end{array}\qquad(3.1)$$

Juste comme pour la cas de l'addition, nous devons vérifier que cette définition est *consistante*, c'est-à-dire que le calcul de $\mathtt{C}_1\cdot\mathtt{C}_2$ ne dépend pas des représentants choisis. Pour cela nous devons vérifier que l'implication suivante est vraie,

$$\left.\begin{array}{l}m_1,s_1\in\mathtt{C}_1\\ m_2,s_2\in\mathtt{C}_2\end{array}\right\}\Longrightarrow\mathbf{cl}(m_1\cdot m_2)=\mathbf{cl}(s_1\cdot s_2).$$

[TH 5]

Or

$$\begin{array}{lll} m_1, s_1 \in \mathsf{C}_1 & \Longrightarrow & m_1 \,\mathsf{R}_{n\mathbb{Z}}\, s_1 \Longrightarrow s_1 - m_1 \in n\mathbb{Z} \Longrightarrow s_1 = m_1 + k_1 n \\ m_2, s_2 \in \mathsf{C}_2 & \Longrightarrow & s_2 = m_2 + k_2 n, \end{array}$$

ce qui entraîne

$$s_1 \cdot s_2 = (m_1 + k_1 n)(m_2 + k_2 n) = m_1 m_2 + (k_2 m_1 + k_1 m_2) n$$

et nous avons bien $s_1 s_2 - m_1 m_2 \in n\mathbb{Z}$ soit $\mathbf{cl}(s_1 s_2) = \mathbf{cl}(m_1 m_2)$. La définition du produit est donc consistante.

En particulier, sont valables les règles de calculs suivantes

$$\mathbf{cl}(m) \cdot \mathbf{cl}(r) = \mathbf{cl}(mr), \quad m, r \in \mathbb{Z} \tag{3.2}$$

ou encore, en utilisant la notation $\mathbf{cl}(m) = \overline{m}$,

$$\overline{m} \cdot \overline{r} = \overline{mr}, \quad m, r \in \mathbb{Z}. \tag{3.3}$$

Il découle facilement de ces relations que la loi $\cdot$ est associative et commutative et qu'elle admet $\overline{1}$ comme élément neutre. Voici la table de multiplication dans $\mathbb{Z}_4$ et $\mathbb{Z}_5$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Table de multiplication dans $\mathbb{Z}_4$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Table de multiplication dans $\mathbb{Z}_5$

THÉORÈME 6. — *$(\mathbb{Z}_n, +, \cdot)$ est un anneau commutatif unitaire.*

Démonstration. Toutes les propriétés ont déjà été établies exceptée la distributivité qui découle aisément de la distributivité de la multiplication par rapport à l'addition dans $\mathbb{Z}$. En effet

$$\overline{m} \cdot (\overline{r} + \overline{s}) = \overline{m} \cdot \overline{r+s} = \overline{m(r+s)} = \overline{mr + ms} = \overline{mr} + \overline{ms} = \overline{m} \cdot \overline{r} + \overline{m} \cdot \overline{s}. \quad \blacksquare$$

En général, l'anneau $\mathbb{Z}_n$ n'est pas intègre. Par exemple dans $\mathbb{Z}_4$ nous avons $\overline{2} \neq \overline{0}$ et pourtant $\overline{2} \cdot \overline{2} = \overline{0}$. Plus généralement si $n = n_1 n_2$ alors $\overline{n_1}$ et $\overline{n_2}$ sont des diviseurs de zéro dans $\mathbb{Z}_n$ car $\overline{n_1} \cdot \overline{n_2} = \overline{n} = \overline{0}$. Cela montre en particulier qu'une condition pour que $\mathbb{Z}_n$ soit intègre est que n soit un nombre premier et dans ce cas nous allons voir que c'est un corps.

3.2 Le groupe des éléments inversibles de $\mathbb{Z}_n$

THÉORÈME 7. — *Soit $n \geq 2$. Pour que $\overline{r} \in \mathrm{U}(\mathbb{Z}_n)$ il faut et il suffit que r et n soient premiers entre eux.*

Nous retrouvons la même condition que celle donnée au théorème I::31. Nous renvoyons au commentaire qui a été fait à la suite de l'énoncé de ce résultat.

COROLLAIRE 8. — *Soit $n \geq 2$. $\overline{r} \in \mathrm{U}(\mathbb{Z}_n)$ si et seulement s'il est un générateur de du groupe $(\mathbb{Z}_n, +)$.*

Démonstration du théorème 7. Supposons d'abord que $\overline{r}$ soit inversible. Nous montrons que n'importe quel représentant μ de $\overline{r}$ est premier avec n. Par définition d'un élément inversible, il existe $\overline{s} \in \mathbb{Z}_n$ avec $\overline{s} \neq \overline{0}$ tel que $\overline{\mu} \cdot \overline{s} = \overline{r} \cdot \overline{s} = \overline{1}$ autrement dit $\overline{\mu s - 1} = \overline{0}$ de sorte que n divise $\mu s - 1$ ou $\mu s - 1 = kn$ soit $\mu s - kn = 1$ ce qui implique, d'après le théorème de Bézout I::6, que μ et n sont premiers entre eux. La réciproque est pratiquement identique, si r est un représentant quelconque de $\overline{r}$ premier avec n alors il existe des entiers u et v tels que $ur + vn = 1$ d'où nous tirons $\overline{u} \cdot \overline{r} = 1$ qui donne l'inversibilité de $\overline{r}$. ■

Exemple 3. Le tableau suivant montre la liste des éléments inversibles et des inverses de $\mathbb{Z}_n$ pour quelques valeurs de n.

n	(x, x^{-1})
2	$(\overline{1}, \overline{1})$
3	$(\overline{1}, \overline{1})$, $(\overline{2}, \overline{2})$
4	$(\overline{1}, \overline{1})$, $(\overline{3}, \overline{3})$
5	$(\overline{1}, \overline{1})$, $(\overline{2}, \overline{3})$, $(\overline{3}, \overline{2})$, $(\overline{4}, \overline{4})$
6	$(\overline{1}, \overline{1})$, $(\overline{5}, \overline{5})$

Nous voyons que tous les éléments non nuls de $\mathbb{Z}_2$, $\mathbb{Z}_3$ et $\mathbb{Z}_5$ sont tous inversibles et ces anneaux forment donc des corps. La propriété sera vérifiée chaque fois que n est premier.

E. 85. Déterminer les éléments inversibles de $\mathbb{Z}_{12}$ et dans chaque cas donner les inverses.

E. 86. Est-il vrai que si $\overline{r}$ est un élément non inversible de $\mathbb{Z}_n$ alors il est un diviseur de 0.

E. 87. Trouver un exemple d'anneau unitaire A qui n'est pas égal à la réunion de ses éléments inversibles et de ses diviseurs de 0. s: p. 105 s:5

Il y a encore une condition importante équivalente à celle d'engendrer $(\mathbb{Z}_n, +)$ et d'être un élément de $\mathrm{U}(\mathbb{Z}_n)$. Soit f un morphisme de $(\mathbb{Z}_n, +)$ puisque

$$f(\overline{s}) = f(\underbrace{\overline{1} + \cdots + \overline{1}}_{s \text{ fois}}) = f(\overline{1}) + \cdots + f(\overline{1}) = \underbrace{\overline{a} + \cdots + \overline{a}}_{s \text{ fois}} = \overline{as} = \overline{a} \cdot \overline{s},$$

[TH 8]

où $\overline{a} = f(\overline{1})$. Cela montre que tous endomorphismes de $(\mathbb{Z}_n, +)$ sont de la forme $f : \overline{s} \in \mathbb{Z}_n \to \overline{sa} \in \mathbb{Z}_n$ où $\overline{a}$ est-un élément quelconque de $\mathbb{Z}_n$. Il est alors facile de déterminer lesquels, parmi ces morphismes, sont des automorphismes. Puisque nous allons d'un groupe fini dans lui-même, un morphisme sera bijectif s'il est injectif c'est-à-dire si son noyau se réduit à l'élément neutre (de $(\mathbb{Z}_n, +)$). Ici, $f(\overline{s}) = \overline{0}$ équivaut à $\overline{sa} = \overline{0}$ c'est-à-dire à n divise sa où s et a sont deux représentants quelconque de $\overline{s}$ et $\overline{a}$. Si a est premier avec n alors $n|sa$ entraîne $n|s$ ou $\overline{s} = 0$ et l'application est bien injective. Par contre, si n et a ont le diviseur d, $1 < d < n$ en commun alors, posant $s = n/d$, $\overline{s}$ est non nul et nous avons $f(\overline{s}) = \overline{(a/d)n} = \overline{0}$ et l'application n'est pas injective.

THÉORÈME 9. — *Le groupe* $(\mathrm{U}(\mathbb{Z}_n), \cdot)$ *est isomorphe au groupe* $(\mathsf{Aut}(\mathbb{Z}_n, +), \circ)$.

Démonstration. Nous montrons que l'application Ψ qui a $\overline{a} \in \mathrm{U}(\mathbb{Z}_n)$ associe le morphisme $\Psi_{\overline{a}}$ défini par

$$\Psi_{\overline{a}}(\overline{s}) = \overline{a} \cdot \overline{s}, \quad \overline{s} \in \mathbb{Z}_n,$$

est un isomorphisme entre $(\mathrm{U}(\mathbb{Z}_n), \cdot)$ et $(\mathsf{Aut}(\mathbb{Z}_n, +), \circ)$. La discussion précédente montre que Ψ prend bien ses valeurs dans $\mathsf{Aut}(\mathbb{Z}_n, +)$ et qu'elle est surjective. Il reste à montrer que c'est bien un morphisme puis qu'il est injectif. La démonstration de ces deux points est laissée en exercice. [s:6] ■ s: p. 105

E. 88. Les groupes $(\mathbb{Z}_n, +)$ et $\mathsf{End}(\mathbb{Z}_n, +)$ sont-ils isomorphes ?

3.3 Le corps $\mathbb{Z}_p$, p premier

Le théorème précédent nous permet de trouver les premiers (et plus importants) exemples de corps finis (ayant un nombre fini d'éléments).

THÉORÈME 10. — *Si* $p \geq 2$ *est un nombre entier premier alors* $(\mathbb{Z}_p, +, \cdot)$ *est un corps (commutatif).*

La condition d'être premier est en réalité nécessaire et suffisante puisque nous avons vu au dessus que si n n'est pas premier alors $\mathbb{Z}_n$ n'est pas intègre ce qui rend impossible qu'il soit un corps.

Démonstration. Nous devons vérifier que si $\overline{r} \in \mathbb{Z}_p$ alors $\overline{r}$ est inversible. Or cela sera le cas, d'après le théorème 7, si r est premier avec p. Or p étant premier, r est premier avec p à moins qu'il ne soit un multiple de p ce qui impossible puisque $\overline{r} \neq \overline{0}$. ■

Exemple 4. Le corps fini le plus simple est $(\mathbb{Z}_2, +, \cdot)$. Il est aussi très utile, particulièrement dans les mathématiques appliquées à l'informatique. Nous avons $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ et les tables sont

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

,

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

.

E. 89. Résoudre l'équation $x^2 = \bar{1}$ dans $\mathbb{Z}_5$ et dans $\mathbb{Z}_7$.

Voici une conséquence du théorème en arithmétique.

THÉORÈME 11. — *Soient p premier et $a \in \mathbb{Z}$ tel que $p \not| a$. On a toujours*

$$a^{p-1} \equiv 1 \quad [p].$$

Autrement dit p divise toujours $a^{p-1} - 1$ dès lors qu'il ne divise pas a.

Démonstration. Dire que $a^{p-1} \equiv 1 \quad [p]$ c'est dire que $\overline{a^{p-1}} = \bar{1}$ dans le corps $\mathbb{Z}_p$, ou encore en utilisant les propriétés des classes, $\bar{a}^{p-1} = \bar{1}$. Maintenant puisque p ne divise pas a, $\bar{a}$ est différent de $\bar{0}$ et donc appartient au groupe des éléments inversibles $(\mathbb{Z}_p)^\star$ qui est un groupe de cardinal $p-1$. Donc, d'après le corollaire I::27 du théorème de Lagrange, $\bar{a}^{p-1} = \bar{1}$. ■

COROLLAIRE 12. — *Si p est un nombre premier et a un entier quelconque alors p divise $a^p - a$.*

s: p. 105 E. 90. Démontrer le corollaire[s:7].

HISTOIRE 2. — Ce théorème, connu sous le nom de *Petit théorème de Fermat* a été énoncé par Pierre de Fermat en 1640. La formulation était la suivante

> «Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous multiple du nombre premier donné -1 ; et après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même la question.»

Si le lecteur réussi à le traduire en langage moderne, il verra que l'énoncé de Fermat affirme un peu plus que le théorème 11. C'est un exercice simple de démontrer cette information supplémentaire. Fermat cependant n'accompagnait pas son énoncé d'une démonstration. La première démonstration est semble-t-il due à L. Euler (1707-1783) qui l'obtint en 1736, ainsi que la généralisation donnée au paragraphe suivant établie en 1760, par des méthodes assez techniques et assez éloignées de celles que nous donnons ici. Le lecteur intéressé pourra consulter (**?**, Chap. VI) pour une présentation de la méthode d'Euler et des informations plus détaillées sur son histoire.

E. 91. Cette exercice propose une autre démonstration du petit théorème de Fermat. Considérons l'application $\psi : \mathbb{Z}_p \to \mathbb{Z}_p$ définie par $\psi(x) = \bar{a} \cdot x$. Montrer que ψ est une bijection et en déduire d'abord que

$$\prod_{x \in (\mathbb{Z}_p)^\star} x = \prod_{x \in (\mathbb{Z}_p)^\star} \bar{a} \cdot x,$$

s: p. 105 puis le théorème de Fermat. [s:8]

3.4 L'indicatrice d'Euler

La démonstration du théorème 11 repose entièrement sur le théorème de Lagrange et n'utilise que la structure de groupe de $(\mathbb{Z}_p)^\star$. Or nous avons vu $(\mathbb{Z}_n)^\star$ est un groupe,

que n soit premier ou non. Appelons $\phi(n)$ l'ordre de ce groupe. Le théorème 7 nous dit que

$$\phi(n) = \text{card}\{j \in \{1,\dots,n-1\} \ : \ n \text{ et } j \text{ sont premiers entre eux}\}.$$

Nous avons $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 5$, $\phi(6) = 1$ et pour tout nombre premier p, $\phi(p) = p-1$. Le raisonnement utilisé dans la démonstration du théorème 11 conduit immédiatement au suivant, connu comme le théorème de Fermat généralisé.

