Structures algébriques

Didier Piau et Bernard Ycart

L'expérience indique que l'étude abstraite des structures algébriques peut se révéler fascinante ou épuisante selon la personnalité de chacun. Un inconvénient, peut-être inévitable, de cette étude est qu'il est difficile de mettre immédiatement en relief l'utilité des résultats démontrés ; il faut passer un certain temps dans la théorie, puis de nouveau un certain temps dans des chapitres plus concrets où les résultats accumulés seront recyclés.

Tentons cependant de rassurer le lecteur grâce à la constatation suivante (à moins que cette constatation ne l'effraie encore plus) : une bonne part des résultats énoncés sur les groupes finis (concept d'ordre, théorème de Lagrange, etc.) aura l'occasion d'être mise en application dès le chapitre d'arithmétique. En effet, une première utilité de la théorie des groupes est de formaliser et systématiser les calculs usuels qu'on sait pratiquer sur les ensembles de nombres.

L'autre point de vue sur lequel on peut insister est celui des groupes formés de bijections, mais malheureusement on aura peu l'occasion de les voir vraiment appliqués dans la suite de ce cours de première année. En revanche, on peut affirmer que des connaissances sur les groupes de permutations (groupes de bijections des ensembles finis) sont bien utiles de ci de là, en informatique par exemple. Et de toutes façons l'investissement sera rentabilisé dès que le lecteur apprendra plus de géométrie, ce qui reste un cadre idéal d'usage des groupes de transformations.

Table des matières

8 novembre 2011

1 Cours

1.1 Relations

Vous avez déjà rencontré cette notion dans votre cursus ; rappelons qu'intuitivement, une relation sur un ensemble E est la description de liens entre certains éléments de E. Donnons des exemples avant même la définition.

Exemple 1. 1) La relation « est inférieur ou égal à » sur l'ensemble $\mathbb{R}$ des réels : pour deux réels x et y, on peut avoir $x \leqslant y$ ou non.
2) La relation « est inclus dans » sur l'ensemble des parties d'un ensemble : pour deux parties A et B, on peut avoir $A \subset B$ ou $B \subset A$ ou aucun des deux.
3) La relation « a le même cardinal que » sur l'ensemble des parties d'un ensemble fini.
4) Plus exotique : la relation « coïncide en au moins un point avec » pour des fonctions définies sur un même ensemble.

Définition 1. *Le* graphe *d'une relation $\mathcal{R}$ sur un ensemble E est l'ensemble des couples (a, b) de $E \times E$ tels que $a\mathcal{R}b$.*

Sermon

Attention à bien lire cette définition, qui, comme toutes ses consœurs de la suite de ce cours, peut être mal retenue par de jeunes âmes peu scrupuleuses mathématiquement parlant. Il est facile de retenir que le graphe de $\mathcal{R}$ a un rapport avec $a\mathcal{R}b$. Mais soulignons que le graphe est un *ensemble*.

Profitons en pour signaler dès l'abord que les divers objets qui sont définis dans ce cours entrent dans un petit nombre de catégories : souvent des ensembles, assez souvent des applications, souvent des n-uplets (qui ne sont rien d'autres que des applications particulières, sauriez-vous préciser pourquoi ?), souvent aussi des nombres (entiers, réels ou autres), plus rarement des relations, etc. Il n'est pas difficile de savoir dans quelle catégorie ranger les graphes : ce ne sont manifestement pas des triplets, ni des nombres complexes ! Le plus important est de ne pas oublier de les ranger quelque part. Savoir à quelle catégorie appartient un objet permet d'éviter les bourdes les plus monumentales : ainsi, le symbole $\cap$ aura un sens entre deux ensembles, pas entre deux réels, et réciproquement pour le symbole $+$. On profitera du fait que la première phrase de cette section contient les mots « élément » et « ensemble » pour vérifier qu'on ne confond pas les deux.

C'était la fin de notre sermon d'aujourd'hui.

Voici maintenant quatre définitions rébarbatives, mais incontournables.

Définition 2. *Soit E un ensemble et $\mathcal{R}$ une relation sur E.*

1) La relation $\mathcal{R}$ est réflexive *lorsque pour tout élément a de E, $a\mathcal{R}a$.*

2) La relation $\mathcal{R}$ est symétrique *lorsque pour tous éléments a et b de E, si $a\mathcal{R}b$, alors $b\mathcal{R}a$.*

3) La relation $\mathcal{R}$ est transitive *lorsque pour tous éléments a, b et c de E, si $a\mathcal{R}b$ et si $b\mathcal{R}c$, alors $a\mathcal{R}c$.*

4) La relation $\mathcal{R}$ est anti-symétrique *lorsque pour tous éléments a et b de E, si $a\mathcal{R}b$ et si $b\mathcal{R}a$, alors $a = b$.*

Quelques commentaires sur la dernière condition, qui est sans doute la plus difficile à bien mémoriser des quatre : c'est, comme son nom l'indique, en gros le contraire de la propriété de symétrie. La symétrie exige que quand deux éléments sont liés dans un sens, ils le sont aussi dans l'autre. L'anti-symétrie, c'est approximativement demander que si deux éléments sont liés dans un sens, ils ne le sont pas dans l'autre. Mais cette condition empêcherait un élément d'être lié à lui-même, ce qui ne serait pas désespérant en soi mais ne serait pas conforme à l'usage. De fait, l'usage s'est fait de compliquer la définition afin de garder la permission pour un élément d'être lié à lui-même.

On comprendra peut-être un peu mieux la définition en écrivant la contraposée de l'implication qu'elle contient.

Autre formulation de la définition de l'anti-symétrie *Une relation $\mathcal{R}$ sur un ensemble E est anti-symétrique lorsque pour tous éléments a et b distincts de E, on ne peut avoir simultanément $a\mathcal{R}b$ et $b\mathcal{R}a$.*

Comme nous sommes encore débutants, faisons l'effort d'expliciter une autre façon de présenter la même notion.

Autre formulation de la définition de l'anti-symétrie *Une relation $\mathcal{R}$ sur un ensemble E est anti-symétrique lorsque pour tous éléments a et b distincts de E, $a\mathcal{R}b$ est faux ou $b\mathcal{R}a$ est faux.*

Bien évidemment, ce genre de liste de formulations équivalentes n'est surtout pas à « savoir par cœur ». Ce qui est par contre indispensable, c'est de se familariser avec les petites manipulations qui permettent de passer de l'une à l'autre, selon les besoins.

En pratique, les relations qui pourront nous intéresser dans ce cours ne seront jamais bien compliquées ; le vocabulaire que nous avons dû ingurgiter depuis le début de ce chapitre n'a d'utilité que pour savoir reconnaître deux types très particuliers de relations : les relations d'ordre, auxquelles cette section est consacrée, puis, dans la section prochaine, les relations d'équivalence.

Définition 3. *Une relation est une* relation d'ordre *lorsqu'elle est simultanément réflexive, transitive et anti-symétrique.*

Considérons par exemple la relation « divise » sur l'ensemble $E = \{1, 2, 3, 4, 5, 6\}$. C'est une relation d'ordre ; son graphe est visualisé par des flèches sur la figure 1.

Intuitivement, une relation d'ordre est une relation qui peut raisonnablement être appelée « est supérieur ou égal à » ou, bien sûr, « est inférieur ou égal à ».

Exemple 2. *La relation « $\leqslant$ » sur $E = \mathbb{R}$ est une relation d'ordre. Pour tout ensemble A fixé, la relation « $\subset$ » sur $E = \mathcal{P}(A)$ est une relation d'ordre. La seconde est sans*

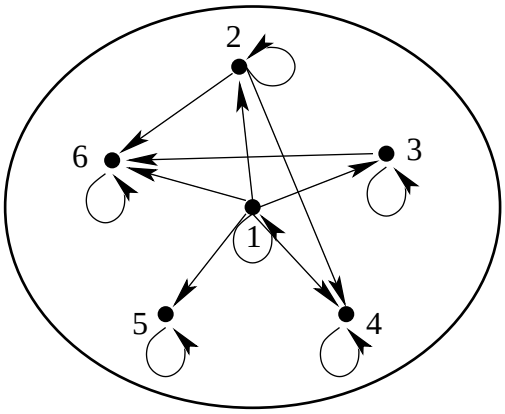

FIGURE 1 – Représentation graphique de la relation « divise » sur $\{1, 2, 3, 4, 5, 6\}$.

doute plus compliquée à maîtriser que la première dans la mesure où deux parties de A ne sont pas forcément comparables l'une à l'autre.

Le morceau est plus sérieux pour les relations d'équivalence que pour les relations d'ordre, car on ne va pas se contenter de donner une définition, mais on va aussi voir le lien avec un autre concept. Pour expliquer intuitivement ce qui va suivre, une relation d'équivalence est une relation qui peut raisonnablement s'appeler « est de la même catégorie que » et une partition est une répartition en catégories.

Définition 4. *Une relation est une* relation d'équivalence *lorsqu'elle est simultanément réflexive, symétrique et transitive.*

Exemple 3. *L'égalité sur n'importe quel ensemble E fixé. La relation « a même parité que » sur l'ensemble $\mathbb{N}$ des entiers naturels. La relation « est confondue avec ou parallèle à » sur l'ensemble des droites d'un plan affine.*

Avalons encore trois définitions de plus en plus indigestes mais ce n'est pas gratuit, les concepts serviront plus loin, notamment en arithmétique.

Définition 5. *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E, et soit a un élément de E. On appelle* classe d'équivalence *de a modulo $\mathcal{R}$ l'ensemble*

$$\{x \in E \mid a\mathcal{R}x\}.$$

Avec des mots, la classe d'équivalence de a est l'ensemble formé des éléments de la même catégorie que a.

Notation 1. *On note $\mathfrak{cl}_{\mathcal{R}}(a)$ la classe d'équivalence d'un élément a de E pour la relation d'équivalence $\mathcal{R}$.*

On abrège souvent $\mathfrak{cl}_{\mathcal{R}}(a)$ en $\mathfrak{cl}(a)$. Une autre notation pour la classe d'équivalence de a est $\dot{a}$ mais nous l'utiliserons rarement dans ce cours. Par contre, nous désignerons souvent les relations d'équivalence par le signe $\sim$.

Sans commentaires, car il y en aura plus loin, un objet plus étrange :

Définition 6. *Soit $\sim$ une relation d'équivalence sur un ensemble E. On appelle* ensemble-quotient *de E par la relation $\sim$ l'ensemble :*

$$\{\, \mathfrak{cl}(a) \mid a \in E \,\}.$$

Attention tout de même ! Comme $\mathfrak{cl}(a)$ est une partie (et non un élément) de E, l'ensemble-quotient est un ensemble de parties de E. Ce n'est pas une partie de E mais une partie de $\mathcal{P}(E)$. Ce n'est pas si compliqué, mais il ne faut pas s'y perdre.

Notation 2. *L'ensemble-quotient de E par $\sim$ est noté $E/\sim$.*

On remarquera qu'en général, chaque élément c de l'ensemble quotient $E/\sim$ peut s'écrire comme $c = \mathfrak{cl}(a)$ pour de nombreux éléments a différents de E : très précisément, c s'écrit $c = \mathfrak{cl}(a)$ pour un élément a de E tel que $a \in c$, et aussi $c = \mathfrak{cl}(b)$ pour tous les éléments b de E tels que $a \sim b$.

Définition 7. *Une* partition *d'un ensemble E est un ensemble $\mathcal{Q}$ de parties de E vérifiant les trois propriétés suivantes :*
(i) L'ensemble vide n'est pas un élément de $\mathcal{Q}$.
(ii) Deux éléments distincts de $\mathcal{Q}$ sont disjoints.
(iii) Tout élément de E appartient à un élément de $\mathcal{Q}$.

C'est dur à avaler parce qu'on rentre inévitablement dans le monde des ensembles dont les éléments sont eux-mêmes des ensembles. Les éléments de $\mathcal{Q}$ sont des parties de E et doivent donc être pensés comme des groupes d'éléments de E vérifiant une condition commune. Et $\mathcal{Q} \subset \mathcal{P}(E)$: une partition de E est une partie de l'ensemble des parties de E (ouf !).

Exemple 4. *En notant $I \subset \mathbb{N}$ l'ensemble des entiers impairs et $P \subset \mathbb{N}$ l'ensemble des entiers pairs, $\{I, P\}$ est une partition de $\mathbb{N}$.*

Tentons maintenant de commenter les conditions de la définition 7. La condition (i) est sans grand intérêt et juste là pour que les énoncés marchent bien. La condition (ii) nous assure qu'on n'a inscrit aucun élément de E dans deux catégories à la fois. La condition (iii) signifie qu'on n'a oublié d'inscrire personne : tout élément de E est dans un groupe.

On remarquera qu'on peut regrouper les deux conditions significatives, ce qui donne l'énoncé suivant.

Autre formulation de la définition d'une partition *Une partition d'un ensemble E est un ensemble $\mathcal{Q}$ de parties de E vérifiant les deux propriétés (i) et (iv) ci-dessous :*

(i) L'ensemble vide n'est pas un élément de $\mathcal{Q}$.
(iv) Tout élément de E appartient à un et un seul élément de $\mathcal{Q}$.

Bien évidemment là encore il n'est pas question d'apprendre par cœur ce genre de reformulation. Il faut se convaincre, et ici ce n'est peut-être pas facile, qu'elle est bien équivalente à la précédente.

Et voici maintenant la synthèse finale, qui expliquera ce qu'est un ensemble-quotient à ceux qui ont compris ce qu'est une partition, et expliquera ce qu'est une partition à ceux qui ont compris ce qu'est un ensemble-quotient (figure 2).

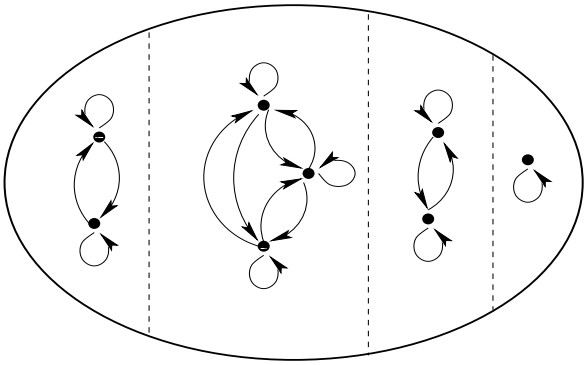

FIGURE 2 – Représentation graphique d'une relation d'équivalence. Partition en classes d'équivalence.

Proposition 1. *Soit $\sim$ une relation d'équivalence sur un ensemble E. L'ensemble-quotient $E/\sim$ est une partition de E.*

Complément *Toute partition de A peut s'obtenir ainsi comme quotient par une relation d'équivalence de E et cette relation d'équivalence est unique.*

La preuve du complément est laissée au lecteur.

Démonstration : Vérifions successivement les trois propriétés définissant une partition.

Vérification de (i) : Soit A un élément de $E/\sim$. Par définition de $E/\sim$, il existe un élément a de E tel que $A = \mathfrak{cl}(a)$. Comme $\sim$ est réflexive, $a \sim a$, donc a appartient à $\mathfrak{cl}(a) = A$. Ainsi A n'est pas réduit à l'ensemble vide.

Vérification de (ii) : Soient A et B deux éléments de $E/\sim$. On peut trouver des éléments a et b de E tels que $A = \mathfrak{cl}(a)$ et $B = \mathfrak{cl}(b)$. On doit montrer que si A et B sont distincts, ils sont alors disjoints, et on va procéder par contraposition, c'est-à-dire en montrant que si A et B ne sont pas disjoints, ils sont égaux.

Supposons donc A et B non disjoints. L'objectif est de prouver que $A = B$, on va montrer successivement les inclusions $A \subset B$ et $B \subset A$.

Par l'hypothèse qu'on vient de faire, on peut prendre un élément c de E qui appartient simultanément à A et à B.

Première inclusion : Montrons tout d'abord que $A \subset B$. Pour ce faire, prenons un $x \in A$ quelconque et prouvons que $x \in B$.

Comme $x \in A = \mathfrak{cl}(a)$, par définition d'une classe d'équivalence, on obtient $a \sim x$. Comme $c \in A = \mathfrak{cl}(a)$, on obtient de même $a \sim c$, puis, grâce à la symétrie de $\sim$, on obtient $c \sim a$. Comme $c \in B = \mathfrak{cl}(b)$, on obtient enfin $b \sim c$. En mettant bout à bout les trois informations ainsi obtenues ($b \sim c$, $c \sim a$ et $a \sim x$) et en jouant deux fois sur la transitivité de $\sim$, on obtient alors que $b \sim x$, c'est-à-dire que $x \in B$.