THÉORÈME 13. — *Soit n un entier positif et a un entier premier avec n. On a toujours*

$$a^{\phi(n)} \equiv 1 \quad [n].$$

L'application ϕ s'appelle l'**indicatrice d'Euler**. Le théorème précédent montre l'intérêt qu'il y a à connaître les valeurs de ϕ. Celles-ci peuvent se déduire, au moins pour des valeurs de n pas trop grandes des deux règles calculs qui suivent.

THÉORÈME 14. — *Si p est un nombre premier et $s \in \mathbb{N}^\star$ alors $\phi(p^s) = p^s - p^{s-1}$.*

Démonstration. Un entier de $\{1,\dots,p^s-1\}$ ne sera pas premier avec p^s si et seulement s'il est un multiple de p. Ces multiples sont au nombre de $p^{s-1}-1$, ce sont les entiers kp avec $1 \le k \le p^{s-1}-1$. Il suit que $\phi(p^s) = (p^s-1) - (p^{s-1}-1) = p^s - p^{s-1}$. ■

THÉORÈME 15. — *Si m et n sont deux entiers premiers entre eux* ($\text{pgcd}(m,n) = 1$) *alors $\phi(mn) = \phi(m)\phi(n)$.*

Une fonction satisfaisant cette propriété est dite **multiplicative**. La démonstration du théorème sera proposée en exercice.

3.5 Sous-corps premiers

Nous connaissons déjà suffisamment d'éléments sur la théorie des corps pour décrire en quelque sorte le coeur de n'importe quel corps, son **sous-corps premier**. Etant donné un corps K, le sous-corps premier $P(K)$ est le plus petit sous-corps de K. En d'autres mots, c'est l'intersection de tous les sous-corps de K. Puisque tout sous-corps contient l'unité 1_K, $P(K)$ n'est autre que le sous-corps de K engendré par l'unité,

$$P(K) = (1_K).$$

S'agissant d'un corps, s'il contient 1_K, il contiendra aussi $n1_K$, $n \in \mathbb{Z}$ et les inverses de ces éléments lorsqu'ils différent de 0_K. Deux cas de figures sont possibles.

(i) Soit $(n1_K) \neq 0_K$ pour tout $n \in \mathbb{Z}^\star$,

(ii) soit il existe $s \in \mathbb{N}^\star$ pour lequel $s1_K = 0_K$. Ici, il est permis de supposer que $s \in \mathbb{N}$ puisque $n1_K = 0 \implies (-n)1_K = 0_K$.

Dans le premier cas, $P(K)$ contiendra tous les éléments de la forme $(n1_K)\cdot(m1_K)^{-1}$, $(n,m)\in\mathbb{Z}\times\mathbb{Z}^\star$, dont nous vérifions aisément qu'ils forment un sous-corps de K. Il suit que

$$P(K)=\{(n1_K)\cdot(m1_K)^{-1}\ :\ (n,m)\in\mathbb{Z}\times\mathbb{Z}^\star\}.$$

Si la seconde alternative se produit, l'ensemble des entiers $\{n\in\mathbb{N}^\star\ :\ n1_k=0\}$ est non vide et il contient par conséquent un plus petit élément. Appelons q ce plus petit élément. Il ne peut être qu'un nombre premier car si q se laisse factoriser $q=q_1q_2$ avec chacun des q_i plus plus petit que q alors

$$0_K=(q1_K)=(q_11_K)\cdot(q_21_K), \tag{3.4}$$

et puisque K, comme tout corps, est intègre, nous en tirons $q_11_K=0_K$ ou $q_21_K=0_K$ ce qui contredit la minimalité de q. Observons que le nombre premier q est supérieur ou égal à 2 (puisque $1_K=0_K$ est impossible). Nous avons alors

$$P(K)=\{m1_K\ :\ m=0,\dots,q-1\}. \tag{3.5}$$

La démonstration que $P(K)$ est effectivement un sous-corps de K est laissée en exercice. Ces considérations conduisent à la définition de la **caractéristique** d'un corps. Lorsque le sous-corps premier de K est donné par (3.4) nous disons que K est un corps de caractéristique nulle. Lorsqu'au contraire $P(K)$ est donné par (3.5), nous disons que q est la caractéristique de K. Remarquons que si K est se caractéristique $q>0$, nous avons $qx=0_K$ pour tout $x\in K$,

$$\mathrm{car}(K)=q\implies qx=0_K,\quad x\in K. \tag{3.6}$$

En effet $qx=q(1_Kx)=(q1_K)x=0_K$. Lorsqu'il n'est pas nécessaire de spécifier la valeur de $q\geq 2$, nous dirons simplement que nous avons à faire à un corps de caractéristique positive.

THÉORÈME 16. — *Tout sous-corps premier est isomorphe soit à $(\mathbb{Q},+,\cdot)$ soit à un corps $(\mathbb{Z}_q,+,\cdot)$ où q est un nombre premier.*

Démonstration. Lorsque K est de caractéristique nulle, nous utilisons l'application $x: n/m\in Q\to(n1_K)/(m1_K)^{-1}\in P(K)$ tandis que lorsque K est de caractéristique q, nous utilisons l'application $\bar{s}\in\mathbb{Z}_q\to s1_K\in P(K)$. La démonstration du fait que ces applications sont bien définies et sont des isomorphismes est laissée en exercice. ■

Tous les corps rencontrés jusqu'ici sont de caractéristique nulle à l'exception de $\mathbb{Z}_p$ qui est de caractéristique p. Nous rencontrerons plus loin d'autres corps de caractéristiques p. Un corps contenant un nombre fini d'éléments est nécessairement de caractéristique positive mais nous verrons qu'il existe des corps de caractéristique positive contenant un nombre infini éléments. L'algèbre des corps de caractéristique positive est sensiblement différente de celle des corps de caractéristique nulle. Le résultat suivant donnera une illustration de ces différences.

THÉORÈME 17. — *Dans un corps (commutatif) K de caractéristique $q>0$, la relation suivante est vraie*

$$(x+y)^q = x^q + y^q, \quad x,y \in K.$$

Puisque, le corps étant supposé commutatif, nous avons toujours $(xy)^q = x^q y^q$, le théorème précédent montre que l'application $x \to x^q$ est un endomorphisme de K. Remarquons que dans le cas du seul corps de caractéristique $q>0$ que nous connaissons jusqu'à présent, le théorème est une conséquence immédiate du théorème de Fermat qui dit que $x^q = x$ pour tout $x \in \mathbb{Z}_q$. Un autre corps (infini) de caractéristique q sera donné à la section 6.8 qui donnera un peu plus de substance à ce théorème. Un corps contenant 9 éléments est construit à l'exercice 118.

Démonstration. Nous pouvons utiliser la formule du binôme du Newton du théorème 2 pour écrire

$$(x+y)^q = \sum_{j=0}^{q} \binom{q}{j} x^j y^{q-j} = x^q + y^q + \sum_{j=1}^{q-1} \binom{q}{j} x^j y^{q-j}.$$

Compte tenu de (3.6), pour établir la relation du théorème, il suffit d'établir que les entiers $N = \binom{q}{j}$ sont divisibles par q pour tout $j \in \{2,\dots,q-1\}$. Pour s'assurer de cette propriété, remarquons que puisque j est non nul

$$j!N = q(q-1)\cdots(q-j+1).$$

Piusque q divise le terme de droite, il divise celui de gauche. Cependant, $q|j!N \implies q|N$ car j est plus petit que q et que celui-ci est un nombre premier. La propriété $q|\binom{q}{j}$ est établie et cela achève la démonstration du théorème. ■

§ 4. IDÉAUX D'UN ANNEAU COMMUTATIF. ANNEAUX QUOTIENT

4.1 Vers la définition d'un idéal

Soient $(A,+,\cdot)$ un anneau commutatif et I un sous-groupe de $(A,+)$. Puisque ce dernier est un groupe commutatif, I est un sous-groupe distingué de A et nous pouvons considérer le groupe quotient $(A/I,+)$. Les éléments de A/I sont de la forme $\mathtt{C} = \mathbf{cl}(a) = a+I = \{a+h : h \in I\}$ et la loi $+$ (précédemment notée $\overline{+}$) sur A/I vérifie

$$\mathbf{cl}(a) + \mathbf{cl}(b) = \mathbf{cl}(a+b)$$

et, plus généralement,

$$\underset{\substack{\uparrow \\ \text{loi } + \text{ dans } A/I}}{\mathtt{C}_1 + \mathtt{C}_2} = \mathbf{cl}\left(\begin{array}{c} \text{n'importe quel} \\ \text{représentant de } \mathtt{C}_1 \end{array} \underset{\nearrow \\ \text{loi } + \text{ dans A}}{+} \begin{array}{c} \text{n'importe quel} \\ \text{représentant de } \mathtt{C}_2 \end{array} \right).$$

Il est bien naturel de vouloir définir une loi de produit sur A/I en utilisant la règle

$$\begin{array}{ccccc} A/I \times A/I & \longrightarrow & A/I & & \\ (\mathtt{C}_1\,,\,\mathtt{C}_2) & \longmapsto & \mathbf{cl}\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_1\end{array} \cdot \begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_2\end{array}\right) & \cdot\,: & (4.1) \\ \uparrow & & \nearrow & & \\ \text{loi produit dans } A/I & & \text{loi produit dans A} & & \end{array}$$

Pour que cette définition soit consistante, c'est-à-dire, qu'il soit effectivement possible de choisir un représentant quelconque sans changer le résultat, il sera nécessaire que le sous-groupe I satisfasse une condition que nous allons mettre en évidence maintenant. Nous devons pouvoir être sûrs que si $\mathbf{cl}(a) = \mathbf{cl}(b)$ et $\mathbf{cl}(a') = cl(b')$ alors $\mathbf{cl}(aa') = \mathbf{cl}(bb')$. Les hypothèses nous disent que $a = b + i$ et $a' = b' + i'$ avec $i, i' \in I$ de sorte que $aa' = bb' + ib' + i'b + ii'$. Pour avoir $\mathbf{cl}(aa') = \mathbf{cl}(bb')$, nous devons pouvoir affirmer que $ib' + i'b + ii' \in I$. cette condition sera satisfaite si l'ensemble I possède la propriété que tout élément de A multiplié par un élément de I est encore un élément de I. Nous sommes ainsi conduit à poser la définition suivante. Un sous-groupe I de $(A,+)$ est appelé un **idéal** de l'anneau $(A,+,\cdot)$ lorsque pour tout $a \in I$ et tout $i \in I$, nous avons $ai \in I$. Nous pourrions dire que les idéaux sont les sous-groupes de (A,+) qui sont absorbants pour la multiplication. Avec cette terminologie, la discussion précédente nous a permis d'établir le théorème suivant. Remarquons que l'ensemble réduit à l'élément neutre 0_A est toujours un idéal de A.

THÉORÈME 18. — *Si I est un idéal de $(A,+,\cdot)$ alors la relation (4.1) définit une loi interne sur A/I.*

E. 92. Pour que la propriété de consistance soit satisfaite, nous avons dit qu'il suffisait que A soit un idéal. Montrer qu'en réalité la condition est aussi nécessaire. [s:9]

s: p. 105

Le démonstration du théorème suivant est bien simple. Elle est laissée en exercice.

THÉORÈME 19. — *Tout idéal I de A est un sous-anneau de A.* [s:10]

s: p. 105

Nous verrons dans la section suivante des exemples de sous-anneaux qui ne sont pas des idéaux.

4.2 Exemple d'idéaux

(4.2.1) Idéaux principaux. Il a profusion d'idéaux dans presque tous les anneaux. Prenons en effet un a un élément non nul de $(A,+,\cdot)$ alors l'ensemble des multiples de a, que nous noterons $\langle a \rangle$,

$$\langle a \rangle = \{xa \,:\, x \in A\}$$

forme un idéal de A. Il est appelé l'**idéal principal** engendré par a. Ces idéaux forment la classe la plus simple d'idéaux et c'est la seule qui jouera un rôle substantiel dans ce chapitre.

E. 93. Soit I un idéal de A et $a \in A$. Montrer que $\langle a \rangle \subset I$. [s:11] s: p. 106

E. 94. Soient a et b deux éléments non nuls d'un anneau intègre commutatif unitaire A. Montrer que $\langle a \rangle = \langle b \rangle$ si et seulement s'il existe $c \in A^*$ tel que $a = cb$. [s:12] s: p. 106

Lorsque tous les idéaux de A sont des idéaux principaux, nous disons que l'anneau A est **principal**. Les anneaux principaux sont rares mais ils jouent un rôle essentiels à commencer par le suivant.

THÉORÈME 20. — *Les idéaux de $(\mathbb{Z},+,\cdot)$ sont les ensembles $n\mathbb{Z}$, $n \in \mathbb{N}$. En particulier $\mathbb{Z}$ est un anneau principal.*

Démonstration. Soit I un idéal de $(\mathbb{Z},+,\cdot)$. Puisque I est en particulier un sous-anneau de $\mathbb{Z}$, en vue de ((1.5.1)), il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z} = \langle n \rangle$. Réciproquement tout ensemble $\langle n \rangle$ est un idéal de $\mathbb{Z}$. ■

(4.2.2) Idéaux de type fini. Ce que nous avons fait avec un seul éléments peut-être avec une famille finie d'éléments. Ainsi, si $a_1, \ldots, a_s$ sont s éléments de A, nous posons

$$\langle a_1, a_2, \ldots, a_s \rangle = \{x_1a_1 + x_2a_2 + \cdots x_sa_s \ : (x_1, x_2, \ldots, x_s) \in A^s\}.$$

Cet ensemble est un idéal de A que nous appelons l'idéal engendré par $a_1, \ldots a_s$. Nous disons que c'est un idéal de type fini. Les idéaux principaux sont les idéaux de types finis les plus simples. Ces idéaux jouent un rôle fondamental dans l'étude des anneaux de polynômes de plusieurs variables lesquels sont au coeur d'une branche maîtresse des mathématiques, la géométrie algébrique dont l'objet est l'étude des ensembles définis par des équations polynomiales, dont les exemples les plus élémentaires sont les coniques (ellipse, hyperbole) dans le plan.

(4.2.3) Noyau des morphismes.

THÉORÈME 21. — *Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Le noyau* $\ker f$ *est un idéal de A.*

Démonstration. Nous savons déja que $\ker f$ est un sous-groupe de $(A,+)$. Ensuite si $x \in A$ et $a \in \ker f$ alors $f(xa) = f(x)f(a) = f(x)0_A = 0_A$ ce qui montre que $xa \in \ker f$, ce qu'il fallait montrer. ■

E. 95. Montrer que si K est un corps alors K contient seulement deux idéaux : le singleton $\{0_K\}$ et K lui-même.

Cet exercice fournit quantité de sous-anneaux qui ne sont pas des idéaux, par exemple $\mathbb{Z}$ est un sous-anneau de $(\mathbb{Q},+,\cdot)$ mais n'est pas un idéal de $\mathbb{Q}$.

NOTE 13. — Il n'est pas difficile de définir un idéal dans un anneau non commutatif (c'est simplement inutile pour nous). Dans un anneau non commutatif, nous devons exiger que xa et ax soient des éléments de I dès que $x \in A$ et $a \in I$, la première condition n'entraînant pas la seconde (trouver un exemple[s:13]). s: p. 106

4.3 Anneaux quotients

THÉORÈME 22. — *Soit $(A,+,\cdot)$ un anneau commutatif et I un idéal de A alors $(A/I,+,\cdot)$ où $+$ et $\cdot$ sont définies comme ci-dessus est un anneau commutatif. Si A est unitaire alors A/I est aussi unitaire et $1_{A/I} = \mathbf{cl}(1_A)$.*

Comme dans le cas des groupes et celui de $\mathbb{Z}_n$, nous noterons généralement la classe de a par $\bar{a}$ plutôt que $\mathbf{cl}(a)$. On trouve aussi dans la littérature la notation $\dot{a}$.

Démonstration. Toutes les propriétés requises découlent des relations $\mathbf{cl}(a+b) = \mathbf{cl}(a) + \mathbf{cl}(b)$ et $\mathbf{cl}(a\cdot b) = \mathbf{cl}(a)\cdot\mathbf{cl}(b)$. ■

THÉORÈME 23. — *Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Il existe un (unique) isomorphisme d'anneau $\gamma : A/\ker f \to f(A)$ tel que $f = \gamma \circ s$ où s est la surjection canonique de A sur $A/\ker f$. Nous avons donc*

$$\frac{A}{\ker f} \simeq f(A).$$

Démonstration. Le théorème d'isomorphisme I::32 donne toutes les propriétés énoncés exceptée le fait que γ soit un isomorphisme d'anneau plutôt que simplement de groupe. La condition manquante est $\gamma(\bar{a}\cdot\bar{b}) = \gamma(\bar{a})\cdot\gamma(\bar{b})$ où, comme il montré dans la démonstration du théorème I::32, $\gamma(\bar{a}) = f(a)$. La relation découle alors de la relation

$$\gamma(\bar{a}\cdot\bar{b}) = \gamma(\mathbf{cl}(a\cdot b)) = f(ab) = f(a)f(b) = \gamma(\bar{a})\gamma(\bar{b}). \quad ■$$

Exemple 5. Soit K un corps de caractéristique $q \geq 2$. L'application $f : s \in \mathbb{Z} \to s1_K \in K$ est un morphisme d'anneau dont le noyau est $q\mathbb{Z}$. En effet, $f(s) = 0 \implies s1_F = 0$ et écrivant $s = qr + t$ avec $t \in \{0,\ldots,q-1\}$, il vient $0_K = r(q1_K) + t1_K = t1_K$ et comme q est le plus petit entier positif satisfaisant $q1_K = 0$ il vient $t = 0$ et $s \in q\mathbb{Z}$. Le théorème d'isomorphisme ci-dessus nous dit que $\mathbb{Z}/q\mathbb{Z} = (\mathbb{Z}_q)$ est isomorphe à $f(\mathbb{Z})$. Puisque q est premier $\mathbb{Z}_q$ est un corps et donc aussi $f(\mathbb{Z}_q)$. Tout corps contenant 1_K contiendra $f(\mathbb{Z})$ et il s'ensuit que le sous-corps premier $P(K)$ est $f(\mathbb{Z}_q)$.

§ 5. LE CORPS DES FRACTIONS D'UN ANNEAU INTÈGRE

5.1 Introduction

Chaque fois que les mathématiciens se sentirent à l'étroit, dans un certain sens, dans un ensemble de nombres, ils imaginèrent une nouvelle famille de nombre dans laquelle ils apprirent petit à petit à se mouvoir jusqu'à ce qu'ils en maîtrisent parfaitement le maniement et que d'autres en construisent une définition – a posteriori – qui répondaient

aux canons de leur époque. Le prototype de ce processus d'extension de l'espace numérique est celui qui commande le passage de l'ensemble des entiers ($\mathbb{Z}$) à celui des fractions rationnelles ($\mathbb{Q}$). Le problème, c'est qu'il n'est en général pas possible de résoudre des équations de la forme $bx = a$ dans $\mathbb{Z}$. De nombreuses raisons pratiques nécessitaient pourtant la résolution de ces questions, typiquement des questions de partages de biens, et la solution d'un telle équation avait bien souvent une signification physique très claire à la mesure de laquelle il suffisait d'attribuer en somme une étiquette, disons l'étiquette (b,a) pour la solution de $bx = a$. Simplement le calcul sur ces nouveaux nombres étaient loin d'être évident et il est encore aujourd'hui bien loin de l'être pour les collégiens. Remarquons d'abord que, puisque l'équation $0x = a$ ne saurait avoir de solution unique, il fallait exclure que b puisse prendre la valeur nulle. Ensuite, puisque l'équation $\alpha bx = \alpha a$ doit certainement posséder la même solution que $ax = b$, il fallait que le symbole $(\alpha a, \alpha b)$ désigne le même objet que (a,b). Des règles de calcul strictes sont aussi imposées par la signification de notre étiquette. Si (a,b) est solution de $bx = a$ et (c,d) est solution de $dy = c$ alors xy, à supposer que nous puissions former un produit, devra être solution de $(ab)z = cd$ de sorte qu'il faudra poser $(a,b)\cdot(c,d) = (ab,cd)$. De la même manière, si $bx = a$ et $dx = c$ alors, en multipliant la première équation par d et la seconde par b puis en additionnant les deux relations obtenues, il vient $bd(x+y) = ad+bc$ de sorte qu'il nous faudra poser $(a,b)+(c,d) = (ad+bc,bd)$. Il n'est nullement évident qu'avec cette dernière, nous obtenons un ensemble de règles complets et non plus que celles-ci sont compatibles entre elles. Nous allons voir dans cette partie et dans un cadre plus général que la réponse est positive. Peut-être le lecteur doute-t-il que le problème que nous évoquons ici soit en rapport avec le sujet de ce chapitre. En réalité, si a et b sont des éléments d'un anneau A, avec $b \neq 0_A$, la solution de $bx = a$ sera donnée par $x = b^{-1}a$ si $b \in A^\star$ et si b n'est pas inversible dans A, il pourrait bien l'être dans un corps Q contenant A, tout comme 2 n'est pas inversible dans $\mathbb{Z}$ mais l'est dans $\mathbb{Q}$. Etant donné un anneau commutatif intègre et unitaire, le problème consiste ainsi à construire un corps Q qui contiendra A. Si nous voulons, comme il est naturel, agrandir notre ensemble A de la manière la plus économique possible, nous devrons proposer un corps Q le plus petit possible.

5.2 Construction

Soit A un anneau (commutatif unitaire) intègre. Suivant le raisonnement esquissé dans la partie précédente, nous considérons le produit cartésien $A\times A^0$ où $A^0 = A/\{0_A\}$, et définissons la relation $\mathfrak{R}$ sur $A\times A^0$ par

$$(a,b)\,\mathfrak{R}(c,d) \quad \text{si} \quad ad-bc = 0, \quad (a,b),;(c,d) \in A\times A^0.$$

THÉORÈME 24. — *Le relation $\mathfrak{R}$ est une relation d'équivalence sur $A\times A^0$.*

La vérification de cette propriété est laissée en exercice. Limitons-nous à observer qu'il s'agit d'une relation d'équivalente dont la nature est bien différente de celle que

nous avons rencontrées dans les parties précédentes. La première différence fondamentale, c'est que cette relation n'est pas définie sur A mais bien sur le produit cartésien $A \times A^0$ dans lequel l'ordre des ensembles a toute son importance.

La classe d'équivalence d'un élément $(a,b) \in A \times A^0$ sera notée $\frac{a}{b}$. Nous avons donc

$$\mathbf{cl}_{\mathfrak{R}}((a,b)) := \frac{a}{b}.$$

C'est l'ensemble de ces classes d'équivalence que nous noterons $Q(A)$, i.e.

$$Q(A) := \left\{ \frac{a}{b} : a \in A, b \in A^0 \right\}.$$

Nous allons définir des lois $+$ et $\cdot$ sur $Q(A)$. Si la nature des classes d'équivalence est différente de celle que nous avons considérées précédemment, se posera exactement la même question de la consistance des définitions. Si (a,b) est n'importe quel représentant de $\mathtt{C}_1$ et (c,d) n'importe quel représentant de $\mathtt{C}_2$ alors nous posons

$$\mathtt{C}_1 + \mathtt{C}_2 := \mathbf{cl}(ad+bc, bd) \tag{5.1}$$
$$\mathtt{C}_1 \cdot \mathtt{C}_2 := \mathbf{cl}(ac, bd). \tag{5.2}$$

Autrement dit,

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}, \tag{5.3}$$
$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}. \tag{5.4}$$

Ces formules sont les seules possibles comme le montre le raisonnement présenté dans l'introduction. Pour montrer la consistance de la définition que nous venons de poser, nous devons garantir l'indépendance du résultat quant au choix des représentants. Précisément, si

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{et} \quad \frac{c}{d} = \frac{c'}{d'}$$

alors il s'agit de vérifier que

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \quad \text{et} \quad \frac{ab}{cd} = \frac{a'b'}{c'd'}.$$

Nous laissons encore au lecteur le soin d'effectuer les calculs nécessaires.

THÉORÈME 25. — *Les relations (5.1) et (5.2) définissent des lois internes sur $Q(A)$.*

THÉORÈME 26. — *$(Q(A),+,\cdot)$ est un corps commutatif avec $0_{Q(A)} = \frac{0}{1}$ et $1_{Q(A)} = \frac{1}{1}$.*

[TH 26]

Le corps $Q(A)$ s'appelle le **corps des fractions** de l'anneau intègre A.

Nous voulions aussi que notre corps $(Q(A)$ contiennent A – on dit qu'il forme une *extension* de l'anneau A. Les éléments de $Q(A)$ étant des classes d'équivalence d'une relation sur $A \times A^0$, cela ne peut se faire que par l'entremise d'un artifice formel qui est généralement justifié par le raisonnement suivant. Considérons l'application

$$\varphi : a \in A \to (a, 1_A) \in Q(A).$$

Il est bien facile de vérifier que φ est un morphisme d'anneaux unitaires et qu'il est injectif, de sorte que A est isomorphe à son image $\varphi(A)$. On décide alors de confondre – certains disent d'identifier – A et son image [*], de sorte que a est confondu avec $\mathbf{cl}(a, 1_A) = \frac{a}{1_A}$ pour écrire $a = \frac{a}{1_A}$. Cette identification étant faite, nous pouvons dire que le neutre et l'unité de $Q(A)$ sont les mêmes que le neutre et l'unité de A.

Exemple 6. Puisque nous avons exactement reproduit le passage de $\mathbb{Z}$ à $\mathbb{Q}$, le lecteur ne sera pas surpris de lire que $Q(\mathbb{Z}) = \mathbb{Q}$. Un autre exemple de coprs de fraction sera présenté plus bas après que nous aurons défini les anneaux de polynômes.

5.3 La minimalité de $Q(A)$

Au moment de poser le problème, nous demandions de construire le plus petit corps contenant A. Si la propriété était comprise dans un sens étroit, il faudrait établir que si K est un corps contenant A alors $Q(A) \subset K$. Cependant comme il est évident à la lecture de la construction de $Q(A)$ la notion d'inclusion lorsqu'elle concerne les structures algébriques n'a pas de sens très profond. L'anneau A n'a lui-même été vu comme un sous-ensemble de $Q(A)$ que grâce à l'intervention d'un morphisme bien choisi. Nous devons établir une condition de minimalité à morphisme près comme dans le théorème suivant.

THÉORÈME 27. — *Soient A un anneau commutatif intègre et unitaire et K un corps. S'il existe un morphisme d'anneaux injectif $\phi : A \to K$ alors il existe un morphisme $\Psi : Q(A) \to K$ tel que la restriction de ψ à A coïncide avec ϕ.*

Nous disons que tout morphisme injectif de A dans K se prolonge en un morphisme de $Q(A)$ dans K. Rappelons qu'en vue du théorème 4, tout morphisme d'un corps dans un autre est nécessairement injectif.

Démonstration. Il suffit de définir ψ sur $Q(A)$ par la relation $\Psi\left(\frac{a}{b}\right) = \phi(a)(\phi(b))^{-1}$. Comme d'habitude, cette définition soulève une question de consistance – (a,b) n'est qu'un représentant parmi tant de $\mathbf{cl}(a,b) = \frac{a}{b}$ – qu'il faudra régler avant tout calcul. ■

∗. Plusieurs autres identifications du même type seront faites par la suite, notamment en 6.2 et 6.7.

§ 6. ANNEAUX DE POLYNÔMES

6.1 Introduction

Les polynômes ou fonctions polynomiales sont certainement très familières à n'importe quel lecteur de ce texte. Elle s'obtiennent à partir des fonctions affines $x \mapsto ax+b$ par multiplication et additions successives pour arriver à une expression de la forme $x \mapsto a_n x^n + \cdots a_1 x + a_0$. Elles sont en particulier des combinaisons linéaires des fonctions, appelées monômes, $x \mapsto x^n$, $n = 0, 1, \ldots$. Le monôme $x \to x^n$ est dit de degré n et le degré d'une fonction polynomiale est le plus grand degré des monômes qui interviennent dans sa définition. Les a_i intervenant dans la définition sont appelés les coefficients de la fonction polynomiale. Ici, en parlant de la fonction $x \mapsto a_n x^n + \cdots a_1 x + a_0$, nous avons omis, ce qui est une erreur, de préciser l'ensemble de départ (et d'arrivée). Jusqu'à présent le lecteur à vraisemblablement travaillé uniquement avec des fonctions polynomiales définies pour un x réel ou complexe. Depuis la fin de ses études secondaires, le lecteur connaît ou sait redémontrer toutes les propriétés utiles des polynômes de degré au plus deux. Il connaît aussi le principe fondamental qui dit que deux fonctions polynomiales sont égales si et seulement si elles possèdent les mêmes coefficients. Or pour calculer $a_n x^n + \cdots a_1 x + a_0$, il suffit de disposer d'un produit (pour calculer x^i puis $a_i x^i$) et une somme pour additionner les termes $a_i x^i$. De telles fonctions sont donc naturellement définies pour x et les a_i dans un même anneau A (que nous supposerons toujours commutatif) et c'est naturellement la raison pour laquelle leur étude apparaît à ce moment précis du texte. Cependant, l'extension des ces fonctions à un anneau commutatif arbitraire soulève des difficultés qu'il était difficile de soupçonner lorsque nous nous limitions aux nombres réels ou complexes. Considérons par exemple la fonction polynomiales définie sur le corps $(\mathbb{Z}_2, +, \cdot)$ par $p : x \in \mathbb{Z}_2 \to \bar{1}x^3 + \bar{1}x$. Nous avons $p(\bar{0}) = \bar{0}$ et $p(\bar{1}) = \bar{0}$ de sorte que p est la fonction constante égale à $\bar{0}$ et coïncide donc avec la fonction polynomiale $N : x \in \mathbb{Z}_2 \to \bar{0} \in \mathbb{Z}_2$. La règle fondamentale qui nous disait que les coefficients déterminaient de manière unique la fonction polynomiale ne demeure donc plus et nous sommes mis devant l'alternative suivante : renoncer au principe ou modifier la définition en sorte qu'il soit maintenu. Il se trouve qu'il est plus utile et plus fécond de conserver le principe. Il faut alors introduire une distinction entre les fonctions polynomiales et les polynômes lesquels seront exclusivement définis par la donnée de leurs coefficients. Une conséquence regrettable est que la définition devient formellement lourde et les vérifications des axiomes d'anneaux désagréables sans être instructives.