Ceci prouve bien que $A \subset B$.

Deuxième inclusion : L'astuce est ici classique, elle consiste à remarquer que nos hypothèses (à savoir que A et B sont des classes d'équivalence, et qu'elles ne sont pas disjointes) sont symétriques en A et B. Dès lors, en échangeant A et B dans le morceau précédent de la preuve, on obtient bien l'inclusion $B \subset A$.

Par double inclusion, on a donc $A = B$.

Finalement, on a montré que si $A \cap B \neq \emptyset$, alors $A = B$. La propriété (ii) est prouvée. Ouf, c'était le plus gros morceau !

Vérification de (iii) : Soit a un élément de E. Comme $\sim$ est réflexive, a appartient à $\mathfrak{cl}(a)$, et de ce fait on a bien trouvé un élément de $E/\sim$ dont a est lui-même élément. C'est fini ! □

1.2 Lois de composition et morphismes

Définition 8. *On appelle* loi de composition *sur un ensemble E une application de $E \times E$ vers E.*

En fait, bien que cette définition soit générale, on n'aurait pas l'idée d'appeler « loi de composition » n'importe quelle application de $E \times E$ vers E ; le vocable n'est utilisé que quand il est naturel de noter l'application par un symbole opératoire. Des exemples typiques de lois de composition sont l'addition $+$ de $\mathbb{R}^2$ vers $\mathbb{R}$, qui associe $x + y$ à (x, y) ; ou bien la loi de composition $\circ$ sur l'ensemble E^E des applications de E vers E, qui associe l'application $f \circ g$ au couple d'applications (f, g). Pour des lois de composition abstraites, le symbole opératoire $*$ a été à la mode et nous l'utiliserons occasionnellement, surtout au début, mais nous nous contenterons rapidement de la notation multiplicative $a \cdot b$, ou même simplement ab, pour l'élément obtenu en appliquant la loi de composition à (a, b).

Voici un peu de vocabulaire au sujet des lois de composition.

Définition 9. *Soit $*$ une loi de composition sur un ensemble E.*

1. *On dit que $*$ est* commutative *lorsque pour tous éléments a et b de E,*

$$a * b = b * a.$$

2. *On dit que $*$ est* associative *lorsque pour tous éléments a, b et c de E,*

$$(a * b) * c = a * (b * c).$$

3. *On dit qu'un élément e de E est* élément neutre *pour $*$ lorsque pour tout élément a de E,*

$$a * e = e * a = a.$$

La cohérence de ce qui suit nécessite d'énoncer tout de suite un résultat simplissime.

Proposition 2. *Une loi de composition possède au plus un élément neutre.*

Démonstration : Soit e_1 et e_2 deux éléments neutres pour une loi de composition $*$. Comme e_2 est neutre, $e_1 * e_2 = e_1$ et comme e_1 est neutre, $e_1 * e_2 = e_2$. Donc $e_1 = e_2$. □

On parlera donc de l'élément neutre avec l'article défini, lorsqu'il existe un élément neutre.

Définition 10. *Soit $*$ une loi de composition sur un ensemble E admettant un élément neutre noté e et soit a un élément de E. On dit qu'un élément b de E est* symétrique *(ou* inverse*) de a lorsque*

$$a * b = b * a = e.$$

Là encore, glissons sans tarder une évidence.

Proposition 3. *Soit $*$ une loi de composition sur un ensemble E, associative et possédant un élément neutre. Chaque élément possède au plus un symétrique.*

Démonstration : Soit e le neutre de $*$, soit a un élément de E et soient b_1 et b_2 deux symétriques de a. Alors d'une part $(b_1 * a) * b_2 = e * b_2 = b_2$ et d'autre part $b_1 * (a * b_2) = b_1 * e = b_1$. Par associativité de la loi de composition, $(b_1 * a) * b_2 = b_1 * (a * b_2)$, d'où $b_1 = b_2$. □

Les lois de composition intéressantes étant en pratique associatives, on pourra donc faire plein usage de la notation suivante.

Notation 3. *Le symétrique d'un élément a est noté a^{-1}.*

Maintenant que nous savons manipuler une loi de composition sur un seul ensemble, apprenons à évoluer d'un ensemble muni d'une loi de composition vers un autre.

Définition 11. *Soit E un ensemble muni d'une loi de composition $*$ et F un ensemble muni d'une loi de composition $\cdot$. On dit qu'une application $f : E \to F$ est un* morphisme *lorsque pour tous éléments a et b de E, on a l'identité :*

$$f(a * b) = f(a) \cdot f(b).$$

Définition 12. *Un morphisme* bijectif *est appelé un* isomorphisme.

Il semble plus facile d'expliquer la notion d'isomorphisme que celle de morphisme en général ; deux lois de composition sur deux ensembles fourniront des structures isomorphes lorsque ces deux lois de composition agissent de la même façon, seuls les noms des éléments changeant. La phrase précédente n'étant peut-être pas si claire que cela, donnons plutôt des exemples, c'est toujours bien les exemples.

Exemple 5. Considérons tout d'abord la bijection σ de l'ensemble $E = \{0, 1, 2, 3\}$ définie par

$$\sigma(0) = 1, \quad \sigma(1) = 2, \quad \sigma(2) = 3, \quad \sigma(3) = 0.$$

Avec à peine un peu de bon sens (tout mathématicien pense très vite à σ comme « faisant tourner » les quatre éléments de E), on voit sans guère de calculs que $\sigma \circ \sigma$ est la bijection τ de E définie par

$$\tau(0) = 2, \quad \tau(1) = 3, \quad \tau(2) = 0, \quad \tau(3) = 1,$$

puis que $\sigma \circ \sigma \circ \sigma$ est la bijection ϱ de E définie par

$$\varrho(0) = 3, \quad \varrho(1) = 0, \quad \varrho(2) = 1, \quad \varrho(3) = 2,$$

et enfin que $\sigma \circ \sigma \circ \sigma \circ \sigma$ est tout simplement l'identité de E, que l'on note désormais e.

Pour abréger les calculs qui suivent, introduisons une notation.

Notation 4. *Pour tout élément a d'un ensemble E muni d'une loi de composition $*$ et pour tout entier $n \geqslant 1$, notons a^{*n} la composition de a avec lui-même n fois. Ainsi, $a^{*1} = a$ puis, pour tout $n \geqslant 1$, $a^{*n+1} = a^{*n} * a$. Si la loi de composition $*$ est munie d'un neutre e, on notera aussi $a^{*0} = e$. Enfin, on abrège souvent a^{*n} en a^n.*

En utilisant cette notation, on peut très facilement calculer tous les produits deux à deux des bijections introduites ici ; par exemple $\varrho \circ \tau = \sigma^3 \circ \sigma^2 = \sigma^5 = \sigma^4 \circ \sigma = e \circ \sigma = \sigma$.

On considère alors l'ensemble $S = \{e, \sigma, \tau, \varrho\}$ et on voit que $\circ$ est une loi de composition sur ce sous-ensemble de E^E, qui sera agréablement décrite par le tableau suivant, que l'on appelle une *table de composition*.

$\circ$	e	σ	τ	ϱ
e	e	σ	τ	ϱ
σ	σ	τ	ϱ	e
τ	τ	ϱ	e	σ
ϱ	ϱ	e	σ	τ

Considérons à présent l'ensemble des nombres complexes dont la puissance quatrième vaut 1, c'est-à-dire l'ensemble $F = \{1, \mathrm{i}, -1, -\mathrm{i}\}$. Il est très facile de constater

que la multiplication des nombres complexes définit une loi de composition sur F, dont la table est donnée ci-dessous.

$\circ$	1	i	-1	$-$i
1	1	i	-1	$-$i
i	i	-1	$-$i	1
-1	-1	$-$i	1	i
$-$i	$-$i	1	i	-1

Visuellement, on retrouve la même table, seuls les noms des éléments ont changé. C'est signe qu'il y a un isomorphisme camouflé. On le détectera facilement ; c'est bien sûr l'application g de E vers F définie par :

$$g(e) = 1 \qquad g(\sigma) = \mathrm{i} \qquad g(\tau) = -1 \qquad g(\varrho) = -\mathrm{i}.$$

Exemple 6. Soit R l'ensemble des rotations de centre $(0, 0)$ dans le plan, et soit $\mathbb{U}$ le cercle-unité de $\mathbb{C}$, c'est-à-dire l'ensemble des nombres complexes de module 1. Les lois de composition respectivement envisagées sur R et sur $\mathbb{U}$ sont la composition des applications et la multiplication. On définit une application $f : R \to \mathbb{U}$ en envoyant la rotation d'angle θ sur le nombre $\mathrm{e}^{\mathrm{i}\theta}$.

Il faut tout d'abord se soucier de vérifier que cette définition n'est pas ambiguë, car elle n'est pas loin de l'être ! Une rotation peut en effet être caractérisée par plusieurs angles (tourner d'un quart de tour dans le sens trigonométrique, c'est aussi tourner de trois quarts de tour dans le sens des aiguilles d'une montre), mais deux angles distincts θ_1 et θ_2 correspondant à la même bijection diffèrent d'un multiple entier de 2π ; il existe donc un entier $k \in \mathbb{Z}$ tel que $\theta_2 = \theta_1 + 2k\pi$. Les valeurs $\mathrm{e}^{\mathrm{i}\theta_1}$ et

$$\mathrm{e}^{\mathrm{i}\theta_2} = \mathrm{e}^{\mathrm{i}\theta_1 + 2k\mathrm{i}\pi} = \mathrm{e}^{\mathrm{i}\theta_1}(\mathrm{e}^{2\mathrm{i}\pi})^k = \mathrm{e}^{\mathrm{i}\theta_1}$$

sont donc égales, et l'application f est bien définie.

Une fois cette mise au point effectuée, vérifier que f est un morphisme est sans problème : si ϱ_1 est la rotation d'angle θ_1 et ϱ_2 la rotation d'angle θ_2, la composée $\varrho_1 \circ \varrho_2$ est la rotation ϱ d'angle $\theta_1 + \theta_2$, et on a donc :

$$f(\varrho_1 \circ \varrho_2) = f(\varrho) = \mathrm{e}^{\mathrm{i}(\theta_1+\theta_2)} = \mathrm{e}^{\mathrm{i}\theta_1}\mathrm{e}^{\mathrm{i}\theta_2} = f(\varrho_1)f(\varrho_2).$$

Montrer que f est bijective n'est pas difficile ; on en conclut que f est un isomorphisme, en d'autres termes que l'étude des nombres complexes de module 1 nous instruira sur le fonctionnement des rotations.

Exemple 7. Voici enfin un morphisme qui n'est pas un isomorphisme et qui est pourtant une simple variante du précédent. Considérons l'application F de $\mathbb{R}$ (muni de

l'addition) vers $\mathbb{U}$ (le même qu'à l'exemple précédent, muni de la multiplication) définie par $F(\theta) = \mathrm{e}^{\mathrm{i}\theta}$. On voit facilement que F est un morphisme, mais comme, par exemple, $F(0) = F(2\pi)$, F n'est pas une bijection donc pas un isomorphisme.

À l'évidence (et c'est sans doute ce que vous fîtes au lycée), on peut voir F comme l'application qui « enroule » de façon régulière une corde (la droite $\mathbb{R}$) sur une roue (le cercle $\mathbb{U}$), encore et encore.

1.3 Groupes

Définition 13. *Soit G un ensemble muni d'une loi de composition $*$. On dit que G est un* groupe *lorsque les trois conditions suivantes sont réalisées :*
(i) La loi de composition $*$ est associative.
(ii) La loi de composition $*$ possède un élément neutre.
(iii) Tout élément de G possède un symétrique pour $*$.

Définition 14. *Un groupe G est dit* abélien *(ou* commutatif*) lorsque sa loi de composition est commutative.*

Avant de donner des exemples, quelques remarques d'ordre purement calculatoire sur les groupes. Comme promis plus haut, on utilise désormais la notation multiplicative, donc ab désigne le composé des éléments a et b d'un groupe G.

Proposition 4. *Soit G un groupe. Alors pour tous éléments a, b et x de G :*
1) Si $ax = bx$, alors $a = b$.
2) Si $xa = xb$, alors $a = b$.
3) Le symétrique de ab est $b^{-1}a^{-1}$.

Démonstration : Il n'y a que des vérifications simples et basées sur l'associativité ; pour (1), si on suppose $ax = bx$, en multipliant à droite par x^{-1} on obtient $(ax)x^{-1} = (bx)x^{-1}$ et donc $a(xx^{-1}) = b(xx^{-1})$, c'est-à-dire $a = b$. On prouve (2) de la même façon en multipliant à gauche par x^{-1}. La preuve du (3) se réduit à deux calculs élémentaires :

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e,$$

et

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e,$$

ce qui conclut la démonstration. □

Remarque Au fait, pourquoi faut-il effectuer les deux calculs élémentaires ci-dessus ? Un seul ne suffirait-il pas ? La réponse est non ; on rappelle que y est le symétrique de x si xy **et aussi** yx valent e.

Maintenant que l'on sait calculer dans les groupes, il est temps de donner les exemples les plus élémentaires : regardons les lois de composition que nous connaissons le mieux, elles concernent les ensembles de nombres usuels.

Additions : elles sont associatives, ont un élément neutre noté 0. Dans $\mathbb{N}$, le symétrique peut faire défaut ; ainsi 2 n'a pas d'opposé. Dans $\mathbb{Z}$ (puis dans les ensembles usuels bien connus), l'opposé existe. Ainsi $\mathbb{Z}$ est un groupe pour l'addition.

Multiplication : 0 n'a jamais d'inverse, donc les ensembles de nombres bien connus ne sont jamais des groupes pour la multiplication. En revanche, si on considère le sous-ensemble formé des éléments non nuls, la multiplication y est bien définie, elle est associative et elle possède un élément neutre noté 1. Le point à problème est l'existence du symétrique (de l'inverse en notation multiplicative). Dans $\mathbb{Z}^*$, il fait défaut à la plupart des éléments, ainsi 2 n'a pas d'inverse ; $\mathbb{Z}^*$ n'est donc pas un groupe. En revanche, dans $\mathbb{Q}^*$ (l'ensemble des fractions non nulles) ou $\mathbb{R}^*$ ou $\mathbb{C}^*$, l'existence de l'inverse ne pose pas de problème. Tous ces ensembles sont donc des groupes multiplicatifs.

Encore quelques propriétés de bon sens, mais qu'il ne coûte rien d'énoncer. Elles paraissent évidentes si on comprend qu'un morphisme est moralement une application qui transporte la structure ; si elle transporte la loi de composition, elle doit aussi transporter ses caractéristiques, telles que l'élément neutre et le symétrique.

Proposition 5. *Soit f un morphisme d'un groupe G, d'élément neutre e, vers un groupe G', d'élément neutre e'.*

Alors $f(e) = e'$ et, pour tout élément a de G, $[f(a)]^{-1} = f(a^{-1})$.

Démonstration : Essentiellement de la simple vérification ; pour le neutre, il s'agit d'une (petite) astuce : on calcule $f(e)f(e) = f(ee) = f(e) = f(e)e'$ puis on simplifie par $f(e)$. Pour l'inverse, on fait un calcul très simple : $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$ et simultanément, $f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$. Ceci montre bien que $f(a^{-1})$ est l'inverse de $f(a)$. □

1.4 Exemples fondamentaux de groupes finis

Cette partie est consacrée à deux exemples fondamentaux de classes de groupes finis. La première classe est composée de groupes abéliens, la seconde de groupes non abéliens sauf dans des cas dégénérés.

Définition 15. *Pour tout entier $n \geqslant 1$, appelons Z_n le groupe*

$$Z_n = \{0, 1, \ldots, n-1\},$$

muni de la loi de composition, notée $\oplus$, définie comme suit. Si les éléments i et j de Z_n sont tels que $i + j \leqslant n - 1$, on pose $i \oplus j = i + j$. Sinon, $i + j \geqslant n$ et on pose $i \oplus j = i + j - n$.

Proposition 6. *Pour tout $n \geqslant 1$, $(Z_n, \oplus)$ est un groupe abélien de neutre 0.*

Démonstration : Le seul point notable est que l'inverse de 0 vaut 0 et celui d'un élément $i \neq 0$ vaut $n - i$. □

On verra plus tard une présentation plus intrinsèque des groupes Z_n comme quotients du groupe $\mathbb{Z}$ muni de l'addition. Profitons tout de même du moment pour introduire une définition.