6.2 Définitions

Puisque nous voulons définir un polynôme par la seule donnée de ces coefficients, un polynôme doit être simplement définie comme la famille de ses coefficients. La position du coefficient jouant un rôle essentiel, ces familles devront être ordonnées. La difficulté

provient du fait que le nombre de coefficients, quoique toujours fini, varie en fonction du polynôme. Nous procéderons comme suit.

Soit A un anneau commutatif unitaire. Une suite d'éléments de A est une fonction s de $\mathbb{N}$ dans A. Elle est souvent représentée sous la forme $(s[0], s[1], s[2], \dots)$. Nous disons que cette suite est à support fini si $s[n] = 0$ pour n assez grand. Par exemple $(0_A, 1_A, 0_A, 0_A, \dots)$ est une suite à support fini puisque tous les termes sont nuls à partir du troisième. Nous appellerons **polynôme** à coefficients dans A toute suite de A à support fini. Cet ensemble est muni d'un loi d'addition $(+)$ et d'une loi produit $(\cdot)$ définies comme suit. Si p_1 et p_2 sont deux polynômes alors

(i) $p_1 + p_2$ est le polynôme défini par

$$(p_1 + p_2)[n] = p_1[n] + p_2[n], \quad n \in \mathbb{N}.$$

(ii) $p_1 \cdot p_2$ est le polynôme défini par

$$(p_1 \cdot p_2)[n] = \sum_{i=0}^{n} p_1[i] p_2[n-i], \quad n \in \mathbb{N}.$$

L'ensemble des polynômes sera provisoirement noté $\mathscr{P}_A$.

THÉORÈME 28. — *Soit $(A, +, \cdot)$ un anneau commutatif unitaire. $(\mathscr{P}_A], +, \cdot)$ est un anneau commutatif unitaire avec $0_{\mathscr{P}_A} = (0_A, 0_A, \dots)$ et $1_{\mathscr{P}_A} = (1_A, 0_A, 0_A, \dots)$.*

Nous voudrions aussi que nos polynômes contiennent les éléments de A aussi bien pour fournir l'analogue des fonctions polynomiales constantes que pour pouvoir multiplier un polynôme par un élément de A. Les éléments de $\mathscr{P}_A$ étant des suites, nous ferons à nouveau appel à l'artifice employé dans la section précédente lorsque voulions regarder A comme un sous-anneau du corps des fractions $Q(A)$. Ici, nous considérons l'application

$$\varphi : a \in A \to (a, 0_A, 0_A, \dots) \in \mathscr{P}_A.$$

Il est bien facile de vérifier que φ est un morphisme d'anneaux unitaires et qu'il est injectif, de sorte que A est isomorphe à son image $\varphi(A)$. On décide alors de confondre A et son image, de sorte que $a = (a, 0_A, 0_A, \dots)$. * Nous pouvons ainsi écrire

$$0_{A[X]} = 0_A \quad \text{et} \quad 1_{A[X]} = 1_A.$$

L'anneau A étant devenu un sous-anneau de $\mathscr{P}_A$, il est désormais possible de calculer le produit d'un élément de A par un polynôme. Nous appellerons X le polynôme particulier

$$X = (0_A, 1_A, 0_A, 0_A, \dots).$$

∗. Une autre identification du même type sera faite en 6.7.

La définition du produit de deux polynômes donne rapidement

$$X^2 = (0_A, 0_A, 1_A, 0_A, 0_A, \dots),$$

et plus généralement nous établissons par un raisonnement par récurrence que

$$X^n = (0_A, 0_A, \dots, 0_A, \underbrace{1_A}_{n+1\text{-ème place}}, 0_A, 0_A, \dots), \quad n \in \mathbb{N}^\star.$$

Nous avons alors

$$\begin{aligned} aX^n &= (a, 0_A, 0_A, \dots) \cdot (0_A, 0_A, \dots, 0_A, \underbrace{1_A}_{n+1\text{-ème place}}, 0_A, 0_A, \dots) \\ &= (0_A, 0_A, \dots, 0_A, \underbrace{a}_{n+1\text{-ème place}}, 0_A, 0_A, \dots). \end{aligned}$$

Il suit que si $P = (a_0, a_1, \dots, a_n, 0_A, 0_A, \dots)$ alors

$$\begin{aligned} P &= \sum_{i=0}^{n} (a_0, a_1, \dots, a_n, 0_A, 0_A, \dots) \\ &= \sum_{j=0}^{n} (0_A, 0_A, \dots, 0_A, \underbrace{a_j}_{j+1}, 0_A, 0_A, \dots) \\ &= \sum_{j=0}^{n} a_j X^j, \end{aligned}$$

et nous avons ainsi le théorème suivant.

THÉORÈME 29. — *Soit P un polynôme. Il existe $n \in \mathbb{N}$ et des éléments $a_0, a_1, \dots, a_n \in A$ tels que P s'écrive*

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{i=0}^{n} a_i X^i. \tag{6.1}$$

De plus si

$$P = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad P = \sum_{i=0}^{m} b_i X^i$$

sont deux écritures de $P \in \mathscr{P}_A$, avec disons $n \leq m$, alors nécessairement

$$a_i = b_i \text{ pour } 0 \leq i \leq n \text{ et } b_i = 0_A \text{ pour } n < i \leq m.$$

Cela signifie que, si nous enlevons les termes nuls inutiles, l'écriture $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ est unique.

[TH 29]

Le principe que nous voulions maintenir est donc intrinsèque à la définition d'un polynôme. Le théorème justifie aussi la notation $A[X]$ que nous utiliserons à partir de maintenant pour désigner l'ensemble des polynômes $\mathscr{P}_A$. Les éléments a_i dans (6.1) s'appelle les coefficients du polynôme P. Conformément à la définition d'un polynôme, nous avons $a_i = P[i]$. S'il faut être précis nous disons que a_i est de coefficient de X^i dans P. La plus grande valeur de n pour lequel a_n est non nul dans (6.1) s'appelle le **degré** de P et est noté $\deg(P)$. Le coefficient a_n correspondant s'appelle le **coefficient dominant** de P. Il est noté $\mathrm{dom}(P)$. Les polynômes particuliers $M_n = X^n (= 1_A X^n)$ sont des **monômes**. Très souvent, le polynôme P dans (6.1) sera aussi désigné comme le polynôme $P(X)$.

6.3 Le degré

Le polynôme X est parfois appelé l'**indéterminée** et l'anneau $A[X]$ est parfois décrit dans la littérature comme comme l'anneau des polynômes à coefficients dans A en l'indéterminée X.

THÉORÈME 30. — *Si $P, T \in A[X]$ $\deg(P+T) \leq \max(\deg(P), \deg(Q))$ et l'égalité a lieu dès lors que $\mathrm{dom}(P) \neq -\mathrm{dom}(Q)$.*

Avec la convention $\deg(0) = -\infty$, la formule (6.2) ci-dessus reste vraie lorsque $P = 0$ ou $Q = 0$.

THÉORÈME 31. — *Si l'anneau commutatif unitaire A est intègre alors $A[X]$ est aussi intègre et*

$$\deg(PT) = \deg(P) + \deg(T). \tag{6.2}$$

Démonstration. Soient $P_1 = \sum_{j=0}^{m_1} a_j X^j$ et $P_2 = \sum_{j=0}^{m_2} b_j X^j$ avec $a_{m_1} \neq 0$ et $b_{m_2} \neq 0$ deux polynômes non nuls. Nous montrons que le produit $P_1 \cdot P_2$ ne peut être nul ce qui établira l'intégrité de l'anneau. D'après la définition de l'anneau, nous avons

$$(P_1 \cdot P_2) = a_{m_1} a_{m_2} X^{m_1+m_2} + \sum_{j=0}^{m_1+m_2-1} (P_1 \cdot P_2)[j] X^j.$$

Puisque A est intègre et que les coefficients a_{m_1} et b_{m_2} sont non nuls leur prouit l'est aussi et $(P_1 \cdot P_2)$ est non nul puisqu'il a un coefficient non nul. La relation sur le degré découle aussi de l'expression ci-dessus. ■

THÉORÈME 32. — *Si l'anneau commutatif unitaire A est intègre alors $(A[X])^\star = A^\star$.*

Démonstration. L'inclusion $A^\star \subset (A[X])^\star$ est évidente. Nous montrons que si $\deg P \geq 1$ alors P n'est pas inversible. En effet, s'il l'était nous aurions une relation $PQ = 1_A$ qui entraînerait $\deg(P) + \deg(Q) = 0$ ce qui est impossible. ■

E. 96. Montrer que le résultat n'est plus sans l'hypothèse que A est intègre en trouvant un polynôme de degré 1 inversible dans $\mathbb{Z}_8[X]$. [s:14] s: p. 106

6.4 Polynômes et fonctions polynomiales

Ayant une idée claire de ce qu'est un polynôme, nous pouvons maintenant définir ce qu'est la fonction polynomiale associée à un polynomiale et mettre en évidence la différence entre les deux objets. Soit A un anneau commutatif unitaire. A tout polynôme $P \in A[X]$, $P = a_0 + a_1X + \cdots + a_nX^n$, nous faisons correspondre une fonction polynomiale $\tilde{P} : A \to A$ définie par

$$\tilde{P}(t) = a_0 + a_1t + \cdots + a_nt^n, \quad t \in A.$$

Par exemple, au polynôme nul $P = 0$ correspond la fonction constante nulle et au polynôme $P = X$ correspond la fonction identité de A. Plus généralement, au polynôme $(X-a)^n$ correspond la fonction $x \in A \to (x-a)^n$. Notant $\mathscr{F}(A)$ l'anneau des fonctions de A dans A (muni de la somme et du produit habituel des fonctions), voir ((1.5.2)).

THÉORÈME 33. — *L'application*

$$\mathbf{F}_A : \begin{array}{ccc} A[X] & \longrightarrow & \mathscr{F}(A) \\ P & \longmapsto & \tilde{P} \end{array}$$

est un morphisme d'anneau.

L'ensemble image $\mathbf{F}_A(A[X])$ est formé de toutes les fonctions polynomiales et c'est un sous-anneau de $\mathscr{F}(A)$. Le théorème d'isomorphisme nous dit alors que

$$A[X]/\ker \mathbf{F}_A \simeq \mathbf{F}_A(A[X])$$

qui signifie que les fonctions polynomiales sont en bijection avec les polynômes si et seulement si le noyau $\ker \mathbf{F}_A$ se réduit au polynôme nul. Nous mettrons plus loin en évidence le cas de figure le plus général pour lequel cette condition est satisfaite.

Nous noterons par la suite $P(t)$ plutôt que $\tilde{P}(t)$. C'est un raccourci commode mais auquel il faut prendre garde.

E. 97. Montrer que lorsque $A = \mathbb{Z}_2$ alors $\mathbf{F}_A(A[X])$ n'est constitué que de quatre éléments. Quels sont les éléments de $\ker \mathbf{F}_A$ [s:15].

s: p. 106

6.5 Division euclidienne des polynômes

THÉORÈME 34. — *Soient A un anneau commutatif unitaire intègre et $D \in A[X]$ un polynôme dont le coefficient dominant est inversible (i.e. $\mathrm{dom}(D) \in A^*$). Quel que soit $P \in A[X]$, il existe un et un seul couple de polynômes (Q,R) tels que*

$$\begin{cases} \deg R < \deg D \\ P = QD + R \end{cases}.$$

[TH 34]

Nous dirons que Q est **le quotient** de la division euclidienne de P par D et R est **le reste** et nous noterons

$$Q = \texttt{QUOT}(P, D) \quad \text{et} \quad R = \texttt{REST}(P, D).$$

Lorsque $P = QD$, c'est-à-dire $\texttt{REST}(P, D) = 0_A$, nous disons que D divise P et nous notons $D|P$.

Démonstration. Montrons d'abord que si le couple (Q,R) existe alors il est unique. Supposons que (Q_1,R_1) soit un autre couple satisfaisant les conditions demandées. Nous avons

$$QD+R = Q_1D+R_1 \implies (Q-Q_1)D = (R-R_1) \implies \deg((Q-Q_1)D) = \deg(R_1-R).$$

Donc $\deg(Q-Q_1)+\deg(D) = \deg(R-R_1)$. Puisque $\deg D > \deg R \geq \deg(R-R_1)$ la seule possibilité est que $\deg(Q-Q_1) = -\infty$ d'où $Q = Q_1$ qui entraîne aussi $R = R_1$.

L'existence du couple (Q,R) est immédiate dans le cas où $\deg P < \deg D$ car il suffit alors de choisir $Q = 0$ et $R = P$. Nous supposerons que $\deg P = \deg D + k$, $k \geq 0$ et montrons l'existence du couple (Q,R) par récurrence sur k.

Étape 1. Le cas $k = 0$.

Il suffit de prendre $Q = \text{dom}(P)(\text{dom}(D))^{-1}$ et $R = P - \text{dom}(P)(\text{dom}(D))^{-1}D$. Dans ce cas, nous avons bien $P = QD+R$ et $\deg R < \deg D$ car les termes de plus haut degré de P et de $\text{dom}(P)(\text{dom}(D))^{-1}D$ d'éliminent dans la définition de Q

Étape 2. Nous supposons que l'existence du couple (Q,R) a été établie pour $k = 0,\ldots,n$ et nous la montrons pour $k = n+1$.