Définition 16. *Soit G un groupe de loi de composition $*$ et de neutre e et soit a un élément de G. L'**ordre** de a est le plus petit entier $k \geqslant 1$, s'il existe, tel que $a^{*k} = e$. Sinon on dit que l'ordre de a est infini.*

Bien sûr, l'ordre du neutre vaut toujours 1 et l'ordre de tout élément d'un groupe fini de cardinal fini n est fini et inférieur ou égal à n. Nous verrons bientôt que c'est forcément un diviseur de n.

Outre les groupes Z_n, les groupes les plus directement utilisables sont sans doute ceux qui interviennent en géométrie. Ce sont des groupes de transformations « respectant » telle ou telle propriété ; ainsi les isométries, qui conservent les distances, ou les similitudes, qui conservent les angles. Et ils constituent notre deuxième classe d'exemples.

Tous ces groupes ont le point commun d'avoir pour loi de composition $\circ$, la composition des applications, et d'être formés de bijections.

Fondamentale (quoique très facile) sera donc l'affirmation suivante.

Proposition 7. *Soit E un ensemble. L'ensemble des bijections de E dans lui-même forme un groupe pour la composition.*

Démonstration : Tout est très simple. On vérifie que, pour toute bijection f de E, la bijection réciproque est un symétrique de f ; que la composée de deux bijections est une bijection, par exemple parce que $g^{-1} \circ f^{-1}$ se révèle un inverse de $f \circ g$; que la composition est associative ; et enfin que id_E est son neutre. On a déjà fini ! □

Notation 5. *Soit E un ensemble. L'ensemble des bijections de E dans lui-même est noté $\mathcal{S}(E)$.*

On utilise souvent (au moins en mathématiques, en informatique et en analyse du génome) le cas particulier du groupe des bijections d'un ensemble fini. L'archétype d'un tel ensemble fini étant $\{1, \ldots, n\}$, cela justifie d'introduire une toute spéciale notation.

Notation 6. *Pour tout entier $n \geqslant 1$, on note $\mathbb{N}_n = \{1, 2, \ldots, n\}$. L'ensemble des bijections de $\mathbb{N}_n$ s'appelle le groupe des permutations sur n éléments. On le note $\mathcal{S}_n$.*

Tentons de découvrir comment fonctionne le groupe des permutations $\mathcal{S}_n$ pour n pas trop gros ; il vaut même mieux prendre n franchement petit, car $\mathcal{S}_n$ possédant $n!$ éléments, on serait vite débordé.

Pour $n = 1$, le groupe n'a qu'un élément ; sa table est vite tracée.

$\circ$	e
e	e

Pour $n = 2$, il y a deux bijections de $\{1, 2\}$: celle qui échange les deux éléments, qu'on notera τ, et l'identité.

La table du groupe est donc la suivante.

$\circ$	e	τ
e	e	τ
τ	τ	e

À partir de $n = 3$, les calculs complets seraient nettement plus fastidieux. On va en profiter pour introduire des notations et énumérer les ensembles $\mathcal{S}_n$.

Notation 7. *On dispose de plusieurs notations pour désigner une permutation s élément de $\mathcal{S}_n$. La première est*

$$s = \begin{pmatrix} 1 & 2 & \cdots & n \\ s(1) & s(2) & \cdots & s(n) \end{pmatrix},$$

que l'on abrège parfois en

$$s = (s(1), s(2), \ldots, s(n)).$$

Définition 17. *Une orbite d'une permutation s élément de $\mathcal{S}_n$ est une partie*

$$\{s^{\circ k}(i)\,;\, k \geqslant 1\}, \quad i \in \mathbb{N}_n.$$

On peut expliciter la structure des orbites comme suit.

Proposition 8. *Pour toute permutation s et tout élément i de $\mathbb{N}_n$, il existe un entier $k \geqslant 1$ tel que $s^{\circ k}(i) = i$. Le plus petit entier $k \geqslant 1$ qui vérifie cette propriété est le cardinal de l'orbite de i et s'appelle la taille de l'orbite de i.*

Définition 18. *Un cycle s est un élément de $\mathcal{S}_n$ qui possède exactement une orbite de longueur différente de* 1.

Pour tout cycle s de longueur $k \geqslant 2$, il existe donc une partie $S \subset \mathbb{N}_n$ de cardinal k telle que $s(i) = i$ pour tout élément i de $\mathbb{N}_n \setminus S$. De plus, on peut numéroter les éléments de S comme suit :

$$S = \{i_1, i_2, \ldots, i_k\}, \quad s(i_j) = i_{j+1},\ 1 \leqslant j \leqslant k-1,\ s(i_k) = i_1.$$

Notation 8. *On désigne le cycle s de longueur $k \geqslant 2$ ci-dessus par l'écriture*

$$s = (i_1 i_2 \ldots i_k).$$

Avertissement On aura remarqué que la notation 8 est affreusement proche de l'écriture abrégée d'une permutation quelconque donnée dans la notation 7, la seule différence portant sur la présence ou l'absence de virgules.

Bien sûr, si le nombre d'entiers figurant dans l'écriture de s est différent de n, on désigne forcément le cycle. Dans le cas contraire, on veillera à ne pas confondre

$$a = (123) \quad \text{et} \quad e = (1, 2, 3),$$

puisque a est un cycle de longueur 3 et e est la permutation identité.

Enfin, remarquons qu'un cycle dispose de plusieurs écritures différentes, par exemple

$$a = (123) = (231) = (312).$$

Fin de l'avertissement.

Il est à présent facile d'énumérer les éléments de $\mathcal{S}_3$: outre l'identité, que l'on va noter e, il y en a trois d'apparence identique : l'un, que je noterai t, échange 1 et 2 en laissant 3 fixe ; un autre, que je me garderai astucieusement de noter, échange 2 et 3 en laissant 1 fixe ; le dernier échange 3 et 1 en laissant 2 fixe. Enfin deux autres jouent aussi des rôles voisins : l'un, que je noterai a, fait « tourner » les trois éléments de $\{1, 2, 3\}$ en envoyant 1 sur 2, 2 sur 3, et 3 sur 1 ; l'autre, dont je remarquerai que c'est le carré de a, les fait « tourner » dans l'autre sens. Ainsi,

$$t = (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad a = (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad a^2 = (132) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

On va remplir la table du groupe par ajouts successifs d'information. L'information la plus récente sera systématiquement portée en gras.

Au point où nous en sommes, il est facile de commencer en remarquant que $a^3 = e$ tandis que a^2, comme on l'a déjà dit, est distinct de a. En outre les trois autres éléments ont un carré égal à e.

$\circ$	e	a	a^2	t		
e	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{a^2}$	$\boldsymbol{t}$		
a	$\boldsymbol{a}$	$\boldsymbol{a^2}$	$\boldsymbol{e}$			
a^2	$\boldsymbol{a^2}$	$\boldsymbol{e}$	$\boldsymbol{a}$			
t	$\boldsymbol{t}$			$\boldsymbol{e}$		
					$\boldsymbol{e}$	
						$\boldsymbol{e}$

C'est le bon moment pour glisser une remarque importante : dans la table de composition d'un groupe on trouve chaque élément du groupe une fois et une seule dans

chaque ligne, et dans chaque colonne. Sauriez-vous le démontrer ? Sinon, cher lecteur, nous vous conseillons d'arrêter votre lecture et de chercher une démonstration.

Le produit at ne peut être présent deux fois dans la colonne a, ni deux fois dans la ligne t. Il est donc distinct des éléments qui y figurent déjà, c'est-à-dire de e, de a, de a^2 et de t. C'est donc un cinquième élément, qu'on peut alors faire figurer dans la cinquième ligne et la cinquième colonne du tableau. On calcule au passage sans mal $(a^2)(at) = (a^3)t = et = t$, et $(at)t = a(t^2) = ae = a$.

$\circ$	e	a	a^2	t	at	
e	e	a	a^2	t	$\boldsymbol{at}$	
a	a	a^2	e	$\boldsymbol{at}$		
a^2	a^2	e	a		$\boldsymbol{t}$	
t	t			e		
at	$\boldsymbol{at}$			$\boldsymbol{a}$	e	
						e

Puis à son tour, a^2t ne peut déjà figurer dans la ligne a^2 ni dans la colonne t : c'est donc le sixième élément. On peut l'ajouter au tableau en complétant par quelques calculs évidents.

$\circ$	e	a	a^2	t	at	a^2t
e	e	a	a^2	t	at	$\boldsymbol{a^2t}$
a	a	a^2	e	at	$\boldsymbol{a^2t}$	$\boldsymbol{t}$
a^2	a^2	e	a	$\boldsymbol{a^2t}$	t	$\boldsymbol{at}$
t	t			e		
at	at			a	e	
a^2t	$\boldsymbol{a^2t}$			$\boldsymbol{a^2}$		e

En utilisant toujours l'astuce selon laquelle il ne peut y avoir deux fois la même valeur dans une ligne ni dans une colonne, on arrive à calculer $(at)(a^2t)$ et $(a^2t)(at)$ par simple élimination de cinq valeurs impossibles.

$\circ$	e	a	a^2	t	at	a^2t
e	e	a	a^2	t	at	a^2t
a	a	a^2	e	at	a^2t	t
a^2	a^2	e	a	a^2t	t	at
t	t			e		
at	at			a	e	$\boldsymbol{a^2}$
a^2t	a^2t			a^2	$\boldsymbol{a}$	e

Surprise ! On vient de montrer avec une étonnante économie de calculs que le groupe n'est pas commutatif ; en effet $(at)(a^2t) \neq (a^2t)(at)$.

Le même truc des répétitions interdites permet de compléter le coin inférieur droit du tableau.

$\circ$	e	a	a^2	t	at	a^2t
e	e	a	a^2	t	at	a^2t
a	a	a^2	e	at	a^2t	t
a^2	a^2	e	a	a^2t	t	at
t	t			e	$\boldsymbol{a^2}$	$\boldsymbol{a}$
at	at			a	e	a^2
a^2t	a^2t			a^2	a	e

Dernier obstacle inattendu, alors que nous avions presque fini, avec la méthode, maintenant classique pour nous, de remplir les cases par élimination, cette méthode est insuffisante pour remplir les six misérables cases laissées blanches ! Il faut une nouvelle astuce pour passer cet obstacle. Concentrons-nous sur la case correspondant au produit ta. Pour calculer ce produit, bidouillons un peu : $ta = tae = ta(t^2) = [t(at)]t = a^2t$. Une nouvelle case est remplie :

$\circ$	e	a	a^2	t	at	a^2t
e	e	a	a^2	t	at	a^2t
a	a	a^2	e	at	a^2t	t
a^2	a^2	e	a	a^2t	t	at
t	t	$\boldsymbol{a^2t}$		e	a^2	a
at	at			a	e	a^2
a^2t	a^2t			a^2	a	e

Cette étape franchie, il est désormais très facile de finir de remplir la table en utilisant l'idée simple : pas plus d'une apparition par ligne ou par colonne.

$\circ$	e	a	a^2	t	at	a^2t
e	e	a	a^2	t	at	a^2t
a	a	a^2	e	at	a^2t	t
a^2	a^2	e	a	a^2t	t	at
t	t	a^2t	at	e	a^2	a
at	at	t	a^2t	a	e	a^2
a^2t	a^2t	at	t	a^2	a	e

On a donc obtenu la table complète de la loi de composition $\circ$ sur $\mathcal{S}_3$, en n'utilisant que des techniques élémentaires.

1.5 Sous-groupes

Maintenant que nous connaissons ce que nous avons pompeusement appelé les exemples fondamentaux, il reste à apprendre à tirer de ces exemples trop fondamentaux pour être vraiment utiles des exemples plus concrets.

Pour cela, introduisons une nouvelle notion.

Définition 19. *Soit G un groupe. On dit qu'un sous-ensemble H de G est un* sous-groupe *de G lorsque les trois conditions suivantes sont vérifiées :*

(i) L'ensemble H n'est pas vide.

(ii) Pour tous a et b de H, le produit ab est aussi dans H.

(iii) Pour tout a de H, l'inverse a^{-1} de a est aussi dans H.

Avant de commenter ce que ça veut dire, donnons tout de suite une proposition très simple, et utile en pratique pour vérifier qu'un sous-ensemble d'un groupe est un sous-groupe.

Proposition 9. *Soit G un groupe. Un sous-ensemble H de G est un sous-groupe de G si et seulement si les deux conditions suivantes sont vérifiées :*

(i) L'ensemble H n'est pas vide.

(iv) Pour tous a et b de H, le produit ab^{-1} est aussi dans H.

Démonstration : Supposons que H est un sous-groupe de G, c'est-à-dire qu'il vérifie (i), (ii) et (iii). Il est alors clair que (i) est vérifiée.

Montrons que H vérifie (iv). Soit a et b deux éléments de H. En appliquant (iii) à b, on constate que b^{-1} est aussi dans H, puis en appliquant (ii) à a et b^{-1} que le produit ab^{-1} aussi. Cette partie de la preuve est déjà finie !

Supposons maintenant que H vérifie (i) et (iv). Vérifier (i) est bien sûr sans problème. Avant de montrer que H vérifie (ii) et (iii), montrons préalablement que e appartient à H, où e désigne l'élément neutre de G. En effet H n'étant pas vide, on peut prendre un élément c dans H, puis appliquer l'hypothèse (iv) à c et c pour conclure que $cc^{-1} = e$ appartient à H.

Montrons maintenant que H vérifie (iii). Soit a un élément de H. Puisqu'on sait maintenant que e aussi est dans H, on peut appliquer (iv) à e et a pour obtenir $ea^{-1} \in H$, c'est-à-dire $a^{-1} \in H$.

Montrons enfin que H vérifie (ii). Soit a et b deux éléments de H. Par la propriété (iii) appliquée à b, $b^{-1} \in H$, puis par la propriété (iv) appliquée à a et b^{-1}, $a(b^{-1})^{-1} \in H$, c'est-à-dire $ab \in H$. □

Bien que le résultat qui suive soit très simple à démontrer, son importance lui fait mériter l'appellation de :

Théorème 1. *Soit G un groupe et H un sous-groupe de G. La restriction à H de la loi de composition sur G fait de H un groupe.*

Démonstration : Il ne faut pas manquer de vérifier la possibilité de restreindre la loi de composition initiale, application de $G \times G$ vers G à une loi de composition sur H, c'est-à-dire une application de $H \times H$ vers H. Comme on veut restreindre non seulement l'ensemble de départ mais aussi l'ensemble d'arrivée, on est dans la situation où il faut spécialement prendre garde. Mais la propriété (ii) de la définition des « sous-groupes » assure précisément que la loi de composition de G envoie l'ensemble $H \times H$ dans H et que la restriction a donc bien un sens.

L'associativité de cette restriction est alors évidente. Dans la preuve de la proposition précédente, on a montré au passage que le neutre de G était élément de H. Il est alors évidemment neutre pour la loi de composition restreinte à H. Enfin la propriété (iii) garantit l'existence d'un symétrique pour chaque élément de H. □

Voyons maintenant comment ce théorème permet de fabriquer plein de groupes nouveaux et intéressants.

Exemple 8. Soit G le groupe des bijections strictement croissantes de $\mathbb{R}$ vers $\mathbb{R}$, muni de la composition. Montrer que G est un groupe.

(On rappellera, au cas où ce serait nécessaire, qu'une application f est dite strictement croissante lorsque pour tous x et y, $x < y$ entraîne $f(x) < f(y)$).

La bonne idée est de montrer que G est un sous-groupe du groupe $\mathcal{S}(\mathbb{R})$. Lançons-nous.

La vérification de (i) est évidente : il est clair que l'application identique est une bijection strictement croissante de $\mathbb{R}$ sur $\mathbb{R}$.

Passons à (ii). Soit f et g deux bijections strictement croissantes de $\mathbb{R}$ sur $\mathbb{R}$. On sait déjà que $g \circ f$ est une bijection ; montrons qu'elle est strictement croissante. Soit x et y deux réels avec $x < y$; alors $f(x) < f(y)$ (croissance de f) puis $g(f(x)) < g(f(y))$ (croissance de g). Ceci montre bien que $g \circ f$ est strictement croissante.

Vérifions enfin (iii). Soit f une bijection strictement croissante de $\mathbb{R}$ vers $\mathbb{R}$. Il est bien clair que f^{-1} est bijective ; vérifions qu'elle est strictement croissante. Soit x et y deux réels avec $x < y$. On ne peut avoir $f^{-1}(x) = f^{-1}(y)$, car f^{-1} est injective ; on ne peut avoir $f^{-1}(y) < f^{-1}(x)$, car f étant strictement croissante on en déduirait l'inégalité $f(f^{-1}(y)) < f(f^{-1}(x))$, qui est fausse. Par élimination on a donc bien $f^{-1}(x) < f^{-1}(y)$.

Exemple 9. Soit A un sous-ensemble de $\mathbb{R}^2$ et G l'ensemble des isométries f de $\mathbb{R}^2$ sur $\mathbb{R}^2$ telles que $f(A) = A$. On montrerait par le même genre de méthode que G est un groupe parce que c'est un sous-groupe de $\mathcal{S}(\mathbb{R}^2)$. Dès que A sera un peu trop patatoïdal, G se réduira à $\{\mathrm{Id}_{\mathbb{R}^2}\}$ et sera donc peu intéressant, mais si A possède des symétries raisonnables, par exemple si A est un pentagone régulier, le groupe G méritera notre attention.

Le *théorème de Lagrange* est un résultat simple et élégant, proposé ici surtout pour le plaisir de faire une démonstration agréable.

Théorème 2 (de Lagrange)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors le nombre d'éléments de H divise le nombre d'éléments de G.*

Démonstration : Elle repose sur l'introduction de la relation $\sim$ définie pour tous éléments a, b de G par :

$$a \sim b \qquad \text{si et seulement si} \qquad ab^{-1} \in H.$$

Le plan de la preuve est le suivant :

1. On vérifie que $\sim$, comme son nom le laisse penser, est une relation d'équivalence.
2. On vérifie que toutes les classes d'équivalence pour la relation $\sim$ ont le même nombre d'éléments, à savoir le nombre d'éléments de H.
3. On conclut en quelques mots.

Exécution...

Étape 1. Vérifions successivement les trois propriétés requises des relations d'équivalence.

Soit a un élément de G. Comme $aa^{-1} = e \in H$, $a \sim a$. La relation $\sim$ est donc réflexive.

Soit a et b deux éléments de G, avec $a \sim b$, donc $ab^{-1} \in H$. En prenant l'inverse, $(ab^{-1})^{-1} \in H$, c'est-à-dire $ba^{-1} \in H$, soit $b \sim a$: la relation $\sim$ est donc symétrique.

Soit a, b et c trois éléments de G, avec $a \sim b$ et $b \sim c$. On a donc $ab^{-1} \in H$ et $bc^{-1} \in H$. En multipliant entre eux ces deux éléments de H, on obtient que $(ab^{-1})(bc^{-1})$ appartient à H, c'est-à-dire $ac^{-1} \in H$, soit $a \sim c$. La relation $\sim$ est donc transitive.

La relation $\sim$ est donc une relation d'équivalence.

Étape 2. Soit a un élément fixé de G. L'objectif est de montrer que sa classe d'équivalence $\mathfrak{cl}(a)$ possède le même nombre d'éléments que H. Pour ce faire, une bonne idée serait de montrer qu'il existe une bijection entre $\mathfrak{cl}(a)$ et H. Et pour montrer qu'une bijection existe, une bonne idée pourrait être d'en sortir une de sa manche (en mathématiques, on dit « exhiber »), et voir qu'elle convient !

Introduisons donc l'application $f : H \to \mathfrak{cl}(a)$ définie par : pour tout h de H,

$$f(h) = ha.$$

Vérifions tout d'abord que f est bien une application. La difficulté vient ici de ce que la formule ha possède certes un sens, mais qu'il faudrait savoir que ha appartient bien à $\mathfrak{cl}(a)$. Heureusement, la question est plus facile à résoudre qu'à poser ! C'est en effet une simple vérification : $a(ha)^{-1} = aa^{-1}h^{-1} = h^{-1} \in H$; donc $a \sim ha$; en d'autres termes ha appartient à $\mathfrak{cl}(a)$.

Vérifions que f est une bijection. Soit b un élément de G tel que $b \in \mathfrak{cl}(a)$. Cherchons les antécédents de b. Un élément h de H est antécédent de b par f si et seulement si $b = ah$, c'est-à-dire si et seulement si $h = ba^{-1}$. Il y a donc au plus un antécédent, à savoir ba^{-1}, et comme en outre $b \sim a$, l'élément ba^{-1} est dans H et il y a exactement un antécédent.

Ceci montre que f est une bijection, et $\mathfrak{cl}(a)$ compte donc exactement autant d'éléments que H.

Étape 3. Il ne reste plus qu'à conclure. On dispose d'une relation d'équivalence $\sim$, donc d'un ensemble-quotient $G/\sim$, qui constitue une partition de G. Chacune des parties de G figurant dans cette partition possède exactement $\mathrm{card}(H)$ éléments ; le nombre total d'éléments de G est donc égal au produit de $\mathrm{card}(H)$ par le nombre de parties de G figurant dans la partition $G/\sim$ et est en particulier un multiple de $\mathrm{card}(H)$. □

1.6 Noyaux

Une petite définition, à l'usage pratique pour prouver des injectivités. Pour le reste, une section courte sans guère de commentaires.

Définition 20. *Soit f un morphisme de groupes, allant d'un groupe G vers un groupe G', dont l'élément neutre est noté e'. Le* noyau *de f est par définition l'ensemble des éléments x de G tels que $f(x) = e'$.*

Notation 9. *Le noyau de f est noté* $\mathrm{Ker}(f)$ *(parce que* Ker *est l'abréviation de l'allemand « Kern »).*

Le fait suivant est presque évident, mais on ne peut s'interdire de le souligner.

Proposition 10. *Le noyau d'un morphisme est un sous-groupe du groupe de départ.*

Démonstration : Soit f un morphisme d'un groupe noté G de neutre noté e vers un groupe noté G' de neutre noté e'.

On sait que $f(e) = e'$ donc $e \in \mathrm{Ker}(f)$, qui n'est donc pas vide.

Soit a et b deux éléments de $\mathrm{Ker}(f)$. On a alors $f(ab^{-1}) = f(a)[f(b)]^{-1} = e'e' = e'$, donc ab^{-1} appartient à $\mathrm{Ker}(f)$. □

Proposition 11. *Soit f un morphisme de groupes, le neutre du groupe de départ étant noté e. L'application f est injective si et seulement si* $\mathrm{Ker}(f) = \{e\}$.

Démonstration : Sans surprise, vérifions successivement les deux implications. On notera e' le neutre du groupe d'arrivée.

Preuve de l'implication directe.

Supposons f injective. On sait déjà que $f(e) = e'$, et donc que $\{e\} \subset \mathrm{Ker}(f)$. Réciproquement, si $a \in \mathrm{Ker}(f)$, $f(a) = f(e) = e'$, et comme f est injective, $a = e$. D'où l'égalité $\{e\} = \mathrm{Ker}(f)$.

Preuve de l'implication réciproque.

Supposons que $\mathrm{Ker}(f) = \{e\}$. Soit a et b deux éléments du groupe de départ vérifiant $f(a) = f(b)$. Alors $f(ab^{-1}) = f(a)[f(b)]^{-1} = e'$, donc $ab^{-1} \in \mathrm{Ker}(f)$, donc $ab^{-1} = e$, donc $a = b$. Donc f est injective. □

1.7 Puissances et ordre d'un élément d'un groupe

Rappelons une définition déjà utilisée en partie.

Définition 21. *Soit a un élément d'un groupe et n un entier relatif. On appelle* puissance n-ième *de a l'élément a^n défini comme valant $\underbrace{aa\ldots a}_{n \text{ fois}}$ si $n \geqslant 1$, comme valant l'inverse de a^{-n} si $n \leqslant -1$ et comme valant l'élément neutre si $n = 0$.*

Définition équivalente (évitant l'emploi des trois petits points) *On définit par récurrence a^n pour tout entier n positif ou nul en posant $a^0 = e$ puis, pour tout $n \geqslant 0$, $a^{n+1} = a^n a$, puis on définit directement a^n pour tout entier n négatif en posant $a^n = (a^{-n})^{-1}$ (puisque a^{-n} est alors déjà défini).*

Notation 10. *L'ensemble des puissances de a est noté $\langle a \rangle$.*

Proposition 12. *Soit a un élément d'un groupe et n et m deux entiers ; alors $a^{m+n} = a^m a^n$ et $(a^m)^n = a^{mn}$.*

Démonstration : C'est très simple à voir avec des points de suspension, en n'oubliant pas de distinguer plein de cas selon les signes des divers entiers des formules, la définition dépendant de ce signe. Comme c'est à la fois très facile et très fastidieux, on va oublier discrètement de le faire. □

On en déduit aussitôt la très élémentaire

Proposition 13. *Soit G un groupe, et a un élément de G. L'ensemble $\langle a \rangle$ est un sous-groupe de G.*

Démonstration : L'ensemble $\langle a \rangle$ n'est pas vide, puisqu'il contient a. Si x et y sont deux éléments de $\langle a \rangle$, on peut trouver deux entiers (relatifs) m et n permettant d'écrire $x = a^m$ et $y = a^n$. Dès lors $xy^{-1} = a^{m-n}$ et donc xy^{-1} appartient à $\langle a \rangle$. □

Définition 22. *Soit a un élément d'un groupe, dont le neutre est noté e. Si pour tout $n \geqslant 1$, $a^n \neq e$ on dit que a est* d'ordre infini. *Sinon on appelle* ordre *de a le plus petit entier $n \geqslant 1$ tel que $a^n = e$.*

Afin de tenter de prévenir les confusions, introduisons un autre sens du mot « ordre », pas du tout synonyme du précédent et un peu superflu mais tellement passé dans les usages qu'on ne peut l'éviter.

Définition 23. *Soit G un groupe fini. L'*ordre *de G est son cardinal.*

Histoire d'appliquer rétroactivement la division euclidienne, qui sera correctement définie dans le chapitre sur l'arithmétique, démontrons le

Théorème 3. *Soit a un élément d'un groupe. L'ordre de a est égal au nombre d'éléments de $\langle a \rangle$.*

Démonstration : La preuve étant plus longue que la moyenne, essayons de dégager des étapes intermédiaires avec des énoncés précis, qui nous permettront de souffler quand ils seront atteints. On notera e l'élément neutre du groupe considéré.

Étape intermédiaire 1 : si l'ordre de a est fini, noté n,

$$\langle a \rangle = A, \text{ où on a posé } A = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Preuve de l'étape 1. Soit b un élément de $\langle a \rangle$, c'est-à-dire une puissance de a. On peut donc mettre b sous forme a^k pour un entier relatif k. Effectuons la division euclidienne de k par n, ainsi $k = nq + r$, avec $0 \leqslant r \leqslant n - 1$. On a alors

$$b = a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r,$$

donc b appartient à A, ce qui montre l'inclusion $\langle a \rangle \subset A$; l'autre inclusion étant évidente, l'étape 1 est prouvée.

Étape intermédiaire 2 : si l'ordre de a est fini, le théorème est vrai.

Preuve de l'étape 2. Notons n l'ordre de a. Il découle du résultat de l'étape 1 que dans cette hypothèse l'ensemble $\langle a\rangle$ possède *au plus* n éléments. L'étudiant distrait croira même qu'on a déjà prouvé qu'il en possède exactement n et qu'on a donc fini, mais son condisciple plus observateur remarquera que nous ne savons pas encore si dans l'énumération $e, a, a^2, \ldots, a^{n-1}$ figurent bien n éléments *distincts*.

Prouvons donc ce dernier fait ; supposons que dans cette énumération il y ait deux termes a^i et a^j qui représentent le même élément du groupe, avec pourtant $i < j$. On aurait alors $a^{j-i} = e$. Mais par ailleurs, comme $i < j$, on obtient $0 < j - i$ et donc $1 \leqslant i-j$, et comme $0 \leqslant i$ et $j < n$, on obtient $j-i < n$. Mais ceci contredit la définition de n comme le *plus petit* entier supérieur ou égal à 1 tel que $a^n = e$. L'hypothèse était donc absurde, et l'énumération décrivant $\langle a\rangle$ à l'étape 1 est une énumération sans répétition.

Le nombre d'éléments de $\langle a\rangle$ est donc bien égal à n, et l'étape 1 est prouvée.

Étape intermédiaire 3 : si l'ordre de a est infini, le théorème est vrai.

Preuve de l'étape 3. Dans ce cas, tout le travail consiste à prouver que $\langle a\rangle$ est un ensemble infini. La vérification est du même esprit qu'à l'étape 2, en plus simple : on va prouver que pour $i < j$, les éléments a^i et a^j de $\langle a\rangle$ sont distincts. Pour ce faire, supposons que deux d'entre eux soient égaux ; on aurait alors $a^{j-i} = e$, avec pourtant $1 \leqslant j - i$ et a ne serait pas d'ordre infini. Ainsi l'étape 3 est prouvée. □

Corollaire 1. *L'ordre d'un élément divise l'ordre du groupe.*

Démonstration : Laissée au lecteur, en lui rappelant l'existence dans ce cours d'un théorème dit « de Lagrange » et en lui conseillant tout de même de bien distinguer entre ordre (cardinal) et ordre (d'un élément), comme déjà mentionné. □

Histoire d'utiliser encore un peu la notion d'ordre, donnons un énoncé qui peut servir pour gagner du temps dans tel ou tel exercice très concret.

Proposition 14. *Soit G un groupe* fini *et H un sous-ensemble de G. Alors H est un sous-groupe de G si et seulement si :*

1. L'ensemble H n'est pas vide.

2. Pour tous a, b de H, le produit ab est aussi dans H.

En d'autres termes, dans le cas particulier d'un sous-ensemble d'un groupe *fini* (et seulement dans ce cas !) on peut faire des économies et éviter de travailler sur les ennuyeux symétriques pour examiner un potentiel sous-groupe.

Pour enfoncer le clou sur la nécessité de l'hypothèse selon laquelle G est fini, on pensera au cas $G = \mathbb{Z}$ et $H = \mathbb{N}$.

Démonstration : La seule difficulté est évidemment de vérifier la propriété (iii) de la définition des « sous-groupes ». Prenons donc un élément a de H. On commence par

traiter à part le cas stupide où $a = e$, et où il est clair qu'on a aussi $a^{-1} = e \in H$. Pour le cas sérieux où $a \neq e$, considérons le sous-groupe $\langle a \rangle$ de G. Ce sous-groupe est fini, puisqu'inclus dans G. On déduit donc du théorème précédent (en fait de sa partie la plus facile, l'étape 3 de sa preuve) que a est d'ordre fini. Notons n l'ordre de a ; comme $a \neq e$, on a l'inégalité $n \geqslant 2$ et donc $n-1 \geqslant 1$; écrivons l'identité $a^{n-1} = a^n a^{-1} = a^{-1}$, et revenons dans cette formule à la définition de a^{n-1} : on obtient $a^{-1} = \underbrace{aa\dots aa}_{n-1 \text{ fois}}$ comme produit d'un nombre positif d'exemplaires de a ; par la propriété 2 de l'énoncé de la proposition, on en déduit que $a^{-1} \in H$. □

1.8 Anneaux et corps

Il s'agit ici simplement de rajouter un peu de vocabulaire pour pouvoir décrire les propriétés que possèdent les ensembles de nombres usuels. Le chapitre se limitera donc à quelques définitions.

Définition 24. *Soit A un ensemble muni de deux opérations, notées $+$ et $\times$. On dit que A est un* anneau *lorsque les assertions (i) à (iv) sont vraies.*

(i) Pour l'addition, A est un groupe commutatif.

(ii) La multiplication est associative.

(iii) La multiplication possède un élément neutre.

(iv) La multiplication est distributive par rapport à l'addition ; en d'autres termes, pour tous a, b et c éléments de A,

$$(a+b)c = ac + bc, \qquad c(a+b) = ca + cb.$$

L'archétype de l'anneau est l'ensemble $\mathbb{Z}$ des entiers relatifs ; dans un anneau quelconque on peut calculer « comme » dans $\mathbb{Z}$. Méfiance sur un seul point toutefois : la définition n'exigeant pas que la multiplication soit commutative, certaines formules peuvent être un peu plus perverses ; par exemple $(a+b)^2$ se développe en $a^2+ba+ab+b^2$, mais ne peut pas dans un anneau trop général être regroupé en $a^2 + 2ab + b^2$ puisque ab n'a aucune raison d'être égal à ba.

Voici un autre exemple.

Proposition 15. *Soit E un espace vectoriel. L'ensemble des applications linéaires de E vers E, noté $\mathcal{L}(E)$, est un anneau pour l'addition et la composition.*

Démonstration : Les propriétés d'« anneau » sont généralement évidentes à vérifier ; la plus intéressante est la distributivité, qui est liée à la linéarité, et que nous laissons gentiment au lecteur. Le neutre pour la composition est sans surprise l'application identique. □

Si on choisit pour espace vectoriel $E = \mathbb{R}^n$ et que l'on représente les éléments de $\mathcal{L}(E)$ par des matrices carrées, on obtient l'anneau $\mathcal{M}_n(\mathbb{R})$ des matrices carrées de taille $n \times n$ à coefficients réels.