Posant $m = \deg D$, nous avons

$$P = \text{dom}(P)X^{m+n+1} + P_1 \tag{6.3}$$

avec $\deg P_1 \leq m+n$. L'hypothèse de récurrence assure l'existence d'un couple (Q_1,R_1) tel que

$$P_1 = Q_1D+R_1, \quad \text{avec } \deg(Q_1) < \deg(D). \tag{6.4}$$

D'autre part, reprenant la même idée que dans la première étape, nous pouvons écrire

$$\text{dom}(P)X^{m+n+1} = \text{dom}(P)\text{dom}(D)^{-1}D + T, \tag{6.5}$$

où $T = \text{dom}(P)X^{m+n+1} - \text{dom}(P)(\text{dom}(D))^{-1}D$ est un polynôme de degré au plus $m-1$ car les termes de plus haut degré s'éliminent dans la différence. En reportant les relation (6.4) et (6.5) dans (6.3) nous obtenons

$$P = (Q_1 + \text{dom}(P)\text{dom}(D)^{-1})D + (P_1 + T)$$

et comme chacun des polynômes P_1 et T a un degré moindre que celui de D le relation recherchée est établie. ■

Exemple 7. Pour tout $a \in A$ et tout $P \in A[X]$, le reste de la division de P par $(X-a)$ est donné par la valeur de la fonction polynomiale $\tilde{P}$ en a.

En effet, la division euclidienne nous donne $P = (X-a)Q + R$ avec $\deg R < 1$. Il suit que $R \in A$ et pour trouver R, nous appliquons la fonction $\mathbf{F}_A$ à la relation pour obtenir $\mathbf{F}_A(P) = \mathbf{F}_A(X-a) \cdot \mathbf{F}_A(R)$. Puisque $\mathbf{F}_A(R)$ est la fonction constante égale à R et $\mathbf{F}_A(X-a)$ est la fonction $x \mapsto (x-a)$ en faisant $x = a$ dans la relation, nous trouvons $R = \mathbf{F}_A(P)(a)$ ce qu'il fallait établir.

E. 98. Soit B un polynôme de degré $b \geq 1$ avec $\mathrm{dom}(B) \in A^\star$. Si P est un polynôme de degré p avec $p = qb + r$. Alors il existe une unique famille de polynômes P_i avec $\deg P_i < b$, telle que

$$P = \sum_{i=0}^{q} P_i B^i.$$

6.6 L'anneau principal $\mathbb{K}[X]$

THÉORÈME 35. — *Si $\mathbb{K}$ est un corps alors l'anneau $\mathbb{K}[X]$ est principal.*

Démonstration. Soit I un idéal de $\mathbb{K}[X]$. Nous devons montrer que I est un idéal principal soit, conformément à la définition donnée en (4.2.1), établir l'existence d'un polynôme G tel que $I = \langle G \rangle$ ou encore

$$I = \{GP \ : \ P \in \mathbb{K}[X]\}.$$

Nous éliminons rapidement le cas où I est réduit au polynôme nul pour lequel il suffit de prendre $G = 0$. Nous supposerons donc I contient un polynôme non nul, dans ce cas l'ensemble $\{\deg(P) \ : \ kP \in I \setminus \{0_A\}\}$ est un sous-ensemble non vide de $\mathbb{N}$ et il admet par conséquent un plus petit élément. Nous appellerons d ce plus petit élément et choisirons $G \in I$ tel que $\deg(G) = d$. Nous voulons établir que $I = \langle G \rangle$. Puisque $G \in I$ nous avons immédiatement $\langle G \rangle \subset I$ (voir l'exercice 93) et il reste seulement à établir l'inclusion réciproque, $I \subset \langle G \rangle$. Prenons $P \in I$ et formons sa division euclidienne par G. Nous avons $P = DG + R$ avec $\deg R < \deg G$. Puisque P et G sont des éléments de I, il en est de même de $P - DG$. Le polynôme R est donc un élément de I donc le degré est moindre que celui de G. A cause de la propriété de minimalité du degré qui définit G la seule possibilité est que $R = 0$. Par suite, $P = DG$ et $P \in \langle G \rangle$, ce qu'il fallait établir. ■

6.7 Racines des polynômes

Soit A un anneau commutatif unitaire intègre et $P \in A[X]$. Nous dirons qu'un élément $a \in A$ est un **zéro** de P (ou bien une **racine** de P) si la fonction polynomial associée à P s'annule en a, $\tilde{P}(a) = 0_A$. Par un abus d'écriture que nous avons déjà signalé, nous écrirons $P(a) = 0$ plutôt que $\tilde{P}(a) = 0_A$.

THÉORÈME 36. — *Pour que a soit racine de P il faut et il suffit que le polynôme $X - a$ divise P, c'est-à-dire qu'il existe $Q \in A[X]$ tel que $P = (X-a)Q$.*

Démonstration. Supposons que $P(X) = (X-a)Q(X)$. Puisque l'application qui à un polynôme associe sa fonction polynomiale est un morphisme d'anneau, nous avons la fonction $\tilde{P}(x)$ s'écrit comme $(x-a)$ multiplié par une autre fonction polynomiale et elle s'annule par conséquent pour $x = a$.

Supposons maintenant que a soit racine de P alors, compte tenu de l'exemple 7, nous avons $Q = (X-a)Q + \tilde{P}(a)$. Comme $\tilde{P}(a) = 0$, nous obtenons le fait que $(X-a)$ divise P. ■

Le théorème précédent suggère de définir la multiplicité d'une racine de la manière suivante. Nous dirons que a est une racine (un zéro) d'**ordre** k – ou de **multiplicité** k – lorsque $(X-a)^k$ divise P ($P = (X-a)^k Q$ pour un certain $Q \in A[X]$) mais $(X-a)^{k+1}$ ne divise pas P. En d'autres mots, a est un zéro d'ordre k si $\texttt{REST}(P, (X-a)^k) = 0$ mais $\texttt{REST}(P, (X-a)^{k+1}) \neq 0$.

Le théorème suivant est fondamental. Nous en tirerons deux conséquences essentielles immédiatement à près sa démonstration.

THÉORÈME 37. — *Soient A un anneau commutatif unitaire et $P \in A[X]$. Si A est intègre et si $a_1, a_2, \ldots, a_r$ sont des zéros de P alors*

$$P = (X-a_1)^{k_1}(X-a_2)^{k_2}\ldots(X-a_r)^{k_r}Q$$

où k_i est la multiplicité de a_i ($1 \leq i \leq r$) et aucun des a_i n'est racine de $Q \in A[X]$.

Remarquons que l'énoncé dit que $a_1, a_2, \ldots, a_r$ sont *des* zéros de P et il ne dit pas que $a_1, a_2, \ldots, a_r$ sont *tous* les zéros de P.

Démonstration. Elle s'effectue par récurrence sur r. Lorsque $r = 1$, le théorème est vrai par définition d'une racine multiple. Nous supposons que le théorème est vrai pour $r-1$, $r \geq 2$, et le démontrons pour r. Par hypothèse de récurrence, nous savons que

$$P = (X-a_1)^{k_1}\ldots(X-a_{r-1})^{k_{r-1}}T$$

avec $T(a_i) \neq 0$ pour $i = 1, \ldots, r-1$. Puisque $P(a_r) = 0$ mais $a_r \neq a_i$ ($1 \leq i \leq r-1$) nous avons nécessairement $T(a_r) = 0$ de sorte que a_r est un zéro de T (théorème 36) et nous pouvons écrire écrire $T = (X-a_r)^s Q$ où $Q(a_r) \neq 0$ et s désigne la multiplicité de a_r comme zéro de T. Reportant cette relation dans l'expression de P, il vient

$$P = (X-a_1)^{k_1}\ldots(X-a_{r-1})^{k_{r-1}}(X-a_r)^s Q. \tag{6.6}$$

Pour établir la formule cherchée pour r et donc achever la démonstartion du théorème, il nous reste à établir que $s = k_r$. Puisque a_r est un zéro de P d'ordre k_r, nous pouvons écrire par définition de la multiplicité $P = (X-a_r)^{k_r}U$ avec $U(a_r) \neq 0$. En reportant cette relation dans (6.6) nous arrivons à

$$(X-a_r)^{k_r}U = (X-a_1)^{k_1}\ldots(X-a_{r-1})^{k_{r-1}}(X-a_r)^s Q.$$

Supposons maintenant que $k_r > s$, nous avons

$$(X-a_r)^s\Big((X-a_r)^{k_r-s}U-(X-a_1)^{k_1}\dots(X-a_{r-1})^{k_{r-1}}Q\Big)=0. \tag{6.7}$$

Puisque A est intègre, d'après le Théorème 31, $A[X]$ est aussi intègre et il est permis de simplifier (voir 1.5) par le terme non nul $(X-a_r)^s$ dans (31) pour obtenir

$$(X-a_r)^{k_r-s}U-(X-a_1)^{k_1}\dots(X-a_{r-1})^{k_{r-1}}Q=0.$$

En calculant la fonction polynomiale associée en $t=a_r$ nous arrivons à une contradiction :

$$0+\underbrace{(a_r-a_1)^{k_1}\dots(a_r-a_{r-1})^{k_{r-1}}}_{\neq 0}\underbrace{Q(a_r)}_{\neq 0}=0.$$

Nous montrerions de manière similaire que l'hypothèse $k_r < s$ conduit aussi à une contradiction de sorte que $k_r = s$. ■

THÉORÈME 38. — *Si A est un anneau (commutatif unitaire) intègre alors tout polynôme $P \in A[X]$ non nul admet au plus* $\deg(P)$ *racines en tenant compte de la multiplicité. Autrement dit si P admet m racines a_i ($i \in \{1,2,\dots,m\}$) chacune de multiplicité s_i alors nécessairement $s_1+s_2+\dots+s_m \leq \deg(P)$.*

Ce résultat n'est plus vrai en général si A n'est pas supposé intègre. Par exemple si $A=\mathbb{Z}/8\mathbb{Z}$, le polynôme $P=X^3$ qui est de degré 3 admet 4 racines car $P(\overline{0})=P(\overline{2})=P(\overline{4})=P(\overline{6})=\overline{0}$.

THÉORÈME 39. — *Si A est un anneau commutatif unitaire intègre de cardinal infini alors l'application* F_A *qui a tout polynôme fait correspondre sa fonction polynomiale associée est injective.*

Démonstration. Nous devons montrer que $\mathbf{F}_A : A[X] \to \mathscr{F}(A)$ est injective et pour cela, puisque c'est un morphisme d'anneau, il suffit de vérifier que $\ker \mathbf{F}_A = \{0\}$. Supposons que $\mathbf{F}_A(P)=0$. Cela signifie que $\tilde{P}$ s'annule en tout point de A donc P a une infinité de racines ce qui est impossible d'après le théorème précédent, à moins que $P=0$. ■

Nous sommes encore en présence d'un morphisme d'anneaux injectif et nous pouvons confondre l'anneau de départ $A[X]$ avec son image dans $\mathscr{F}(A)$ qui n'est autre que l'ensemble des fonctions polynomiales.

Ce résultat nous ramène au point dont nous sommes partis. Nous nous sommes donner un grand mal pour distinguer les polynômes des fonctions polynomiales en passant par une définition bien abstraite pour arriver à nouveau à la conclusion que nous pouvons confondre polynômes et fonctions polynomiales, elles sont en correspondance bijective les unes avec les autres. Seulement, c'est vrai uniquement dans le cas ou l'anneau A contient un nombre infini d'éléments. Cependant les polynômes à coefficients dans le

corps $\mathbb{Z}_p$, p premier, jouent un rôle important en algèbre et justifient à eux seuls l'étude des polynômes dans le cadre général qui a été présentée dans cette partie. Un autre argument en défense de la définition formelle des anneaux de polynômes est donnée dans la partie suivante.

6.8 Le corps des fractions rationnelles

Soit K un corps (commutatif), l'anneau $K[X]$ est commutatif intègre et unitaire et nous pouvons former le corps des fractions $Q(K[X])$ tel que défini dans la section 5. Ce corps s'appelle le corps des fractions rationnelles à coefficients dans K et il est noté $K(X)$ (les crochets $[\cdot]$ sont remplacés par des parenthèses) et tout élément de $K(X)$ se représente sous la forme $\frac{P}{Q}$ où P et Q sont deux éléments de $K[X]$. Naturellement à chaque élément de $K(X)$ nous pouvons associer une fonction rationnelle juste comme nous faisions avec les polynômes. Simplement, au contraire des fonctions polynômes, les fonctions rationnelles ne sont pas définies sur K tout entier mais seulement en tout ou le dénominateur ne s'annule pas. Lorsque nous travaillons dans $K(X)$ la question de savoir où le dénominateur s'annule n'a aucune importance et nous pouvons effectuer tous les calculs sans jamais de soucier d'un ensemble de définition. Observons par ailleurs que cette construction nous permet de mettre en évidence un corps infini de caractéristique $q > 1$, à savoir le corps $\mathbb{Z}_q(X)$. Ce cors est évidemment infini (il contient $\bar{1}X^n$, $n \in \mathbb{N}$) et il est bien de caractéristique q puisque son unité est la même que celle de $\mathbb{Z}_q$.

E. 99. Si A est un anneau commutatif intègre unitaire, $A[X]$ possède les mêmes propriétés et nous pouvons considérer $Q(A[X])$. Pourquoi nous sommes nous limité ici à considérer le cas où A est un corps ? On pourra comparer $Q(A[X])$ et $Q(Q(A)[X])$.

6.9 Le théorème fondamental de l'algèbre

Il n'est pas possible de conclure cette partie sans traiter la traiter la question essentielle des racines des polynômes à coefficients complexes qui sont de loin les polynômes les plus utiles. Remarquons que dans ce cas le théorème 39 assure que nous pouvons confondre polynôme et fonctions polynomiales ce que nous ferons sans davantage d'explication. Le théorème ci-dessous, s'il n'est peut-être plus aujourd'hui le seul, reste un des rares résultats clé des mathématiques que tout étudiant doit connaître.

THÉORÈME 40. — *Tout polynôme à coefficients dans $\mathbb{C}$ de degré positif (≥ 1) admet au moins une racine dans $\mathbb{C}$.*

Il pourrait paraître redondant de préciser que la racine est dans $\mathbb{C}$. Où pourrait-elle se trouver, sinon dans $\mathbb{C}$? En réalité, quel que soit le polynôme P à coefficients dans un anneau commutatif intègre et unitaire A, les algébristes sont toujours capables de construire de manière abstraite un corps K contenant A dans lequel le polynôme possédera une racine. Un tel théorème sera étudié plus loin et le lecteur qui reviendra

alors au théorème 40 ci-dessus comprendra l'intérêt de préciser que la racine en question se trouve bien dans $\mathbb{C}$.

Le théorème 40 est souvent utilisé sous une des deux formes ci-dessous qui s'en déduisent assez aisément.

THÉORÈME 41. — *Si $p \in \mathbb{C}[X]$ est de degré positif alors il existe $r \geq 1$ et des nombres complexes $\alpha_1, \ldots, \alpha_r$ et des entiers correspondants $m_1, \ldots, m_r$ tels que*

$$p(X) = \mathrm{dom}(P)(X-\alpha_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_r)^{m_r}. \tag{6.8}$$

En particulier,

$$m_1 + m_2 + \cdots + m_r = \deg(P).$$

Naturellement, r est le nombre de racines distinctes de p et m_i est la multiplicité de la racine α_i.