Définition 25. *Soit A un anneau et $n \geqslant 1$ un entier. L'anneau des matrices carrées de taille n à coefficients dans A, noté $\mathcal{M}_n(A)$, est défini par les lois de composition suivantes. Si $M = (a_{i,j})_{1\leqslant i,j\leqslant n}$ et $N = (b_{i,j})_{1\leqslant i,j\leqslant n}$ sont deux éléments de $\mathcal{M}_n(A)$,*

$$M + N = (a_{i,j} + b_{i,j})_{1\leqslant i,j\leqslant n}, \quad M \times N = (c_{i,j})_{1\leqslant i,j\leqslant n} \text{ avec } c_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j}.$$

Le neutre de $\mathcal{M}_n(A)$ pour l'addition est la matrice nulle, dont tous les coefficients valent le neutre de l'addition de A. Le neutre de $\mathcal{M}_n(A)$ pour la multiplication est la matrice identité, dont tous les coefficients valent le neutre de l'addition de A sauf ceux de la diagonale qui valent le neutre de la multiplication de A.

Définition 26. *Un anneau est dit* commutatif *quand sa multiplication est commutative.*

Définition 27. *Un anneau A est dit* intègre *lorsque :*
(i) L'anneau A possède au moins deux éléments.
(ii) Pour tous a et b éléments non nuls de A, $ab \neq 0$.

Une classe particulière d'anneaux est celle des anneaux tels que la deuxième loi (la multiplication) fournit aussi une structure de groupe (sur l'anneau privé de son zéro).

Définition 28. *On dit qu'un anneau K est un* corps commutatif *lorsque :*
(i) La multiplication est commutative.
(ii) L'anneau K possède au moins deux éléments.
(iii) Tout élément non nul de K possède un inverse pour la multiplication.

Les archétypes de corps commutatifs sont naturellement $\mathbb{Q}$, ensemble des fractions, et, encore mieux connus des étudiants, $\mathbb{R}$ et $\mathbb{C}$. Un autre archétype, au moins aussi important malgré sa simplicité, est Z_p pour p premier. Nous avons déjà défini l'addition sur Z_p. On définit une multiplication $\otimes$, en convenant que $i \otimes j$ est l'unique entier $0 \leqslant k \leqslant n-1$ tel que $ij - k$ est divisible par p. On démontre facilement que $(Z_p, \oplus, \otimes)$ est un anneau pour tout entier p, et que c'est un corps, si et seulement si p est premier. Ces corps servent entre autres en cryptographie. Le plus petit d'entre eux, Z_2, peut être considéré comme la base de toute l'informatique : excusez du peu !

2 Entraînement

2.1 Vrai ou faux

Vrai-Faux 1. Soit $E = \{0, 1, 2\}$. Les graphes suivants définissent-ils une relation d'équivalence sur E (oui ou non et pourquoi) ?

1. $\square$ $\Gamma = \{ (0,0), (0,1), (1,0), (1,1) \}$
2. $\boxtimes$ $\Gamma = \{ (0,0), (0,1), (1,0), (1,1), (2,2) \}$
3. $\square$ $\Gamma = \{ (0,0), (0,1), (1,0), (1,1), (1,2), (2,2) \}$
4. $\square$ $\Gamma = \{ (0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2) \}$
5. $\boxtimes$ $\Gamma = \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2) \}$

Vrai-Faux 2. Soit $E = \{0, 1, 2\}$. Les graphes suivants définissent-ils une relation d'ordre sur E (oui ou non et pourquoi) ?

1. $\boxtimes$ $\Gamma = \{ (0,0), (0,1), (1,1), (2,2) \}$
2. $\square$ $\Gamma = \{ (0,0), (0,1), (1,0), (1,1), (2,2) \}$
3. $\boxtimes$ $\Gamma = \{ (0,0), (0,1), (0,2), (1,1), (2,2) \}$
4. $\square$ $\Gamma = \{ (0,0), (0,1), (1,1), (1,2), (2,2) \}$
5. $\boxtimes$ $\Gamma = \{ (0,0), (0,1), (0,2), (1,1), (1,2), (2,2) \}$

Vrai-Faux 3. Soient E un ensemble fini non vide et x un élément fixé de E. Les relations $\sim$ définies ci-dessous sont-elles des relations d'équivalence sur $\mathcal{P}(E)$ (oui ou non et pourquoi) ?

1. $\boxtimes$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \sim B \iff A = B$
2. $\square$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \sim B \iff A \subset B$
3. $\square$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \sim B \iff (A \cap B = \emptyset)$
4. $\boxtimes$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \sim B \iff \Big((A \cap B = \emptyset) \vee (A \cup B \neq \emptyset) \Big)$
5. $\square$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \sim B \iff (x \in A \cup B)$
6. $\boxtimes$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \sim B \iff \Big((x \in A \cap B) \vee (x \in {}^{c}A \cap {}^{c}B) \Big)$

Vrai-Faux 4. Soient E un ensemble fini non vide et x un élément fixé de E. Les relations $\mathcal{R}$ définies ci-dessous sont-elles des relations d'ordre sur $\mathcal{P}(E)$ (oui ou non et pourquoi) ?

1. $\boxtimes$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \mathcal{R} B \iff A = B$
2. $\boxtimes$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \mathcal{R} B \iff A \subset B$
3. $\square$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \mathcal{R} B \iff (x \in (A \cap {}^{c}B))$
4. $\square$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \mathcal{R} B \iff (x \in (A \cup {}^{c}B))$
5. $\boxtimes$ $\forall A, B \in \mathcal{P}(E)$, $\quad A \mathcal{R} B \iff \Big((A = B) \vee (x \in A \cap {}^{c}B) \Big)$

Vrai-Faux 5. Les relations $\mathcal{R}$ définies ci-dessous sont-elles des relations d'ordre sur $\mathbb{R}$ (oui ou non, et pourquoi) ?

1. $\square$ $\forall x, y \in \mathbb{R}\,, \quad x\mathcal{R}y \iff x < y$
2. $\boxtimes$ $\forall x, y \in \mathbb{R}\,, \quad x\mathcal{R}y \iff \mathrm{e}^x \leqslant \mathrm{e}^y$
3. $\square$ $\forall x, y \in \mathbb{R}\,, \quad x\mathcal{R}y \iff |x| \leqslant |y|$
4. $\boxtimes$ $\forall x, y \in \mathbb{R}\,, \quad x\mathcal{R}y \iff (x-y) \in \mathbb{N}$
5. $\square$ $\forall x, y \in \mathbb{R}\,, \quad x\mathcal{R}y \iff (x-y) \in \mathbb{Z}$

Vrai-Faux 6. Les relations $\mathcal{R}$ définies ci-dessous sont-elles des relations d'équivalence sur $\mathbb{C}$ (oui ou non, et pourquoi) ?

1. $\boxtimes$ $z\mathcal{R}z' \iff |z| = |z'|$
2. $\square$ $z\mathcal{R}z' \iff |z/z'| = 1$
3. $\boxtimes$ $z\mathcal{R}z' \iff \mathrm{e}^z = \mathrm{e}^{z'}$
4. $\square$ $z\mathcal{R}z' \iff |z - z'| = 1$
5. $\boxtimes$ $z\mathcal{R}z' \iff |\mathrm{e}^{z-z'}| = 1$

Vrai-Faux 7. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. $\boxtimes$ La soustraction est une loi de composition interne dans $\mathbb{Z}$.
2. $\square$ 0 est élément neutre de la soustration dans $\mathbb{Z}$.
3. $\square$ La soustraction dans $\mathbb{Z}$ est associative.
4. $\boxtimes$ 0 est élément neutre pour l'addition dans $\mathbb{N}$.
5. $\boxtimes$ L'addition est associative dans $\mathbb{N}$.

Vrai-Faux 8. Les ensembles suivants, munis de l'addition des réels sont-ils des groupes (oui ou non et pourquoi) ?

1. $\boxtimes$ $\Big\{\, a/10^n\,,\ a \in \mathbb{Z}\,,\ n \in \mathbb{N} \,\Big\}$
2. $\boxtimes$ $\Big\{\, a/2^n\,,\ a \in \mathbb{Z}\,,\ n \in \mathbb{Z} \,\Big\}$
3. $\boxtimes$ $\Big\{\, a\sqrt{2}\,,\ a \in \mathbb{Z} \,\Big\}$
4. $\square$ $\Big\{\, a\sqrt{2}\,,\ a \in \mathbb{N} \,\Big\}$
5. $\boxtimes$ $\Big\{\, a\sqrt{2} + b\sqrt{3}\,,\ a, b \in \mathbb{Z} \,\Big\}$
6. $\square$ $\Big\{\, a\sqrt{2} + b\sqrt{3}\,,\ a \in \mathbb{Z}\,,\ b \in \mathbb{N} \,\Big\}$

Vrai-Faux 9. Les ensembles suivants, munis de la multiplication des réels sont-ils des groupes (oui ou non et pourquoi) ?

1. $\boxtimes$ $\Big\{\, 1, -1 \,\Big\}$

2. ☐ $\left\{ 1, -1, 1/2, 2 \right\}$
3. ☒ $\left\{ 2^n\,,\ n \in \mathbb{Z} \right\}$
4. ☒ $\left\{ a2^n\,,\ a = \pm 1\,,\ n \in \mathbb{Z} \right\}$
5. ☐ $\left\{ a + b\sqrt{2}\,,\ a, b \in \mathbb{Q}^* \right\}$
6. ☒ $\left\{ a + b\sqrt{2}\,,\ a, b \in \mathbb{Q} \right\} \setminus \{0\}$

Vrai-Faux 10. Les ensembles suivants, munis de l'addition et de la multiplication des réels sont-ils des anneaux (oui ou non et pourquoi) ?

1. ☐ $\left\{ b\sqrt{2}\,,\ b \in \mathbb{Q} \right\}$
2. ☒ $\left\{ a + b\sqrt{2}\,,\ a, b \in \mathbb{Q} \right\}$
3. ☐ $\left\{ a + b\pi\,,\ a, b \in \mathbb{Q} \right\}$
4. ☒ $\left\{ a + b\sqrt{4}\,,\ a, b \in \mathbb{Q} \right\}$
5. ☐ $\left\{ a + b\sqrt[3]{2}\,,\ a, b \in \mathbb{Q} \right\}$
6. ☐ $\left\{ a + b\sqrt{2} + c\sqrt{3}\,,\ a, b, c \in \mathbb{Q} \right\}$

Vrai-Faux 11. Les ensembles suivants, munis de l'addition et de la multiplication des réels sont-ils des corps (oui ou non et pourquoi) ?

1. ☐ $\left\{ b\sqrt{2}\,,\ b \in \mathbb{Q} \right\}$
2. ☒ $\left\{ a + b\sqrt{2}\,,\ a, b \in \mathbb{Q} \right\}$
3. ☐ $\left\{ a + b\pi\,,\ a, b \in \mathbb{Q} \right\}$
4. ☒ $\left\{ a + b\sqrt{4}\,,\ a, b \in \mathbb{Q} \right\}$
5. ☐ $\left\{ a + b\sqrt[3]{2}\,,\ a, b \in \mathbb{Q} \right\}$
6. ☐ $\left\{ a + b\sqrt{2} + c\sqrt{3}\,,\ a, b, c \in \mathbb{Q} \right\}$

2.2 Exercices

Exercice 1. On considère les relations suivantes sur $\mathbb{R}$.

- $\forall x, y\,, \quad x \mathcal{R} y \iff x \leqslant y$
- $\forall x, y\,, \quad x \mathcal{R} y \iff x^2 \leqslant y^2$
- $\forall x, y\,, \quad x \mathcal{R} y \iff \lfloor x \rfloor \leqslant \lfloor y \rfloor$
- $\forall x, y\,, \quad x \mathcal{R} y \iff \lfloor x \rfloor = \lfloor y \rfloor$
- $\forall x, y\,, \quad x \mathcal{R} y \iff \sin(x) = \sin(y)$
- $\forall x, y\,, \quad x \mathcal{R} y \iff y - x \in \mathbb{N}$

Pour chacune de ces relations $\mathcal{R}$:

1. Représenter graphiquement dans $\mathbb{R}^2$ le graphe de la relation $\mathcal{R}$.
2. Est-ce une relation d'ordre ? une relation d'équivalence ?

Exercice 2. On définit la relation $\mathcal{R}$ sur $\mathbb{N}$ par :

$$\forall m, n \in \mathbb{N}^*\,, \quad m\mathcal{R}n \iff \Big(\exists k \in \mathbb{N}^*\,,\ m^k = n\Big)$$

Démontrer que $\mathcal{R}$ est une relation d'ordre.

Exercice 3. Une relation binaire $\mathcal{R}$ dans un ensemble E est dite circulaire si pour tout $(a, b, c) \in E$,

$$\Big(a\mathcal{R}b \text{ et } b\mathcal{R}c\Big) \implies c\mathcal{R}a$$

Montrer qu'une relation circulaire et réflexive est une relation d'équivalence.

Exercice 4. Soit E et F deux ensembles et f une application de E dans F. On définit la relation $\sim$ sur E par :

$$\forall x, y \in E\,, \quad x \sim y \iff f(x) = f(y)$$

1. Montrer que $\sim$ est une relation d'équivalence.
2. Soit Γ l'ensemble des couples $(\mathfrak{cl}(x), f(x))$, où x parcourt l'ensemble E. Montrer que Γ est le graphe d'une application de l'ensemble-quotient $E/\sim$ dans F. On note g cette application.
3. Montrer que g est une application injective.
4. Soit f l'application de $\mathbb{Z}$ dans $\mathbb{N}$ qui à $n \in \mathbb{Z}$ associe n^2. Décrire $\mathfrak{cl}(0)$ et $\mathfrak{cl}(1)$.
5. Soit f l'application de $\mathbb{C}$ dans $\mathbb{C}$ qui à z associe $f(z) = z^4$. Décrire $\mathfrak{cl}(0)$ et $\mathfrak{cl}(1)$.
6. Soit f l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à un réel x associe sa partie entière. Décrire $\mathfrak{cl}(0)$ et $\mathfrak{cl}(1)$.
7. Soit f l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à un réel x associe sa partie décimale. Décrire $\mathfrak{cl}(0)$ et $\mathfrak{cl}(\frac{1}{2})$.

Exercice 5.

1. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :

   $$\forall x, y \in \mathbb{R}\,, \quad x * y = xy + (x^2 - 1)(y^2 - 1)$$

   Montrer que $*$ est commutative, non associative, et que 1 est élément neutre,
2. On munit $\mathbb{R}^{+*}$ de la loi de composition interne $*$ définie par :

   $$\forall x, y \in \mathbb{R}^{+*}\,, \quad x * y = \sqrt{x^2 + y^2}$$

   Montrer que $*$ est commutative, associative, et que 0 est élément neutre. Montrer que aucun élément de $\mathbb{R}^{+*}$ n'a de symétrique pour $*$.

3. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :

$$\forall x, y \in \mathbb{R}\,, \quad x * y = \sqrt[3]{x^3 + y^3}$$

Montrer que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R}, *)$ vers $(\mathbb{R}, +)$. En déduire que $(\mathbb{R}, *)$ est un groupe commutatif.

Exercice 6. Soit E l'ensemble des parties d'un ensemble à deux éléments, par exemple $E = \mathcal{P}(\{0,1\})$ donc

$$E = \Big\{ \emptyset\,,\, \{0\}\,,\, \{1\}\,,\, \{0,1\} \Big\}$$

On considère les lois de composition $*$ suivantes sur l'ensemble E.

- Réunion : $A * B = A \cup B$
- Intersection : $A * B = A \cap B$
- Différence symétrique : $A * B = A \triangle B = (A \setminus B) \cup (B \setminus A)$
- Réunion des complémentaires : $A * B = {}^cA \cup {}^cB$
- Intersection des complémentaires : $A * B = {}^cA \cap {}^cB$

Pour chacune d'entre elles :

1. Écrire la table de composition de la loi $*$.
2. L'ensemble E possède-t-il un élément neutre pour la loi $*$?
3. La loi $*$ est-elle associative ?
4. La loi $*$ est-elle commutative ?
5. L'ensemble E muni de la loi $*$ est-il un groupe ?
6. Répondre aux questions 2 à 5 en remplaçant E par l'ensemble des parties d'un ensemble quelconque.

Exercice 7. Le but de l'exercice est d'étudier les groupes à $1, 2, 3$ ou 4 éléments.