Démonstration. La démonstration est par récurrence sur le degré du polynôme, étant évidente dans le cas du degré 1. Supposons la propriété vraie pour les polynômes de degré n et supposons que $\deg(p) = n+1$. Le théorème 40 nous assure l'existence de $\alpha \in \mathbb{C}$ tel $p(\alpha) = 0$ ou, en vertu du théorème 36, $p(X) = (X-\alpha)Q(X)$. Nécessairement $\deg(Q) = n$ et $\mathrm{dom}(Q) = \mathrm{dom}(P)$. En appliquant, l'hypothèse de récurrence au polynôme Q, nous obtenons

$$p(X) = \mathrm{dom}(P)(X-\alpha)(X-\alpha_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_r)^{m_r}.$$

Si α ne coïncide avec aucun des α_i, l'expression est définitive, sinon, si $\alpha = \alpha_i$, nous omettons le terme $(X-\alpha)$ et augmentons m_i d'une unité. La vérification du fait que les m_i dans (6.8) sont effectivement les multiplicité des racines α_i est laissée en exercice. ■

Le cas des polynômes à coefficients réels est tout particulièrement important dans la pratique. Il est essentiel de connaître le type de factorisation que nous pouvons obtenir dans le cas où il n'est pas possible de faire intervenir des nombres complexes. La réponse de séduit aisément du théorème fondamental à l'aide du raisonnement suivant. Supposons que $P(X) = \sum_{i=0}^{n} a_i X^i$ soit un polynôme de degré n (de sorte que $a_n \neq 0$) à coefficients réels et que α soit une racine de P. Celle-ci peut-être un nombre réel ou bien un nombre complexe de partie imaginaire non nulle de sorte $\alpha \neq \bar{\alpha}$. Dans ce dernier cas, en utilisant le fait (voir l'exemple 2) que

$$\overline{zw} = \overline{z}\overline{w}, \quad \bar{\bar{z}} = z \quad \text{et} \quad \overline{z+w} = \bar{z} + \bar{w},$$

nous obtenons

$$0 = P(\bar{\alpha}) = \sum_{i=1}^{n} a_i \bar{\alpha}^i = \overline{\sum_{i=0}^{n} \overline{a_i}\alpha^i} = \overline{\sum_{i=0}^{n} a_i \alpha^i}$$

qui montre que $P(\overline{\alpha}) = 0$. Il suit que dès qu'un nombre complexe non réel est racine de p, il est de même de son conjugué. Une raisonnement similaire permet d'établir que les deux racines conjuguées α et $\overline{\alpha}$ ont la même multiplicité. Cela signifie que dans la factorisation (6.8), nous pouvons mettre d'une part les racines réelles (avec leur multiplicité) et de l'autre regrouper les racines complexes deux par deux pour obtenir des termes de la formes $(X-\alpha)^m(X-\bar{\alpha})^m = (X^2 - 2\Re(\alpha)X + |\alpha|^2)^m$. Ici le trinôme $X^2 - 2\Re(\alpha)X + |\alpha|^2$ a des coefficients réels et un discriminant négatif (puisque ses racines ne sont pas réelles).

Le théorème suivant résume les informations obtenues de manière un peu pesante.

THÉORÈME 42. — *Si $p \in \mathbb{R}[X]$ est de degré positif alors il existe $r \geq 1$ et des nombres réels $\alpha_1, \ldots, \alpha_s$, des trinômes du second degré $(X^2 + a_i X + b_i)$ à discriminant négatif, $i = s+1, \ldots, r$ et des entiers correspondants $m_1, \ldots, m_r$ tels que*

$$p(X) = \mathrm{dom}(P)(X-\alpha_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_s)^{m_s} \cdot (X^2 + a_{s+1}X + b_{s+1})^{m_{s+1}}\cdots(X^2 + a_r X + b_r)^{m_r}. \quad (6.9)$$

Nous avons encore,

$$m_1 + m_2 + \cdots + m_s + 2m_{s+1} + \cdots 2m_r = \deg(P).$$

Lorsque toutes les racines de P sont réelles, nous avons $s = r$ et aucun trinôme n'apparaît dans la formule.

6.10 Démonstration du théorème fondamental de l'algèbre

Aucune démonstration du théorème fondamental de l'algèbre n'est à la fois simple et élémentaire. Il en existe beaucoup, Gauss lui-même en avait recueilli ou inventé plusieurs, et on trouve encore aujourd'hui de nombreux collectionneurs de démonstrations du théorème fondamental. Le résultat continue d'exercer une profonde fascination, spécialement chez les jeunes mathématiciens ou ceux de leurs aînés qui privilégient l'aspect récréatif ou ludique des mathématiques. Toutes les démonstrations reposent sur une propriété de nature topologique du plan complexe, plus ou moins apparente, qui sera soulignée plus bas.

La démonstration que nous donnerons fait appel à des techniques d'analyse. Nous utiliserons les notions de limite, de continuité (en particulier, le fait que les fonctions polynomiales à coefficients complexes sont continues sur $\mathbb{C}$) et le fait qu'une fonction continue à valeurs réelles atteint ses bornes sur tout ensemble fermé borné (compact) comme un disque fermé $D(a,r) = \{z \in \mathbb{C} \,:\, |z-a| \leq r\}$. Ces notions et ce résultat sont en général enseignés en seconde année d'études universitaires.

LEMME 2. — *Si $f : \mathbb{C} \to \mathbb{C}$ est continue en tout point de $\mathbb{C}$ et vérifie la condition $\lim_{|z|\to\infty} |f(z)| = \infty$ alors f atteint sa borne inférieure sur $\mathbb{C}$. Autrement dit, il existe*

$b \in \mathbb{C}$ tel que

$$|f(b)| = \min_{z\in\mathbb{C}} |f(z)|.$$

Démonstration. La condition $\lim_{|z|\to\infty} |f(z)| = \infty$ signifie que pour tout réel positif R, il existe $r > 0$ tel que la condition $|z| > r$ entraîne $|f(z)| > R$. Appliquons cette condition en prenant $R = |f(0)|$. Il existe $r_0 > 0$ tel que $|z| > r_0 \implies |f(z)| > |f(0)|$. Ayant choisi r_0, nous considérons alors le disque fermé $\{z \in \mathbb{C} : |z| \leq r_0\}$. C'est un ensemble compact sur lequel la fonction continue à valeur réelle $|f|$ atteint son minimum, disons au point b, de sorte que $|f(b)| = \min_{|z|\leq r_0} |f(z)|$. Maintenant, par définition de r_0, si $|z| > r_0$ alors $|f(z)| \geq |f(0)|$ et, puisque $0 \in D(0, r_0)$, $|f(0)| \geq \min_{|z|\leq r_0} |f(z)| = |f(b)|$. Il suit que $|f(z)| \geq |f(b)|$ que le module de z soit ou non plus petit que r_0, de sorte $|f(b)| = \min_{z\in\mathbb{C}} |f(z)|$, ce qu'il fallait établir. ■

LEMME 3. — *Si p est un polynôme à coefficients complexes de degré positif alors* $\lim_{|z|\to\infty} |p(z)| = \infty$.

Démonstration. Supposons que $p(X) = \sum_{i=0}^{n} a_i X^i$ avec $n \geq 1$ et $a_n \neq 0$. Nous pouvons écrire

$$p(z) = z^n \left(a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right), \quad z \in \mathbb{C}^\star.$$

Puisque $\lim_{|z|\to\infty} z^{-j} = 0$, $j = 1, \ldots, n$, la fonction entre parenthèses ci-dessus tend vers a_n lorsque $|z| \to \infty$. Par conséquent, pour z assez grand en module, disons pour $|z| \geq \mu$, le module du terme entre parenthèses sera supérieur à $|a_n|/2$ de sorte que

$$|p(z)| \geq |a_n||z|^n/2, \quad |z| \geq \mu.$$

Puisque le terme minorant ci-dessus tend vers ∞ lorsque $|z| \to \infty$, il en est de même du terme majorant et c'est ce qu'il fallait établir. ■

Nous pouvons passer à la démonstration du théorème 40. La démonstration se fait par l'absurde. Nous supposons que p est un polynôme de degré $d \geq 1$ [*] qui n'admet pas de racine dans $\mathbb{C}$ et nous recherchons une contradiction. Le second lemme nous assure que $\lim_{|z|\to\infty} |p(z)| = \infty$ et nous pouvons par conséquent appliquer le premier lemme et choisir $z_0 \in \mathbb{C}$ tel que

$$|p(z_0)| = \min_{z\in\mathbb{C}} |p(z)|.$$

Puisque p est supposé ne pas avoir de racine, nous avons $|p(z_0)| > 0$. Pour des raisons de simplification d'écriture, il est commode de travailler avec l'origine plutôt qu'avec z_0. Le polynôme $P(z) = p(z - z_0)$ est lui-aussi de degré d, il est sans racine et son minimum

∗. Nous pourrions supposer immédiatement que d est au moins plus grand que 2 mais cela ne nous servira pas.

est atteint en 0. Ce minimum sera noté μ. Nous avons $|P(z)| \geq |P(0)| = \mu > 0$, $z \in \mathbb{C}$. Nous pouvons écrire

$$P(z) = a_0 + a_1 z + \cdots + a_d z^d, \quad z \in \mathbb{C}$$

en sachant que $a_0 \neq 0$ (car $p(0) \neq 0$) et $a_d \neq 0$ (car P est de degré d). Pour ce qui est des coefficients $a_1, \ldots, a_{d-1}$. Nous ne pouvons rien dire. Nous noterons k le plus petit entier positif dans $\{1, \ldots, d\}$ tel que $a_k \neq 0$ de sorte que

$$P(z) = a_0 + a_k z^k + a_{k+1} z^{k+1} + \ldots a_d z^d, \quad z \in \mathbb{C}. \tag{6.10}$$

Il n'est pas exclu à priori que cet entier k soit égal à d mais dans ce cas $P(z) = a_0 + a_d z^d$ et le polynôme admet certainement une racine contrairement à l'hypothèse. En effet, si $-a_0/a_d = \rho e^{i\theta}$, une racine est donnée par $z = \rho^{1/d} e^{i\theta/d}$. Nous pouvons donc supposer que k est compris entre 1 et $d-1$. Dans ce cas, nous avons

$$\lim_{z \to 0} \left| \frac{a_{k+1} z^{k+1} + \cdots + a_d z^d}{z^k} \right| = 0. \tag{6.11}$$

Comme par ailleurs,

$$\lim_{z \to 0} |a_k z^k| = 0, \tag{6.12}$$

nous pouvons choisir $\eta > 0$ tel que

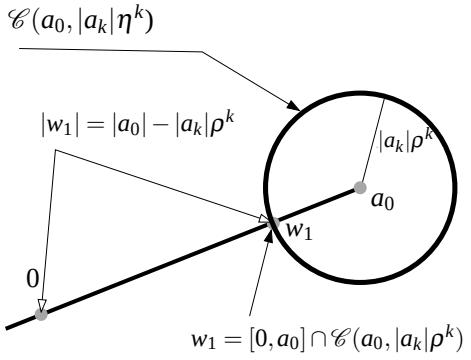
$$|z| = \eta \implies \begin{cases} |a_{k+1} z^{k+1} + \cdots a_d z^d| < |a_k z^k|, \\ |a_k z^k| < \mu. \end{cases} \tag{6.13}$$

Maintenant lorsque z parcourt le cercle de centre l'origine et de rayon η alors $a_0 + a_k z^k$ parcourt k fois le cercle de centre a_0 et de rayon $|a_k|\eta^k$.

En d'autre termes, si T désigne l'application $T : z \in \mathbb{C} \to a_0 + a_k z^k$ alors

$$T(\mathscr{C}(0, \eta)) = T(\mathscr{C}(a_0, |a_k|\eta^k)).$$

Puisque $|a_0| = |P(0)| = \mu$ et $|a_k|\eta^k < \mu$, l'origine est à l'extérieur du cercle image $\mathscr{C}(a_0, |a_k|\eta^k)$ et le segment $[0, a_0]$ rencontre le cercle en un unique point que nous noterons w_1 *. Nous pouvons alors choisir $z_1 \in \mathscr{C}(0, \eta)$ tel que $T(z_1) = w_1$. Maintenant nous avons



∗. Comment démontreriez vous cette propriété ?

$$\begin{aligned}
|P(z_1)| &= |a_0 + a_k z_1^k + a_{k+1} z_1^{k+1} + \dots a_d z_1^d| && \text{(voir (6.10))}\\
&\le |a_0 + a_k z_1^k| + |a_{k+1} z_1^{k+1} + \dots a_d z_1^d| && \text{(utilise l'inégalité triangulaire)}\\
&\le |w_1| + |a_{k+1} z_1^{k+1} + \dots a_d z_1^d| && \text{(par définition de } w_1)\\
&\le |a_0| - |a_k \eta^k| + |a_{k+1} z_1^{k+1} + \dots a_d z_1^d| && \text{(par construction de } w_1)\\
&< |a_0| - |a_k \eta^k| + |a_k z_1^k| && \text{(par définition de } \eta \text{ dans 6.13 en}\\
& && \text{tenant compte que } |z_1| = \eta)\\
&< |a_0| && \text{(puisque } -|a_k \eta^k| + |a_k z_1^k| = 0).
\end{aligned}$$

Mais la relation $|P(z_1) < |a_0|$ est absurde puisque $|a_0| = \mu = \min_{z\in\mathbb{C}} |P(z)|$. La supposition que p (ou P) n'a pas de racine conduit donc à une contradiction et ceci achève la démonstration du théorème. ■

Nous avons dit que la raison profonde expliquant le théorème est de nature topologique mais la topologie, à part peut-être le fait que les fonctions continues atteignent leurs bornes sur les ensembles compacts, n'est pas apparue de manière évidente dans la démonstration. Les propriétés fondamentales sur lesquelles reposent la démonstration sont celles de la fonction exponentielle complexe et spécialement de la fonction $t \in \mathbb{R} \to \exp(it) \in \mathbb{C}$. Nous avons utilisé deux fois (où ?) le fait que cette application définit une surjection de $\mathbb{R}$ sur le cercle unité. Cette propriété est enseignée très tôt mais elle ne peut être démontrée rigoureusement sans une étude précise de la série définissant l'exponentielle.

§ 7. EXERCICES ET PROBLÈMES COMPLÉMENTAIRES

100. Un anneau non intègre peut-il admettre un sous-anneau intègre ?

101. Soient $a < b$ deux réels. On note $\mathsf{C}[a,b]$ l'ensemble des fonctions continues sur $[a,b]$. Expliquer (rapidement) pourquoi $(\mathsf{C}[a,b], +, \cdot)$ est un anneau commutatif unitaire. Est-il intègre ? Déterminer le groupe des éléments inversibles $(\mathsf{C}[a,b])^*$. Démontrer que $\mathsf{C}[a,b]$ et $\mathsf{C}[0,1]$ sont isomorphes.