1. Ecrire la table de composition d'un groupe à 1 élément.
2. Ecrire la table de composition d'un groupe à 2 éléments. Vérifier qu'il est isomorphe aux groupes suivants.

$$Z_2 \quad ; \quad \mathcal{S}_2 \quad ; \quad \Big(\{1, -1\}\,, \times \Big) \quad ; \quad \Big(\big\{ x \mapsto x\,,\, x \mapsto 1/x \big\}\,, \circ \Big)$$

$$\left(\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \times \right)$$

3. Ecrire la table de composition d'un groupe à 3 éléments. Vérifier qu'il est isomorphe aux groupes suivants.

$$Z_3 \quad ; \quad \Big(\{1, \mathrm{e}^{2\mathrm{i}\pi/3}, \mathrm{e}^{4\mathrm{i}\pi/3}\}\,, \times \Big) \quad ; \quad \Big(\big\{ (1,2,3), (2,3,1), (3,1,2) \big\}\,, \circ \Big)$$

$$\left(\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}, \times \right)$$

4. Soit $\Big(\{e,a,b,c\}\,,\,*\Big)$ un groupe à 4 éléments, d'élément neutre e.
   (a) Montrer qu'il existe au moins un élément, autre que l'élément neutre, qui est son propre symétrique. On suppose désormais que b est son propre symétrique.
   (b) On suppose $a*c=c*a=e$. Remplir la table de composition du groupe. Montrer qu'il est isomorphe aux groupes suivants.

$$Z_4 \quad ; \quad \Big(\{1,\mathrm{i},-1,-\mathrm{i}\}\,,\times\Big)$$

$$\Big(\Big\{(1,2,3,4),(2,3,4,1),(3,4,1,2),(4,1,2,3)\Big\}\,,\circ\Big)$$

$$\left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&-1\\1&0\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\},\times\right)$$

   (c) On suppose $a*a=c*c=e$. Remplir la table de composition du groupe. Montrer qu'il est isomorphe aux groupes suivants.

$$Z_2\times Z_2 \quad ; \quad \Big(\mathcal{P}(\{x,y\})\,,\triangle\Big)$$

$$\left(\left\{\begin{pmatrix}1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&4&3\end{pmatrix},\begin{pmatrix}2&1&3&4\end{pmatrix},\begin{pmatrix}2&1&4&3\end{pmatrix}\right\},\circ\right)$$

$$\left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}0&-1\\-1&0\end{pmatrix}\right\},\times\right)$$

   (d) Vérifier que l'on est toujours dans le cas de la question (4b) ou dans le cas de la question (4c).
5. Vérifier que tous les groupes de cet exercice sont abéliens.

Exercice 8. On considère les éléments suivants de $\mathcal{S}_5$.

$$\sigma=\begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} \quad \text{et} \quad \varrho=\begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix}$$

Calculer les puissances successives et déterminer l'ordre de σ et ϱ, ainsi que de $\sigma\varrho$, $\varrho\sigma$, $\sigma\varrho^{-1}$ et $\varrho^{-1}\sigma$.

Exercice 9. On considère un pentagone régulier : pour fixer les idées, l'ensemble des points du plan complexe dont des sommets ont pour affixes les racines cinquièmes de l'unité, soit

$$P=\Big\{\,\mathrm{e}^{2\mathrm{i}k\pi/5}\,,\ k=0,1,2,3,4\,\Big\}.$$

Le but de l'exercice est d'étudier le groupe (pour la composition des applications) des isométries du plan complexe qui laissent invariant ce pentagone. On notera ϱ la rotation de centre l'origine et d'angle $2\pi/5$, et σ la symétrie qui à un nombre complexe associe son conjugué.

$$\varrho\ : z\longmapsto z\mathrm{e}^{2\mathrm{i}\pi/5} \quad ; \quad \sigma\ : z\longmapsto \overline{z}$$

1. Vérifier que ϱ et σ laissent invariant l'ensemble P.
2. Vérifier que les puissances successives de ϱ sont des rotations dont on donnera l'angle, et déterminer l'ordre de ϱ.
3. Pour $n = 0, \ldots, 4$, montrer que $\sigma\varrho^n$ et $\varrho^n\sigma$ sont des symétries par rapport à un axe passant par l'origine, dont on donnera l'angle par rapport à l'axe réel.
4. Quel est l'ordre d'une symétrie ?
5. Montrer que le produit de deux des symétries de la question 3 est une puissance de ϱ.
6. Montrer que le plus petit groupe contenant ϱ et σ possède 10 éléments.

Exercice 10. On rappelle que Z_n est le groupe des entiers de 0 à $n-1$, muni de l'addition modulo n.

1. Montrer que l'ordre de 1 dans Z_n vaut n.
2. Montrer que l'ordre de k dans Z_n vaut n si et seulement si k est premier avec n.
3. Si k est un diviseur de n, montrer que l'ordre de k est le quotient de n par k.
4. Soit $(G, *)$ un groupe quelconque. On suppose que G contient un élément a d'ordre n. On note f l'application de $\{0, \ldots, n-1\}$ dans G qui à 0 associe l'élément neutre de G et à $k \geqslant 1$ associe la puissance k-ième de a dans G. Montrer que f est un isomorphisme de groupes entre Z_n et $\langle a \rangle$.

Exercice 11.

1. Soit S un ensemble quelconque et $E = \{0,1\}^S$ l'ensemble des applications de S dans $\{0,1\}$. On munit E de l'addition modulo 2 des images : pour tout $f, g \in E$, $f \oplus g$ est l'application de S dans $\{0,1\}$ définie par :

$$f \oplus g(x) = \begin{cases} 1 & \text{si } f(x) \neq g(x) \\ 0 & \text{si } f(x) = g(x) \end{cases}$$

   Montrer que $(E, \oplus)$ est un groupe abélien, dans lequel chaque élément est son propre symétrique.

2. Soit $F = \mathcal{P}(S)$ l'ensemble des parties de S. On munit F de la différence symétrique ensembliste. On considère l'application ϕ, de F dans E qui à une partie de S associe sa fonction indicatrice :

$$\phi \ : A \in \mathcal{P}(S) \longmapsto \mathbb{I}_A \ ,$$

   où pour tout $x \in S$, $\mathbb{I}_A(x) = 1$ si $x \in A$ et $\mathbb{I}_A(x) = 0$ sinon.

   Montrer que ϕ est un isomorphisme de E vers F, pour les lois $\oplus$ et $\triangle$. En déduire que $(F, \triangle)$ est un groupe abélien, dans lequel chaque élément est son propre symétrique.

   Dans toute la suite, G désigne un groupe dans lequel chaque élément est son propre symétrique.

3. Montrer que G est abélien.
4. Soit a un élément quelconque de G, différent de l'élément neutre. On définit la relation $\sim$ sur G par :

$$\forall x, y \in G\ , \quad x \sim y \iff \Big(x = y \text{ ou } x = ay \Big)$$

Montrer que $\sim$ est une relation d'équivalence sur G. Montrer que chaque classe d'équivalence a deux éléments.

5. On définit la loi $*$ sur l'ensemble-quotient $G/\sim$ par :

$$\forall x, y \in G\ , \quad \mathfrak{cl}(x) * \mathfrak{cl}(y) = \mathfrak{cl}(xy).$$

Montrer que $*$ est une loi de composition interne sur $G/\sim$, et que $G/\sim$ muni de $*$ est un groupe abélien, dans lequel chaque élément est son propre symétrique.

6. On suppose que G est *fini*. Déduire des questions précédentes que le cardinal de G est une puissance de 2.

Exercice 12. On considère les applications suivantes, de $\mathbb{R} \setminus \{0, 1\}$ dans lui-même.

$$f_1 : x \mapsto x \quad ; \quad f_2 : x \mapsto 1 - x \quad ; \quad f_3 : x \mapsto \frac{1}{1-x}$$

$$f_4 : x \mapsto \frac{1}{x} \quad ; \quad f_5 : x \mapsto \frac{x}{x-1} \quad ; \quad f_6 : x \mapsto \frac{x-1}{x}$$

On munit l'ensemble $E = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ de la composition des applications.

1. Écrire la table de composition de $(E, \circ)$.
2. Montrer que $G = (E, \circ)$ est un groupe.
3. Est-ce un groupe abélien ?
4. Déterminer tous les sous-groupes de G.
5. Déterminer l'ordre de chacun des éléments de G.
6. Quels sont les éléments de $\langle f_2 \rangle$?
7. Quels sont les éléments de $\langle f_3 \rangle$?

Exercice 13. Soient $(E, *)$ et $(F, \cdot)$ deux groupes. On munit l'ensemble produit $E \times F$ de la loi de composition $\odot$ definie par :

$$\forall (x, y), (x'y') \in E \times F\ , \quad (x, y) \odot (x', y') = (x * x', y \cdot y')$$

1. Montrer que $(E \times F, \odot)$ est un groupe.
2. Soit E' un sous-groupe de E, F' un sous-groupe de F. Montrer que $E' \times F'$ est un sous-groupe de $E \times F$, muni de la loi $\odot$.

Exercice 14. Montrer que les ensembles suivants d'applications de $\mathbb{C}$ dans $\mathbb{C}$, munis de la loi de composition des applications, sont des groupes.

1. $\left\{ z \mapsto z+t\,,\ t \in \mathbb{Z} \right\}$
2. $\left\{ z \mapsto z+t\,,\ t \in \mathbb{C} \right\}$
3. $\left\{ z \mapsto \mathrm{e}^{\mathrm{i}\theta} z\,,\ \theta \in \mathbb{R} \right\}$
4. $\left\{ z \mapsto sz+t\,,\ s \in \mathbb{C}^*\,,\ t \in \mathbb{C} \right\}$
5. $\left\{ z \mapsto \dfrac{az+b}{cz+d}\,,\ (a,b,c,d) \in \mathbb{C}^4\,, ad-bc \neq 0 \right\}$

Exercice 15. Soit G un sous-groupe additif de $(\mathbb{R},+)$. On suppose que $G \neq \{0\}$.

1. Montrer que $G \cap \mathbb{R}^{+*}$ possède une borne inférieure, que l'on notera b.
2. Montrer que $b \in G$.
3. On suppose $b > 0$. Montrer que $G = b\mathbb{Z}$.
4. On suppose $b = 0$. Montrer que si x et y sont deux réels tels que $x < y$, l'intervalle $]x, y[$ contient au moins un élément de G (on dit que G est dense dans $\mathbb{R}$).
5. Montrer que l'ensemble $\{\, m+n\sqrt{2}\,,\ (n,m) \in \mathbb{Z}^2 \,\}$ muni de l'addition est un sous-groupe de $(\mathbb{R},+)$, et qu'il est dense dans $\mathbb{R}$ (on rappelle que $\sqrt{2}$ est irrationnel).

Exercice 16. Soit $n \geqslant 1$ un entier. On définit une multiplication $\otimes$ sur Z_n en convenant que $i \otimes j$ est l'unique entier $0 \leqslant k \leqslant n-1$ tel que $ij - k$ est divisible par n.

1. Montrer que $(Z_n, \oplus, \otimes)$ est un anneau.
2. Montrer que $(Z_n, \oplus, \otimes)$ est un corps si et seulement si $n \geqslant 2$ et n est premier.

Exercice 17. Montrer que l'application de $\mathbb{C}$ dans $\mathbb{C}$ qui à un nombre complexe associe son conjugué est un isomorphisme de corps : c'est une bijection, et un morphisme à la fois pour l'addition et la multiplication.

Exercice 18. On note $\mathbb{Z}[\sqrt{2}]$ l'ensemble de réels suivant :

$$\mathbb{Z}[\sqrt{2}] = \left\{ m+n\sqrt{2}\,,\ m,n \in \mathbb{Z} \right\}.$$

1. Montrer que $\mathbb{Z}[\sqrt{2}]$, muni de l'addition et de la multiplication des réels, est un sous-anneau de $\mathbb{R}$.
2. On considère l'application ϕ, de $\mathbb{Z}[\sqrt{2}]$ dans lui-même, qui à $m+n\sqrt{2}$ associe

   $$\phi(m+n\sqrt{2}) = m - n\sqrt{2}.$$

   Montrer que ϕ est un automorphisme de l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$ (c'est une bijection, et un morphisme pour chacune des deux lois).

3. Pour tout $x \in \mathbb{Z}[\sqrt{2}]$, on pose $N(x) = x\phi(x)$. Montrer que N est une application de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.
4. Démontrer que x est un élément inversible de $\mathbb{Z}[\sqrt{2}]$ si et seulement si $N(x) = \pm 1$.
5. Vérifier que $3 + 2\sqrt{2}$ et $-3 + 2\sqrt{2}$ sont inversibles dans $\mathbb{Z}[\sqrt{2}]$.

Exercice 19. On considère les deux matrices suivantes.

$$U = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

1. Calculer les produits UV et VU.
2. En déduire que $\mathcal{M}_2(\mathbb{R})$ est un anneau non commutatif et non intègre.
3. Étendre ce résultat à l'anneau $\mathcal{M}_n(A)$ des matrices de taille $n \geqslant 2$ sur un anneau A quelconque.

Exercice 20.

1. Soit S un ensemble de cardinal au moins 2 et $E = \{0,1\}^S$ l'ensemble des applications de S dans $\{0,1\}$. On munit E de l'addition modulo 2 des images et de leur multiplication : pour tout $f, g \in E$, $f \oplus g$ et $f \otimes g$ sont les applications de S dans $\{0,1\}$ définies par :

$$f \oplus g(x) = \begin{cases} 1 & \text{si } f(x) \neq g(x), \\ 0 & \text{si } f(x) = g(x), \end{cases} \quad \text{et} \quad f \otimes g(x) = \begin{cases} 1 & \text{si } f(x) = g(x) = 1, \\ 0 & \text{sinon.} \end{cases}$$

   Montrer que $(E, \oplus, \otimes)$ est un anneau commutatif.
2. Soit $\mathbb{I}$ l'application constante égale à 1. Soit f une application non constante de S dans $\{0,1\}$. Calculer $f \otimes (\mathbb{I} \oplus f)$. En déduire que $(E, \oplus, \otimes)$ n'est pas un anneau intègre.
3. Soit $F = \mathcal{P}(S)$ l'ensemble des parties de S. On munit F de la différence symétrique et de l'intersection ensemblistes. On considère l'application ϕ de F dans E qui à une partie de S associe sa fonction indicatrice :

$$\phi \ : A \in \mathcal{P}(S) \longmapsto \mathbb{I}_A,$$

   où, pour tout $x \in S$, $\mathbb{I}_A(x) = 1$ si $x \in A$ et $\mathbb{I}_A(x) = 0$ sinon. Montrer que ϕ est un isomorphisme de $(E, \oplus)$ vers $(F, \triangle)$, et également un isomorphisme de $(E, \otimes)$ vers $(F, \cap)$. En déduire que $(F, \triangle, \cap)$ est un anneau commutatif non intègre.

2.3 QCM

Donnez-vous une heure pour répondre à ce questionnaire. Les 10 questions sont indépendantes. Pour chaque question 5 affirmations sont proposées, parmi lesquelles 2 sont vraies et 3 sont fausses. Pour chaque question, cochez les 2 affirmations que vous pensez vraies. Chaque question pour laquelle les 2 affirmations vraies sont cochées rapporte 2 points.

Question 1. La relation $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{N}$.

A $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n|m.$

B $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n^2 = m^2.$

C $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n^2 + m^2 = 2nm + 2n.$

D $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n^2 - m^2 = 2nm + 2n.$

E $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n^2 + m^2 = 2nm.$

Question 2. La relation $\mathcal{R}$ est une relation d'ordre sur $\mathbb{N}$.

A $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n - m \geqslant 1.$

B $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff n - m \leqslant 1.$

C $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff \exists k \in \mathbb{N}\,,\ m^2 = k - n^2.$

D $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff \exists k \in \mathbb{N}\,,\ m^2 = k + n^2.$

E $\forall n, m \in \mathbb{N}\,, \quad n\mathcal{R}m \iff \exists k \in \mathbb{N}\,,\ m = kn.$

Question 3.

A La division est une loi de composition interne dans $\mathbb{R}^*$.

B La division ne possède pas d'élément neutre dans $\mathbb{R}^*$.

C La division est associative dans $\mathbb{R}^*$

D La division est commutative dans $\mathbb{R}^*$

E Tout élément de $\mathbb{R}^*$ est son propre inverse pour la division.

Question 4. On note $\oplus$ l'addition des entiers modulo 6.

A $(\{2, 4\}, \oplus)$ est un groupe.

B $(\{0, 1, 2\}, \oplus)$ est un groupe.

C $(\{0, 2, 4\}, \oplus)$ est un groupe.

D $(\{0, 3\}, \oplus)$ est un groupe.

E $(\{0, 2, 3\}, \oplus)$ est un groupe.

Question 5. On considère des ensembles de réels, munis de l'addition.

A $(\{a + b\sqrt{5}\,,\ a, b \in \mathbb{N}\}, +)$ est un groupe.

B $(\{a + b\sqrt{5}\,,\ a, b \in \mathbb{Z}\}, +)$ est un groupe.

C $(\{5a + b\sqrt{5}\,,\ a, b \in \mathbb{Z}\}, +)$ est un groupe.

D $(\{5(a + b\sqrt{5})\,,\ a, b \in \mathbb{N}\}, +)$ est un groupe.

E $(\{a + b\sqrt{5}\,,\ a \in \mathbb{Z}\,,\ b \in \mathbb{N}\}, +)$ est un groupe.

Question 6. On considère des ensembles de complexes, munis de la multiplication.

A $(\mathbb{C}, \times)$ est un groupe.

B $(\{1, -1\}, \times)$ est un groupe.

C $(\{\mathrm{i}, -\mathrm{i}\}, \times)$ est un groupe.

D $(\{0, 1, -1\}, \times)$ est un groupe.

E $(\{1, \mathrm{i}, -1, -\mathrm{i}\}, \times)$ est un groupe.

Question 7. On considère le groupe $(\mathbb{C}^*, \times)$ formé de l'ensemble des nombres complexes non nuls, muni de la multiplication.

A L'application qui à $z \in \mathbb{C}^*$ associe z^2 est un automorphisme de $(\mathbb{C}^*, \times)$.
B L'application qui à $z \in \mathbb{C}^*$ associe $2z$ est un morphisme de $(\mathbb{C}^*, \times)$.
C L'application qui à $z \in \mathbb{C}^*$ associe $1/z^2$ est un morphisme de $(\mathbb{C}^*, \times)$.
D L'application qui à $z \in \mathbb{C}^*$ associe $z/\overline{z}$ est un automorphisme de $(\mathbb{C}^*, \times)$.
E L'application qui à $z \in \mathbb{C}^*$ associe $1/z$ est un automorphisme de $(\mathbb{C}^*, \times)$.

Question 8.

A L'application qui à $x \in \mathbb{R}$ associe $\mathrm{e}^{(1+\mathrm{i})x}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.
B L'application qui à $x \in \mathbb{R}$ associe $(1+\mathrm{i})x$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}, +)$.
C L'application qui à $x \in \mathbb{R}$ associe $(1+\mathrm{i})x$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.
D L'application qui à $x \in \mathbb{R}$ associe $x\mathrm{e}^{\mathrm{i}x}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}, +)$.
E L'application qui à $x \in \mathbb{R}$ associe $(x+\mathrm{i})\mathrm{e}^{\mathrm{i}x}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.

Question 9.

A $(\{a\sqrt{2} + b\sqrt{3}\,,\ a, b \in \mathbb{Z}\}, +, \times)$ est un anneau.
B $(\{2a\sqrt{3}\,,\ a \in \mathbb{Z}\}, +, \times)$ est un anneau.
C $(\{a + b\sqrt{3}\,,\ a, b \in \mathbb{Z}\}, +, \times)$ est un anneau.
D $(\{2a + b\sqrt{3}\,,\ a, b \in \mathbb{Z}\}, +, \times)$ est un anneau.
E $(\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\,,\ a, b, c, d \in \mathbb{Z}\}, +, \times)$ est un anneau.

Question 10. On considère $(Z_6, \oplus, \otimes)$, c'est-à-dire l'ensemble $\{0, 1, 2, 3, 4, 5\}$ muni de l'addition modulo 6 et de la multiplication modulo 6.

A Tout élément non nul de Z_6 possède un inverse pour $\otimes$.
B $(Z_6, \oplus, \otimes)$ est un corps.
C L'élément 4 est son propre inverse pour la multiplication.
D L'élément 5 est son propre inverse pour la multiplication.
E $(Z_6, \oplus, \otimes)$ est un anneau commutatif.

Réponses : 1–BE 2–DE 3–AB 4–CD 5–BC 6–BE 7–CE 8–AB 9–CE 10–DE

2.4 Devoir

Essayez de bien rédiger vos réponses, sans vous reporter ni au cours, ni au corrigé. Si vous souhaitez vous évaluer, donnez-vous deux heures ; puis comparez vos réponses avec le corrigé et comptez un point pour chaque question à laquelle vous aurez correctement répondu.

Questions de cours : Soit G un groupe fini et H un sous-groupe de G.

1. Soit $\sim$ la relation définie sur G par :

$$\forall a, b \in G\ , \quad a \sim b \iff ab^{-1} \in H\ .$$

   Montrer que $\sim$ est une relation d'équivalence sur G.
2. Soit a un élément de G et h un élément de H. Montrer que $ha \sim a$.
3. Montrer que si a et b sont deux éléments de G tels que $a \sim b$, alors il existe un élément h de H tel que $b = ha$.
4. Soit a un élément quelconque de G. On note $\mathfrak{cl}(a)$ sa classe d'équivalence pour la relation $\sim$. Soit f l'application qui à un élément h de H associe l'élément ha. Montrer que f est une bijection de H dans $\mathfrak{cl}(a)$.
5. En déduire que le cardinal de H divise le cardinal de G.

Exercice 1 : Soient r et s les applications de $\mathbb{C}$ dans lui-même définies comme suit.

$$\begin{array}{ccc} & r & \\ \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & r(z) = \mathrm{i}z \end{array} \qquad \begin{array}{ccc} & s & \\ \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & s(z) = \overline{z}\ . \end{array}$$

Dans tout l'exercice, on identifiera l'application f de $\mathbb{C}$ dans $\mathbb{C}$, avec l'application du plan complexe dans lui-même, qui à un point M d'affixe z associe le point M' d'affixe $f(z)$.

1. On note r^2 et r^3 les composées $r^2 = r \circ r$ et $r^3 = r \circ r \circ r$. Interpréter comme transformations géométriques du plan complexe les applications r, r^2, r^3, s, $s \circ r$, $s \circ r^2$, $s \circ r^3$.
2. On note e l'application indentité du plan complexe. Montrer que l'ensemble

$$\{e, r, r^2, r^3, s, s \circ r, s \circ r^2, s \circ r^3\}\ ,$$

   muni de la composition des applications est un groupe, dont on donnera la table de composition. Il sera noté G.
3. Montrer que $\{e, r^2\}$, $\{e, s\}$, $\{e, s \circ r\}$, $\{e, s \circ r^2\}$, $\{e, s \circ r^3\}$, sont des sous-groupes de G, tous isomorphes à Z_2.
4. Montrer que $\{e, s, r^2, s \circ r^2\}$ est un sous-groupe de G, isomorphe à $Z_2 \times Z_2$.
5. Montrer que $\{e, r, r^2, r^3\}$ est un sous-groupe de G, isomorphe à Z_4.
6. On note :
   - A_1 le point du plan complexe d'affixe $1 + \mathrm{i}$,
   - A_2 le point du plan complexe d'affixe $-1 + \mathrm{i}$,
   - A_3 le point du plan complexe d'affixe $-1 - \mathrm{i}$,
   - A_4 le point du plan complexe d'affixe $1 - \mathrm{i}$,

   Vérifier que chaque élément du groupe G laisse invariant l'ensemble $\{A_1, A_2, A_3, A_4\}$.

7. Étant donné un élément f du groupe G, on lui associe la permutation $\varphi(f)$ de $\{1,2,3,4\}$ définie par :

$$\forall i,j \in \{1,2,3,4\}\ , \quad \varphi(f)(i) = j \iff f(A_i) = A_j\ .$$

On définit ainsi une application φ de G dans $\mathcal{S}_4$. Montrer que φ est un morphisme de groupes.

8. Écrire in extenso l'image par φ de chacun des éléments de G.
9. Soit H l'image de G par φ. Montrer que H est un sous-groupe de $\mathcal{S}_4$, isomorphe à G.
10. On note :
    - B_1 le point du plan complexe d'affixe $1+\mathrm{i}$,
    - B_2 le point du plan complexe d'affixe $-1-\mathrm{i}$,
    - B_3 le point du plan complexe d'affixe $1-\mathrm{i}$,
    - B_4 le point du plan complexe d'affixe $-1+\mathrm{i}$,

    Reprendre les questions 6, 7, 8, 9, en remplaçant A_1, A_2, A_3, A_4 par B_1, B_2, B_3, B_4.

Exercice 2 : On note A l'ensemble de réels suivant :

$$A = \Big\{ m + n\sqrt{6}\,,\ m,n \in \mathbb{Z} \Big\}.$$

1. Montrer que $(A,+,\times)$ (ensemble A muni de l'addition et de la multiplication des réels), est un sous-anneau de $(\mathbb{R},+,\times)$.
2. On considère l'application ϕ, de A dans lui-même, qui à $m+n\sqrt{6}$ associe :

$$\phi(m+n\sqrt{6}) = m - n\sqrt{6}\ .$$

Montrer que ϕ est un automorphisme de l'anneau $(A,+,\times)$ (c'est-à-dire une bijection, et un morphisme pour chacune des deux lois).

3. Pour tout $x \in A$, on pose $N(x) = x\phi(x)$. Montrer que N est une application de A dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.
4. Démontrer que x est un élément inversible de A si et seulement si $N(x) = \pm 1$.
5. Vérifier que $5+2\sqrt{6}$ est inversible dans A et calculer son inverse.

2.5 Corrigé du devoir

Questions de cours :

1. La relation $\sim$ est :
    - *réflexive* :
      Soit a un élément de G. Le produit $aa^{-1} = e$ appartient à H (tout sous-groupe de G contient l'élément neutre). Donc $a \sim a$.

- *symétrique* :
  Soient a et b deux éléments de G. Supposons $a \sim b$. Alors ab^{-1} appartient à H. Donc l'inverse de ab^{-1} appartient aussi à H. Or cet inverse est $(ab^{-1})^{-1} = ba^{-1}$. Donc $b \sim a$.
- *transitive* :
  Soient a, b, c trois éléments de G. Supposons $a \sim b$ et $b \sim c$. Les deux éléments ab^{-1} et bc^{-1} appartiennent à H, donc leur produit aussi. Ce produit est : $(ab^{-1})(bc^{-1}) = ac^{-1})$. Donc $a \sim c$.

Donc $\sim$ est une relation d'équivalence sur G.

2. L'inverse de ha est $a^{-1}h^{-1}$. Donc $a(ha)^{-1} = (aa^{-1})h^{-1} = h^{-1} \in H$. Donc $a \sim ha$.
3. Si $a \sim b$, $ab^{-1} \in H$. Notons h l'inverse de cet élément : $h = (ab^{-1})^{-1} = ba^{-1}$. Il appartient aussi à H. On a bien $ha = ba^{-1}a = b$.
4. D'après la question 2, pour tout $a \in G$, $a \sim ha$, donc $f(h) \in \mathfrak{cl}(a)$. Soit b un élément de $\mathfrak{cl}(a)$, c'est -à-dire tel que $a \sim b$. D'après la question 3, il existe $h \in H$ tel que $b = ha$, donc $b = f(h)$: l'application f est surjective.
   Montrons que f est injective. Soient h_1 et h_2 deux éléments de H tels que $f(h_1) = f(h_2)$. Alors $h_1 a = h_2 a$, donc $h_1 a a^{-1} = h_2 a a^{-1}$, soit $h_1 = h_2$.
   L'application f est donc une bijection de H dans $\mathfrak{cl}(a)$.
5. S'il existe une application bijective entre deux ensembles finis, alors ces deux ensembles ont même cardinal. D'après la question 4, pour tout $a \in G$, le cardinal de $\mathfrak{cl}(a)$ est égal au cardinal de H. Or l'ensemble des classes d'équivalence pour $\sim$ constitue une partition de E. Donc le cardinal de E est la somme des cardinaux des classes d'équivalence, qui sont tous égaux au cardinal de H. Le cardinal de E est donc un multiple entier du cardinal de H.

Exercice 1 :

1. Soit O l'origine du plan complexe.
   - r est la rotation de centre O et d'angle $\pi/2$.
   - r^2 est la rotation de centre O et d'angle π.
   - r^3 est la rotation de centre O et d'angle $3\pi/2$ (ou $-\pi/2$).
   - s est la symétrie par rapport à l'axe horizontal.
   - $s \circ r$ est la symétrie par rapport à la droite d'équation $y = -x$ (seconde bissectrice).
   - $s \circ r^2$ est la symétrie par rapport à l'axe vertical.
   - $s \circ r^3$ est la symétrie par rapport à la droite d'équation $y = x$ (première bissectrice).
2. Pour montrer que G est un groupe, il suffit de vérifier que c'est un sous-groupe de l'ensemble $\mathcal{S}(\mathbb{C})$ des bijections du plan complexe dans lui-même. L'ensemble proposé est non vide. Observons ensuite que r et r^3 sont inverses l'un de l'autre,

et que chacun des autres éléments de G est son propre inverse. La table de composition ci-dessous montre que le produit de deux éléments quelconques de G est encore dans G. Donc G est un sous-groupe de $\mathcal{S}(\mathbb{C})$. Dans cette table, nous omettons les signes $\circ$ par souci de clarté.

$\circ$	e	r	r^2	r^3	s	sr	sr^2	sr^3
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	sr^3	s	sr	sr^2
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	e	r	r^2	sr^3
sr	sr	sr^2	sr^3	s	r^3	e	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	e	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	e

3. Nous le montrons pour $\{e, r^2\}$, le raisonnement est identique pour les 4 autres. Dans la mesure où r^2 est son propre inverse, $\{e, r^2\}$ est bien un sous-groupe de G. L'application qui à e associe 0 et à r^2 associe 1 est une bijection, et c'est un morphisme pour la loi $\circ$ au départ, et pour l'addition modulo 2 à l'arrivée. Il suffit pour cela de s'assurer que les tables de composition correspondent.

$\circ$	e	r^2
e	e	r^2
r^2	r^2	e

$+$	0	1
0	0	1
1	1	0

4. Ici encore, le plus simple est de définir la bijection, puis de vérifier que c'est un morphisme pour les deux lois en comparant les tables de composition. Remarquons que l'existence d'un isomorphisme entre un sous-ensemble de G et un groupe connu, nous dispense de montrer que ce sous-ensemble est effectivement un sous-groupe. Comme bijection nous choisissons l'application φ, définie par :

$$\varphi(e) = (0,0)\ , \quad \varphi(s) = (0,1)\ , \quad \varphi(r^2) = (1,0)\ , \quad \varphi(s \circ r^2) = (1,1)\ .$$

$\circ$	e	s	r^2	sr^2
e	e	s	r^2	sr^2
s	s	e	sr^2	r^2
r^2	r^2	sr^2	e	s
sr^2	sr^2	r^2	s	e

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

5. Même technique ; la bijection est définie par :

$$\varphi(e) = 0\ , \quad \varphi(r) = 1\ , \quad \varphi(r^2) = 2\ , \quad \varphi(r^3) = 3\ .$$

$\circ$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

6. Vérifions-le pour r et pour s.

$$r(A_1) = A_2\ , \quad r(A_2) = A_3\ , \quad r(A_3) = A_4\ , \quad r(A_4) = A_1\ .$$
$$s(A_1) = A_4\ , \quad s(A_2) = A_3\ , \quad s(A_3) = A_2\ , \quad s(A_4) = A_1\ .$$

Puisque r et s laissent invariant l'ensemble $\{A_1, A_2, A_3, A_4\}$, c'est aussi le cas pour toute transformation du plan composée de r et s, donc pour tous les éléments du groupe G.

7. Soient f et g deux éléments du groupe G. Soient σ et τ les deux permutations de $\mathcal{S}_4$ telles que pour tout $i = 1, 2, 3, 4$:

$$f(A_i) = A_{\sigma(i)} \quad \text{et} \quad g(A_i) = A_{\tau(i)}\ .$$

Alors, pour tout $i = 1, 2, 3, 4$,

$$f \circ g(A_i) = f(g(A_i)) = f(A_\tau(i)) = A_{\sigma(\tau(i))} = A_{\sigma\circ\tau(i)}\ .$$

Donc $\varphi(f\circ g) = \sigma\circ\tau = \varphi(f)\circ\varphi(g)$. Donc φ est un morphisme pour la composition des applications dans G au départ, et pour la composition des permutations à l'arrivée.