102. Montrer les relations suivantes sur la division euclidienne dans l'anneau $\mathbb{K}[X]$. Les symboles $a, b, c, \dots$ désignent des polynômes quelconques de $\mathbb{K}[X]$.

(i) $\mathtt{REST}(a + bc\,,\, c) = \mathtt{REST}(a\,,\, c)$,

(ii) $\mathtt{REST}(ad\,,\, cd) = d\mathtt{REST}(a\,,\, c)$

(iii) $\mathtt{REST}(a + b\,,\, c) = \mathtt{REST}(\mathtt{REST}(a\,,\, c) + \mathtt{REST}(b\,,\, c)\,,\, c)$,

(iv) $\mathtt{REST}(ab\,,\, c) = \mathtt{REST}(\mathtt{REST}(a\,,\, c) \cdot \mathtt{REST}(b\,,\, c)\,,\, c)$,

(v) $\mathtt{QUOT}(\mathtt{REST}(a\,,\, cd)\,,\, c) = \mathtt{REST}(\mathtt{QUOT}(a\,,\, c)\,,\, d)$,

(vi) $\mathtt{REST}(a\,,\, c) + c \cdot \mathtt{REST}(\mathtt{QUOT}(a\,,\, c)\,,\, d) = \mathtt{REST}(a\,,\, cd)$.

103. Soit $(A, +, \cdot)$ un anneau. Le centre $c(A)$ est défini par

$$c(A) = \{x \in A : \forall a \in A\ a \cdot x = x \cdot a\}.$$

Montrer que $c(A)$ est un sous-anneau de A. Quel est le centre de $(M_2(\mathbb{R}),+,\cdot)$?

104. Soit p un nombre premier. Montrer que $\mathbb{Q}_p$ est un sous-anneau de $(\mathbb{Q},+,\cdot)$. On rappelle que $\mathbb{Q}_p = \left\{ \frac{m}{p^n} : \ m \in \mathbb{Z}, n \in \mathbb{N} \right\}$. Déterminer $(\mathbb{Q}_p)^*$.

105. On définit l'ensemble $M_n(\mathbb{Z})$ par la relation

$$M_n(\mathbb{Z}) = \{M \in M_n(\mathbb{R}) : \text{tous les coefficients de } M \text{ sont dans } \mathbb{Z}\}.$$

Montrer que $M_n(\mathbb{Z})$ est un sous-anneau de $(M_n(\mathbb{R}),+,\cdot)$. Déterminer l'ensemble des éléments inversibles (pour la multiplication) de $M_n(\mathbb{Z})$.

106. Soit A un sous-anneau de $(\mathbb{R},+,\cdot)$. On appelle $\mathscr{A}$ l'ensemble des matrices de $M_2(\mathbb{R})$ dont tous les coefficients appartiennent à A.

(i) Montrer que $\mathscr{A}$ est un sous-anneau unitaire de $(M_2(\mathbb{R}),+,\cdot)$.

(ii) Montrer que si $M \in \mathscr{A}$ alors $\det M \in A$.

(iii) Montrer que $M \in \mathscr{A}^\star$ si et seulement si $\det M \in A^\star$.

(iv) Lorsque $A = \mathbb{Z}$, $\mathscr{A}^\star$ contient-il une infinité d'éléments ?

107. On définit $\mathbb{Z}[i] =_{def} \{m+in : m,n \in \mathbb{Z}\} \subset \mathbb{C}$.

A) Montrer que $(\mathbb{Z}[i],+,\cdot)$ est un anneau commutatif unitaire (on montrera que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C},+,\cdot)$).

B) On définit sur $\mathbb{Z}[i]$ l'application N par $N(n+im) = n^2+m^2$. Montrer que pour tous α et β dans $\mathbb{Z}[i]$, on a $N(\alpha\cdot\beta) = N(\alpha)\cdot N(\beta)$. Montrer que si α est inversible alors $N(\alpha) = 1$ en déduire $(\mathbb{Z}[i])^*$, le groupe des éléments inversibles de $\mathbb{Z}[i]$. A quel groupe déjà rencontré $((\mathbb{Z}[i])^*,\cdot)$ est-il isomorphe ?

108. Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{5})$ sont-ils isomorphes ?

109. Résoudre le système suivant dans $\mathbb{Z}_7$

$$\begin{cases} \overline{2}x & + & \overline{3}y & = & \overline{1} \\ \overline{3}x & + & \overline{2}y & = & \overline{5} \end{cases}.$$

110. Déterminer tous les idéaux de $(\mathbb{Q}_p,+,\cdot)$.

111. On considère le produit cartésien des anneaux $\mathbb{Z}_m$ et $\mathbb{Z}_n$ où m et n sont deux entiers premiers entre eux.

A) Montrer que l'application f ci-dessous est bien définie :

$$f : \begin{array}{ccc} \mathbb{Z}_{mn} & \longrightarrow & \mathbb{Z}_m \times \mathbb{Z}_n \\ \mathbf{cl}_{mn}(a) & \longmapsto & (\mathbf{cl}_m(a), \mathbf{cl}_n(a)) \end{array}$$

où on utilise la notation $\mathbf{cl}_s(a)$ pour représenter la classe de a dans $\mathbb{Z}_s$.

B) L'application f est-elle un isomorphisme d'anneau ?

C) Utiliser f pour établir que lorsque m et n sont premiers entre eux on a $\phi(mn) = \phi(m)\phi(n)$. On rappelle que ϕ est l'indicatrice d'Euler.

D) En déduire, en utilisant l'exercice précédent, une formule générale pour le calcul de $\phi(m)$, m entier positif quelconque.

112. Soient $(A,+,\cdot)$ un anneau commutatif unitaire et I un idéal de A. Montrer que si $I\cap A^*\neq\emptyset$ alors $I=A$.

113. Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux commutatifs (unitaires) et $\phi:A\to B$ un morphisme d'anneaux. Est-il vrai que si I est un idéal de A alors $\phi(I)$ est un idéal de B ? Est-il vrai que si J est un idéal de B alors $\phi^{-1}(J)$ est un idéal de A ?

114. Soit $(A,+,\cdot)$ un anneau commutatif unitaire et I un idéal de A. Le **radical** de I, noté $\sqrt{I}$, est l'ensemble des éléments $a\in A$ pour lesquels il existe $m\in\mathbb{N}^\star$ tel que $a^m\in I$.

A) Montrer que $\sqrt{I}$ est un idéal de A. (On utilisera convenablement la formule du binôme de Newton.)

B) On prend $A=\mathbb{Z}$ et $I=36\mathbb{Z}$. Déterminer $\sqrt{I}$. Plus généralement, comment peut-on déterminer $\sqrt{m\mathbb{Z}}$ pour tout $m\in\mathbb{Z}$?

115. On travaille avec $(\mathbb{R}[X],+,\cdot)$ et $(\mathbb{C},+,\cdot)$ et on considère l'application

$$f:\begin{array}{ccc}\mathbb{R}[X] & \longrightarrow & \mathbb{C}\\ P & \longmapsto & P(i)\end{array}$$

où i désigne le nombre complexe habituel.

A) Montrer que f est un morphisme d'anneau. Déterminer l'idéal $\ker f$.

B) En déduire $\mathbb{R}[X]/(X^2+1)\simeq\mathbb{C}$.

C) Que peut-on dire de $\mathbb{Q}[X]/(X^2+1)$?

D) Pouvez-vous trouver un anneau quotient qui soit isomorphe au corps $\mathbb{Q}(\sqrt{d})$?

116. Soit $P\in\mathbb{R}[X]$. On considère l'idéal principal $I=(P)$ engendré par P. Montrer que si P s'écrit $P=P_1P_2$ avec $\deg P_i\geq 1$ alors l'anneau $\mathbb{R}[X]/I$ n'est pas intègre. A quelle(s) condition(s) l'anneau quotient $\mathbb{R}[X]/I$ sera-t-il un corps ?

117. Soit p un nombre premier (≥ 2). On considère les anneaux $\mathbb{Z}[X]$ et $\mathbb{Z}_p$. On définit l'application ϕ par

$$\phi:\begin{array}{ccc}\mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_p[X]\\ P & \longmapsto & \overline{P}\end{array}$$

où $\overline{P}=\sum_{i=0}^n\overline{a_i}X^i$ si $P=\sum_{i=0}^n a_iX^i$. (On rappelle que $\overline{a}$ désigne la classe de $a\in\mathbb{Z}$ dans $\mathbb{Z}_p$.)

A) On prend $p=5$. Soit $f=5X^6+X^5+3x^4+X^3+4X^2-3X-1$ et $g=X^2+X+1$. Déterminer $\overline{f}$ et $\overline{g}$. Montrer que $\overline{g}$ divise $\overline{f}$. Est-il vrai que f est divisible par g ?

B) On revient au cas p premier quelconque. Montrer que ϕ est un morphisme d'anneau. Déterminer son noyau. En déduire un isomorphisme d'anneau. Pouvez-vous généraliser le résultat (que dire si on remplace $\mathbb{Z}$ par A et $p\mathbb{Z}$ par un ideal I de A) ?

C) Soient f et g deux polynômes de $\mathbb{Z}[X]$. On suppose que $\mathrm{dom}(g)\in\mathbb{Z}^*=\{-1,1\}$. Déterminer $Q(\overline{f},\overline{g})$ (resp. $R(\overline{f},\overline{g})$) le quotient (resp. le reste) de la division de $\overline{f}$ par $\overline{g}$ en fonction de $Q(f,g)$ (resp. de $R(f,g)$).

118. On appelle A l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}/3\mathbb{Z}$,

$$A=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}:a,b,c,d\in\mathbb{Z}/3\mathbb{Z}\right\}.$$

On munit A des lois $+$ et $\cdot$ définies par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a\cdot a'+b\cdot c' & a\cdot b'+b\cdot d' \\ c\cdot a'+d\cdot c' & c\cdot b'+d\cdot d' \end{pmatrix}$$

Par exemple, on a

$$\begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{0} \end{pmatrix} + \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{2} & \overline{1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{1} & \overline{2} \end{pmatrix} \cdot \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{1} & \overline{2} \end{pmatrix} = \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix}.$$

On remarquera que, formellement, ce sont exactement les mêmes règles de calculs que pour les matrices usuelles. Il faut cependant prendre garde que tous les coefficients sont des éléments de $\{\overline{0}, \overline{1}, \overline{2}\}$.

On **admet** que $(A, +, \cdot)$ est un anneau unitaire. On a

$$0_A = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix} \quad \text{et} \quad 1_A = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Nota Bene. Nous ne définissons pas d'application déterminant *sur A. L'emploi d'une telle application dans l'exercice est* interdit.

A) Propriétés élémentaires de l'anneau A.

(a) Montrer que A contient 81 éléments.

(b) Soit $M = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$. Vérifier que $M^3 = M$. A t-on $M \in A^\star$?

(c) Montrer que A n'est pas intègre.

B) On considère B le sous-ensemble de A formé des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec a, b quelconques dans $\mathbb{Z}/3\mathbb{Z}$.

(a) Montrer que B est un sous-anneau de $(A, +, \cdot)$.

(b) Donner la liste des éléments de B.

(c) Déterminer l'ensemble des couples $(a, b) \in (\mathbb{Z}/3\mathbb{Z})^2$ tels que $a^2 + b^2$ soit non inversible.

(d) Soient $a, b \in \mathbb{Z}/3\mathbb{Z}$. Calculer

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

(e) En déduire que B est un corps.

(f) Existe-t-il $n \in \mathbb{N}^\star$ tel que B soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$?

Notations et symboles

Les ensembles de nombres usuels sont désigné par $\mathbb{N}$ (entiers naturels), $\mathbb{Z}$ (entiers relatifs), $\mathbb{Q}$ (nombres rationels), $\mathbb{R}$ (nombres réels), $\mathbb{C}$ (nombres complexes).

Ensembles

$\emptyset$	Désigne l'ensemble vide.
$a \in A$	Indique que a est un élément de l'ensemble A, on dit souvent *a appartient à A*
$A \subset B$	A est inclus dans B, se dit lorsque tous les éléments de A sont aussi éléments de B.
$A \cup B$	La réunion de A et B, c'est-à-dire l'ensemble des éléments qui appartiennent à *au moins un* des deux ensembles A et B.
$A \cap B$	L'intersection de A et B, c'est-à-dire l'ensemble des éléments qui appartiennent à la fois à A et à B.
$A \setminus B$	Se lit A privé de B. Désigne l'ensemble des éléments de A qui ne sont pas des éléments de B.
$A \times B$	Le produit cartésien de A par B, c'est-à-dire l'ensemble des couples (a,b) avec $a \in A$ et $b \in B$.
$\text{card}(A)$ ou $\lvert A \rvert$	le cardinal de A, c'est-à-dire le nombre d'éléments de A (s'utilise pour un ensemble fini).

Arithmétique et combinatoire élémentaire

$a \mid b$	a divise b (b est un multiple de a)
$a \nmid b$	a ne divise pas b (b n'est pas un multiple de a).
$n!$	Factorielle de n $(1 \cdot 2 \cdot \cdots \cdot n)$
$\binom{n}{m}$	Nombre de parties à m éléments dans un ensemble qui en compte n. La notation plus communément employée dans les textes de langue française est C_n^p

$\text{pgcd}(m_1, m_2, \ldots, m_s)$	Plus grand commun diviseur des entiers m_i, $i = 1, \ldots, s$.
$a \equiv n \quad [n]$	a est congru à b modulo n. cela signifie que n divise $a - b$.

Matrices et algèbre linéaire

$\mathbf{M}_n(\mathbb{K})$	Matrices à n lignes et n colonnes à coefficients dans $\mathbb{K}$
M^T	Transposée de la matrices M : $(M^T)_{ij} = M_{ji}$.
$\text{comat}(M)$	Comatrice de la matrice M : $(\text{comat}M)_{ij}$ est égal à $(-1)^{i+j}$ multiplié par le déterminant obtenu en omettant la i-ème ligne et la j-ème colonne dans M.

Groupes : généralités

a^n	$a * a * \cdots * a$ (n fois) dans $(G, *)$ si $n > 0$, le symétrique de a^{-n} si $n < 0$ et l'élément neutre si $n = 0$
$o(G)$ (card(G), $\lvert G \rvert$)	Ordre (cardinal) du groupe G
$H < G$ / $H \leq G$)	H est un sous-groupe de G / éventuellement égal à G /
$H \triangleleft G$ / $H \trianglelefteq G$	H est un sous-groupe distingué (ou normal ou invariant) de G / éventuellement égal à G /
$\langle X \rangle$	Sous-groupe engendré par le sous-ensemble non vide X de G
$\langle a_1, a_2, \ldots, a_d \rangle$	$\langle X \rangle$ lorsque $X = \{a_1, a_2, \ldots, a_d\}$ (Cette notation prend un sens différent dans la théorie des idéaux)
$\ker f$	Noyau du morphisme f
$\mathsf{Hom}(G, G')$	morphismes de G dans G'
$\mathsf{End}(G)$	Endomorphismes de G
$\mathsf{Aut}(G)$	Automorphismes de G
R_H	Relation d'équivalence sur $(G, *)$ définie par son sous-groupe H ($x \mathsf{R}_H y \iff x^{-1} * y \in H$)

Groupes remarquables

$\mathbf{GL}_n(\mathbb{K})$	Matrices inversibles de $\mathbf{M}_n(\mathbb{K})$
$\mathbf{Is}(P)$	Isométries du plan euclidien orienté

$\mathbf{S}(\Omega)$	Bijections de Ω dans lui-même
$\mathbf{S}_n$	Bijections de $\{1,2,\ldots,n\}$ dans lui-même
$\mathbf{U}$	Nombres complexes de module égal à 1 (Disque de centre l'origine et de rayon 1)
$\mathbf{U}_n$	Racines n-ième de l'unité
$\mathbb{Z}_n$	Désigne le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Autres ensembles remarquables

$\mathscr{F}(X,Y)$	Applications de X dans Y
$\mathscr{F}(X)$	Applications de X dans lui-même
$\mathbf{M}_n(\mathbb{K})$	Matrices à n lignes et n colonnes à coefficients dans $\mathbb{K}$

Anneaux et Corps

A^* ou $\mathrm{U}(A)$	Éléments inversibles de l'anneau $(A,+,\cdot)$.
$\mathrm{car}(K)$	Caractéristique du corps K, ou bien $\mathrm{car}(K)=0$ ou bien $\mathrm{car}(K)$ est un nombre premier plus grand ou égal à deux.
$A[X]$ $(\mathscr{P}_A)$	Anneaux des polynômes à coefficients dans A.
$\texttt{REST}(P,D)$	Reste dans la division euclidienne de P par D, $P=QD+R$.
$\texttt{QUOT}(P,D)$	Quotient dans la division euclidienne de P par Q, $P=QD+R$.
$Q(A)$	Corps des fractions de l'anneau intègre A.
$K(X)$	Corps des fractions rationnelles à coefficients dans K.

Divers symboles

$\forall$	Abbréviation de *quel que soit*
$\exists$	Abbréviation de *il existe*
$\exists!$	Abbréviation *il existe un et un seul*
$:=$	utilisé pour indiquer *est égal par définition*, autrement dit, le terme de droite sert à définir le terme de gauche
$\Longrightarrow$	Abréviation pour indiquer que le terme de droite se déduit du terme de gauche

$\Longleftrightarrow$	Abréviation pour dire *si et seulement si* autrement dit, le terme de gauche est vrai si et seulement si le terme de droite l'est.
$\simeq$	La notation $X \simeq Y$ indique qu'il existe un isomorphisme entre X et Y. En fonction de la nature des ensembles (et du contexte) il peut s'agir d' un isomorphisme de groupes, d'anneaux (ou corps) voire d'espace vectoriel
$[!]\cdots[!]$	Utilisé autour d'une formule erronée ou dépourvue de sens, insérée dans le texte pour signaler au lecteur une erreur commune.
$\neg$	Employé devant une relation pour la nier : si R est une relation, $x\neg Ry$ signifie que R n'est pas en relation avec R.

SOLUTION DES EXERCICES (I)

p. 6 Aucune des lois indiquées n'est associative.

p. 8 Soit $y \in \mathbb{R}$. Un antécédent de $y \in \mathbb{R}$ par f est donné par $x = g(y)$ puisque $f(x) = f(g(y)) = y$. Cela montre que f est surjective. La propriété est en fait équivalente à la surjectivité de f. Le lecteur dans le doute peut chercher une expression pour la fonction g lorsque f est définie sur $\mathbb{R}$ par les relations

$$f(x) = \begin{cases} x & x \leq 0 \\ x-1 & x > 0 \end{cases}.$$

p. 9 Le fait que $e^{-1} = e$ découle de la relation $e * e = e$. Notons $\square$ le symétrique de g^{-1}, ie $\square = (g^{-1})^{-1}$. Nous avons $\square * g^{-1} = e \implies (\square * g^{-1}) * g = e * g \implies \square * e = g \implies \square = g$. Enfin, des relation $(g * g') * (g'^{-1} * g^{-1}) = e = (g'^{-1} * g^{-1}) * (g * g')$, nous tirons $(g * g')^{-1} = g'^{-1} * g^{-1}$. Les calculs intermédiaires, non spécifiés ici, reposent sur l'associativité de la loi $*$.

p. 10 Le résultat implique que tous les éléments apparaissent une et une seule fois sur chaque colonne de la table, et ils apparaissent aussi une et une seule fois sur chaque ligne.

p. 12 Les éléments de $\mathbf{U}_2 \times \mathbf{U}_2$ sont $(1,1)$ (le neutre), $(1,-1)$, $(-1,1)$, $(-1,1)$. l'opération est la multiplication coordonnée par coordonnée. Voici la table

$\swarrow$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	$(1,1)$

p. 14 L'ensemble $\{-2,2\}$ satisfait la seconde condition sans satisfaire la première. Pouvez-vous décrire tous les sous-ensembles de $\mathbb{Z}$ vérifiant la seconde condition ?

p. 14 En effet si x et y sont dans H alors la condition (ii) assure que $y^{-1} \in H$ et, en appliquant la condition (i) avec x et y^{-1}, tous deux éléments de H, nous obtenons $x * y^{-1} \in H$.

p. 14 En effet si $H = \{x \in \mathbb{R} \,:\, \exp x = 0\}$ alors $x, y \in H$ entraîne $x - y \in H$ de sorte que la condition (iii) du Théorème 4 est satisfaite. Ce qui empêche H d'être un sous-groupe c'est bien sûr qu'il est vide.

p. 15 Non. Soit G est un sous-groupe de $(\mathbb{R},+)$ non réduit à l'élément neutre. Prenons $x \neq 0$ dans g. Puisque G est un sous-groupe, il contient aussi ng, $n \in \mathbb{N}$. Puisque x est non nul, les nx sont deux à deux distincts et G contient par conséquent une infinité d'éléments.

p. 16 $m_1\mathbb{Z} + m_2\mathbb{Z} + \cdots + m_k\mathbb{Z} = \text{pgcd}(m_1, \ldots, m_k)$.

p. 16 Si $mu + nv = \text{pgcd}(m,n)$ alors $mu' + nv' = \text{pgcd}(m,n)$ pour $u' = u - kn$ et $v' = v + km$, k étant un entier quelconque.

p. 18 L'application qui à $g \in G$ fait correspondre $O_{G'}$ est toujours un élément de $\mathsf{Hom}(G, G')$.

p. 18 Soient $x, y \in G$. Nous avons $(g \circ f)(x * y) = g(f(x * y)) = g(f(x) \cdot f(y)) = g(f(x)) \bullet g(f(y)) = (g \circ f)(x) \bullet (g \circ f)(y)$.

p. 34 Non bien sûr, sauf lorsque $x_i = e$. Dans la démonstration du théorème 24, nous ne pouvons donc pas utiliser la technique du ker pour montrer l'injectivité de l'application ϕ.

p. 34 Notons $j = e^{2i\pi/3}$. Nous avons

Diviseurs de 6	1	2	3	6
Sous-groupes de $\mathbf{U}_6$	$\{1\}$	$\{1,-1\}$	$\{1, j, j^2\}$	$\mathbf{U}_6$

p. 36 $\mathscr{R}_A$ étant un groupe abélien, $\{g^k : k = 0, \ldots, n-1\}$ en est un sous-groupe distingué. Ce n'est pas un sous-groupe distingué de $\mathbf{Is}(P)$ car si u est vecteur non nul, l'isométrie $t_u \circ g \circ t_{-u}$ laisse fixe le point $t_u(A)$ sans être égale à l'identité. Puisque u est non nul, $t_u(A) \neq A$ et $t_u \circ g \circ t_{-u}$ ne peut pas être une rotation de centre A de sorte que $t_u \circ g \circ t_{-u} \notin \{g^k : k = 0, \ldots, n-1\}$.

p. 37 Parce que les matrices de la forme λId commutent avec n'importe quelle matrice.

p. 42 Considérer l'application $x \in \mathbb{R} \mapsto \exp(2i\pi x/a) \in \mathbf{U}$.

SOLUTION DES EXERCICES (II)

p. 40 Nous pourrions par exemple dire : *Soit $n \geq 2$ et $r \in \{1, \ldots, r-1\}$. Pour que $\overline{r}$ engendre $\mathbb{Z}_n$ il faut et il suffit que r et n soient premiers entre eux.*

p. 60 Soit A une matrice non inversible de $(M_n(\mathbb{K})$. Cela signifie que son noyau n'est réduit à l'élément neutre et il existe donc un vecteur non nul c dans le noyau de A. Appelons B la matrice dont la première colonne est formée des coordonnées de c et toutes les autres colonnes sont nulles. Nous avons $A \cdot B = 0$ et A est bien un diviseur de zéro.

p. 61 Soit B l'ensemble des éléments x de A qui s'écrivent

$$x = \sum_{i \in I} \pm x_{1i} \cdot x_{2i} \cdots x_{k_i i}$$

où I est un ensemble fini et les $x_{ji} \in X$. Montrer que B est le sous-anneau recherché.

p. 61 En effet dans le terme de droite, $+$ désigne une loi interne sur $\mathscr{F}(A)$ et dans le terme de gauche une loi interne sur A.

p. 68 Utiliser un anneau produit de la forme $A = A_1 \times A_2$. Voir II::1.5(1.5.3).

p. 69 La relation

$$\Psi_{\overline{a}\cdot\overline{b}}(\overline{s}) = \overline{a} \cdot \overline{b} \cdot \overline{s} = \overline{a}\Psi_{\overline{b}}(\overline{s}) = (\Psi_{\overline{a}} \circ \Psi_{\overline{b}})(\overline{s}), \quad \overline{s} \in \mathbb{Z}_n$$

montre que Ψ est un morphisme. Ensuite si $\Psi_{\overline{a}}$ est le morphisme nul (constamment égal à $\overline{0}$) alors en particulier $\Psi_{\overline{a}}(\overline{1}) = \overline{0}$ donc $\overline{a} = \overline{0}$ et cela montre l'injectivité.

p. 70 Nous avons $a^p - a = a(a^{p-1} - a)$. Si a est premier avec p alors, d'après le théorème 11, p divise le second facteur ; sinon il divise le premier

p. 70 Puisque l'ensemble de départ et d'arrivée sont finis et identiques, pour montrer que ψ est bijective, il suffit de vérifier qu'elle est injective. Or $\psi(x) = \psi(y) \implies \overline{a} \cdot x = \overline{a} \cdot y \implies \overline{a} \cdot (x - y) = 0$. Puisque $\mathbb{Z}_p$ est intègre (c'est un corps), la relation $\overline{a} \cdot (x - y) = 0$ entraîne $\overline{a} = \overline{0}$ ou $x - y = 0$. La première alternative est impossible puisque p ne divise pas a. Par conséquent $x = y$ est ψ est injective. Puisque $\psi(\overline{0}) = \overline{O}$, ψ est aussi de bijection de $(\mathbb{Z}_p)^\star$ dans lui-même. Cela montre que Maintenant, puisque ψ est bijective, nous avons

$$\prod_{x \in \mathbb{Z}_p^\star} x = \prod_{x \in \mathbb{Z}_p^\star} \overline{a} \cdot x,$$

car les deux côtés sont donnés par le produit de tous les éléments non nuls de $\mathbb{Z}_p$. Nous en tirons

$$\overline{a}^{p-1} \cdot \prod_{x \in \mathbb{Z}_p^\star} x = \prod_{x \in \mathbb{Z}_p^\star} x.$$

Le théorème de Fermat en découle car nous pouvons simplifier par le terme non nul $\prod_{x \in \mathbb{Z}_p^\star} x$. L'application ψ est-elle un morphisme d'anneau ? de groupe ?

p. 74 Soit $a \in A$ et $i \in I$. Nous avons $\mathbf{cl}(a) = \mathbf{cl}(a+i)$ et $\mathbf{cl}(a) = \mathbf{cl}(a+0_A)$. La consistance exige que $(a^2 \,\mathsf{R}_I\, a(a+i)$ c'est-à-dire $a^2 - a(a+i) \in I$ ce qui force $ai \in I$.

p. 74 Nous savons déjà que I est un sous-groupe de $(A,+)$. Il suffit de vérifier que pour tout i et i' dans I, nous avons $ii' \in I$. Cela est déjà vrai même sas supposer que $i \in I$.

p. 75 Si $b \in \langle a \rangle$ alors $b = ca$ avec $c \in A$. Comme $a \in I$ et I est un idéal $ca \in I$ de sorte que $b \in I$ ce qui montre que $\langle a \rangle \subset I$. Le lecteur pourra vérifier qu'un sous-ensemble I de A est un idéal si et seulement si

$$I = \cup_{a \in I} \langle a \rangle.$$

p. 75 Puisque $a \in \langle b \rangle$, il existe x dans A tel que $a = xb$. De la même manière, puisque $b \in \langle a \rangle$, il existe $y \in A$ tel que $b = ya$. Il suit que $a = xb = xya \implies (1_A - xy)a = 0_A$. puisque A est intègre et $a \neq 0_A$, nous avons $xy = 1_A$ donc x et y sont inversibles. En revenant à la relation $a = xb$ nous avons le résultat demandé.

p. 75 Rechercher cet exemple dans $(M_2(\mathbb{R}),+,.)$ en considérant un ensemble I de la forme $\{MA \ : \ M \in M_2(\mathbb{R})\}$ qui satisfait une seule des deux conditions dès lors que A n'est pas une matrice de la forme λId. Voir le théorème I::47.

p. 83 On peut prendre $p(X) = \bar{4}X + \bar{3}$ qui satisfait $P^2(X) = \bar{1}$.

p. 84 L'ensemble de toutes les fonctions $\mathscr{F}(\mathbb{Z}_2)$ lui-même contient seulement quatre éléments et chacun peut-être donné par une fonction polynomiale : $\mathbf{F}_{\mathbb{Z}_2}(\bar{0})$, $\mathbf{F}_{\mathbb{Z}_2}(\bar{1})$, $\mathbf{F}_{\mathbb{Z}_2}(\bar{1}X)$, $\mathbf{F}_{\mathbb{Z}_2}(\bar{1}X + \bar{1})$. Les éléments de $\ker \mathbf{F}_A$ sont les polynômes qui contiennent un nombre pair de coefficients non nuls.