8. Voici le tableau donnant l'image par φ des éléments de G.

f	$\varphi(f)$	f	$\varphi(f)$
e	$(1,2,3,4)$	s	$(4,3,2,1)$
r	$(2,3,4,1)$	sr	$(3,2,1,4)$
r^2	$(3,4,1,2)$	sr^2	$(2,1,4,3)$
r^3	$(4,1,2,3)$	sr^3	$(1,4,3,2)$

9. Puisque φ est un morphisme, H est un sous-groupe de G. Le tableau de la question précédente liste tous les éléments de H, qui sont tous distincts. Donc la restriction de φ à H à l'arrivée est une bijection : φ est donc un isomorphisme de G sur H.

10. Les deux ensembles $\{B_1, B_2, B_3, B_4\}$ et $\{A_1, A_2, A_3, A_4\}$ sont les mêmes. Les deux sont invariants par G. Le raisonnement pour montrer que φ est un morphisme est identique. Par contre les permutations images des éléments de G ne sont pas les mêmes.

f	$\varphi(f)$	f	$\varphi(f)$
e	$(1,2,3,4)$	s	$(3,4,1,2)$
r	$(4,2,3,1)$	sr	$(2,1,3,4)$
r^2	$(2,1,4,3)$	sr^2	$(4,3,2,1)$
r^3	$(3,2,4,1)$	sr^3	$(1,2,4,3)$

On démontre de la même façon que φ est un isomorphisme de G sur son image. On obtient ainsi un nouveau sous-groupe de $\mathcal{S}_4$, isomorphe au précédent.

Exercice 2 :

1. L'ensemble A est non vide. Il suffit de vérifier que A est un sous-groupe pour l'addition, et que la multiplication est stable. Soient m, n, m', n' quatre éléments de $\mathbb{Z}$.
$$(m + n\sqrt{6}) - (m' + n'\sqrt{6}) = (m - m') + (n - n')\sqrt{6} .$$
Donc $(m + n\sqrt{6}) - (m' + n'\sqrt{6}) \in A$.
$$(m + n\sqrt{6}) \times (m' + n'\sqrt{6}) = (mm' + 6nn') + (mn' + m'n)\sqrt{6} .$$
Donc $(m + n\sqrt{6}) \times (m' + n'\sqrt{6}) \in A$.
2. Observons d'abord que pour tout élément a de A, $\varphi(\varphi(a)) = a$. Donc φ est une bijection, puisque tout élément de A a pour antécédent $\varphi(a)$.
Montrons maintenant que φ est un morphisme pour l'addition.
$$\begin{aligned}\varphi((m + n\sqrt{6}) + (m' + n'\sqrt{6})) &= \varphi((m + m') + (n + n')\sqrt{6}) \\ &= (m + m') - (n + n')\sqrt{6} \\ &= (m - n\sqrt{6}) + (m' - n'\sqrt{6}) \\ &= \varphi(m + n\sqrt{6}) + \varphi(m' + n'\sqrt{6}) .\end{aligned}$$
Montrons enfin que φ est un morphisme pour la multiplication.
$$\begin{aligned}\varphi((m + n\sqrt{6}) \times (m' + n'\sqrt{6})) &= \varphi((mm' + 6nn') + (mn' + m'n)\sqrt{6}) \\ &= (mm' + 6nn') - (mn' + m'n)\sqrt{6} \\ &= (m - n\sqrt{6}) \times (m' - n'\sqrt{6}) \\ &= \varphi(m + n\sqrt{6}) \times \varphi(m' + n'\sqrt{6}) .\end{aligned}$$
3. Soit $a = m + n\sqrt{6}$ un élément quelconque de A.
$$N(a) = a\varphi(a) = (m + n\sqrt{6}) \times (m - n\sqrt{6}) = m^2 - 6n^2 .$$
Donc N est bien une application de A dans $\mathbb{Z}$. Montrons que c'est un morphisme pour la multiplication. Soient a et a' deux éléments de A.
$$N(aa') = aa'\varphi(aa') = aa'\varphi(a)\varphi(a') = (a\varphi(a))(a'\varphi(a')) = N(a)N(a') ,$$
en utilisant le fait que φ est un morphisme pour la multiplication.
4. Si $N(x) = x\varphi(x) = 1$, alors $\varphi(x)$ est inverse de x, et si $N(x) = x\varphi(x) = -1$, alors $-\varphi(x)$ est inverse de x : la condition est suffisante. Montrons qu'elle est nécessaire. Soit x un élément inversible de A : il existe y tel que $xy = 1$. Mais comme N est un morphisme pour la multiplication, $N(x)N(y) = 1$. Or $N(x)$ et $N(y)$ sont des entiers. Les seuls éléments de $\mathbb{Z}$ inversibles pour la multiplication sont 1 et -1. D'où le résultat.

5. Il suffit de calculer l'image par N, et d'appliquer le résultat de la question précédente.
$$N(5+2\sqrt{6}) = 25 - 24 = 1 \ .$$
L'inverse de $5+2\sqrt{6}$ est $5-2\sqrt{6}$.

3 Compléments

3.1 Le programme d'Erlangen

Le programme d'Erlangen est un programme de recherche publié par le mathématicien allemand Felix Klein en 1872 dans un mémoire intitulé *Vergleichende Betrachtungen über neuere geometrische Forschungen*, c'est-à-dire *Étude comparée de différentes recherches récentes en géométrie*.

Felix Klein (1849-1925) naît le 25 avril 1849 à Düsseldorf en Rhénanie alors sous domination prussienne, pendant des journées d'émeutes anti-prussiennes. Il sera toujours très fier d'avoir pour date de naissance trois carrés de nombres premiers (5^2, 2^2 et 43^2). En juillet 1870, après avoir voulu faire des études de physique, Klein est déjà docteur en mathématiques et il se trouve à Paris mais la guerre franco-allemande l'oblige à retourner en Allemagne. Il sert un temps dans l'armée prussienne avant d'être nommé lecteur à Göttingen en 1871. En 1872 (à l'âge de 23 ans !), Klein devient professeur à Erlangen grâce à l'aide providentielle d'Alfred Clebsch (1833-1872, il était temps...) qui voit en lui l'un des futurs plus grands mathématiciens de son temps. En 1875, il épouse Anne Hegel, la petite-fille du philosophe Georg Wilhelm Friedrich Hegel (1770-1831). Installé à Göttingen de 1886 jusqu'à sa mort, Klein s'y consacre en particulier à faire de la revue *Mathematische Annalen* un des journaux de mathématiques les plus connus au monde. Par ailleurs, grâce à ses efforts et à ceux de quelques autres, les femmes sont admises à Göttingen à partir de 1893. Klein supervise lui-même le premier doctorat obtenu par une femme dans une université allemande, toutes disciplines confondues, en l'occurrence la thèse de mathématiques de Grace Chisolm Young (1868-1944), une étudiante anglaise d'Arthur Cayley (1821-1895) qui lui rendra hommage à sa mort. Voici comment elle décrit ses rapports avec Klein au début de sa thèse :

> Professor Klein's attitude is this, he will not countenance the admission of any woman who has not already done good work, and can bring proof of the same in the form of degrees or their equivalent [...] and further he will not take any further steps till he has assured himself by a personal interview of the solidity of her claims. Professor Klein's view is moderate. There are members of the Faculty here who are more eagerly in favour of the admission of women and others who disapprove altogether.

Les premières découvertes importantes de Klein datent de 1870. En collaboration avec le mathématicien norvégien Sophus Lie (1842-1899) qui lui avait présenté le concept de groupes, Klein étudie les propriétés fondamentales des lignes asymptotiques sur la surface de Kummer. Klein et Lie en viennent ainsi à s'intéresser aux courbes invariantes sous un groupe de transformations projectives.

En 1871, Klein montre que les géométries euclidienne et non-euclidienne sont des cas particuliers d'une géométrie définie sur une surface projective. Un corollaire est que les axiomes de la géométrie non euclidienne sont consistants si et seulement si ceux de la géométrie euclidenne le sont, ce qui met fin à une controverse persistante autour des

géométries non euclidiennes.

À son arrivée à Erlangen en 1872, et comme c'est l'usage en pareil cas, Klein doit prononcer un cours inaugural. Il rédige alors le texte qui deviendra connu sous le nom de *Programme d'Erlangen*. Ce texte ne sera jamais donné comme cours puisque Klein prononcera finalement un autre discours mais il influencera profondément le développement et l'évolution de la géométrie et des mathématiques dans leur ensemble. Klein y propose une vision unifiée de la géométrie et décrit en détails comment les propriétés fondamentales d'une géométrie donnée se traduisent par l'action d'un groupe de transformations. Son objectif est donc d'unifier les différentes géométries apparues au cours du XIX^{e} siècle pour en dégager les points de similitude : la géométrie affine, la géométrie projective, la géométrie euclidienne et la géométrie non euclidienne. La clef de voûte de ce programme consiste à fonder la géométrie sur les notions d'actions de groupe et d'invariants, un point de vue révolutionnaire à l'époque qui apparut parfois comme une remise en question de la géométrie elle-même.

Il n'en est rien et le mathématicien, physicien et philosophe français Henri Poincaré (1854-1912) par exemple était arrivé de son côté, dès 1880 et sans connaître le *Programme* de Klein, à la conclusion que toute géométrie se réduit fondamentalement à l'étude d'un groupe de transformations. Poincaré était déjà si bien convaincu de l'importance des idées de théorie des groupes en géométrie et pour toutes les mathématiques que lors du passage de Sophus Lie à Paris en 1882 il n'hésite pas à lui déclarer que la géométrie n'est que l'étude de certains groupes de transformations. Lie décrit alors à Poincaré le *Programme d'Erlangen* de Klein. Encore aujourd'hui, la philosophie du *Programme* influence de nombreux mathématiciens ainsi que des programmes d'enseignement et de recherche. Cette vision est même devenue tellement banale dans l'esprit des mathématiciens qu'il est difficile de juger de son importance, d'apprécier sa nouveauté et de comprendre les oppositions à laquelle elle a dû faire face.

Notons que Klein est parfois surtout connu pour avoir le premier décrit en 1882 une surface maintenant appelée *bouteille de Klein*. Ce nom résulte d'au moins une et peut-être même de deux erreurs de traduction ! En effet, l'expression allemande *Kleinsche Fläche* signifie *surface de Klein* et il y a eu confusion entre *Fläche* (surface) et *Flasche* (bouteille). Cependant le terme fautif s'est imposé, y compris en allemand où l'on utilise maintenant le terme *Kleinsche Flasche* (bouteille de Klein). Il semble même que *Kleinsche* résulte d'une deuxième confusion, cette fois avec *kleine* (petite), de sorte que la fameuse bouteille de Klein ne serait finalement qu'une *petite surface*... ce qui ne l'empêche pas d'être un objet absolument remarquable !

Nous terminerons par une anecdote : le mathématicien et logicien Ernst Zermelo (1871-1953) enseignait à Göttingen à un moment où « Herr Geheimrat » Felix Klein régnait sur le légendaire département de mathématiques. Zermelo stupéfia ses étudiants en leur proposant l'exercice suivant :

> On peut ranger tous les mathématiciens de Göttingen en deux catégories : dans la première catégorie sont ceux qui font ce que Felix Klein aime mais qu'ils n'aiment pas ; dans la seconde catégorie sont ceux qui font ce qu'ils

aiment mais que Felix Klein n'aime pas. À quelle catégorie Felix Klein appartient-il ?

Les étudiants étaient terrorisés par un tel sacrilège et aucun d'eux ne sut répondre. La réponse de Zermelo était pourtant simple :

Felix Klein n'est donc pas un mathématicien.

La fin de l'anecdote est que Zermelo n'obtint jamais de poste de professeur à Göttingen.

3.2 Hamilton et les quaternions

On peut voir l'ensemble $\mathbb{C}$ des nombres complexes comme l'ensemble $\mathbb{R}^2$ des couples de nombres réels, en identifiant $a + \mathrm{i}b$ et (a, b). La multiplication dans $\mathbb{C}$ correspond alors à une façon de multiplier les couples de nombres réels :

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Ce point de vue a été développé en 1835 par William Hamilton. Par la suite, il essaya longuement et sans succès de multiplier des triplets de nombres réels de façon satisfaisante mais il finit par réussir à multiplier des quadruplets, inventant ainsi en 1843 l'ensemble des quaternions, noté $\mathbb{H}$ en son honneur.

Sir William Rowan Hamilton (1805-1865), né à Dublin, fut à la fois un enfant adopté et un enfant surdoué. À 13 ans, il parlait autant de langues que le nombre de ses années : bien sûr la plupart des langues européennes mais aussi les langues persane, arabe, hindoue, malaise, et le sanskrit. Il resta toute sa vie au Trinity College de Dublin, où il avait été nommé professeur d'astronomie à l'âge de 22 ans. Calculateur génial, il semble avoir pris grand plaisir toute sa vie durant à effectuer des multiplications monstrueuses. À 10 ans, il découvre par accident une copie en latin des *Éléments* d'Euclide et à 12 ans il dévore les *Principia* de Newton. Pendant l'été 1822, à 17 ans, il étudie de manière systématique la *Mécanique céleste* de Laplace et y trouve une faute sérieuse, qu'il réussit à corriger. Hamilton décide alors de se consacrer principalement aux mathématiques, ce qui ne l'empêchera pas de fournir également d'importantes contributions en optique et en mécanique.

Le but de Hamilton était donc d'étendre les propriétés des nombres complexes à des dimensions supérieures, essentiellement sans succès. D'ailleurs Frobenius démontrera en 1877 qu'une telle structure ne pouvait pas exister pour l'ensemble des triplets. Hamilton racontera plus tard que, dans la soirée du 16 octobre 1843, il marchait le long du Canal royal de Dublin avec sa femme, en route vers une soirée, quand la solution pour des quadruplets lui apparut soudain, sous la forme

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1,$$

et qu'il grava aussitôt ces équations au couteau dans une pile du pont le plus proche, Broom Bridge. Depuis 1989, la National University d'Irlande organise un pèlerinage

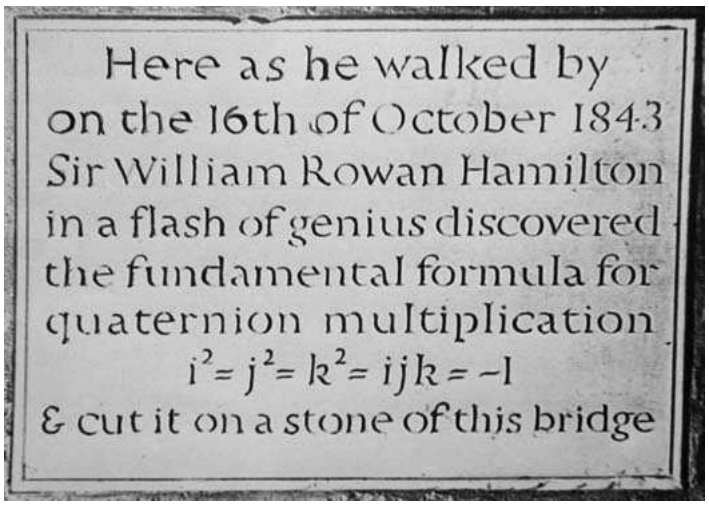

FIGURE 3 – Broom Bridge à Dublin

depuis l'observatoire de Dunsink où Hamilton travaillait jusqu'à ce pont où malheureusement, aucune trace de la formule gravée en 1843 ne demeure (par contre une plaque commémore le geste de Hamilton).

Hamilton aboutit aux quaternions en imposant de respecter la multiplication des modules et en conservant l'associativité mais, geste révolutionnaire pour l'époque, en abandonnant la commutativité. Pour présenter l'algèbre $\mathbb{H}$ en termes modernes, rappelons que le corps $\mathbb{C}$ des nombres complexes peut être représenté par l'algèbre des matrices à coefficients réels de la forme

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Une façon de le voir est de représenter le nombre complexe $a+b\mathrm{i}$ par la transformation de $\mathbb{C}$ dans $\mathbb{C}$ définie par $z \mapsto (a+b\mathrm{i}) \cdot z$, transformation $\mathbb{R}$-linéaire dont la matrice dans la base $(1, \mathrm{i})$ de l'espace vectoriel $\mathbb{C}$ sur $\mathbb{R}$ est précisément la matrice ci-dessus.

De même on représente un quaternion par une matrice complexe

$$\begin{pmatrix} a+b\mathrm{i} & -c-d\mathrm{i} \\ c-d\mathrm{i} & a-b\mathrm{i} \end{pmatrix}.$$

Cette fois, on considère la base $(1, \mathrm{j})$ de l'espace vectoriel complexe $\mathbb{H}$ et il s'agit de la matrice dans cette base de la transformation de $\mathbb{H}$ dans $\mathbb{H}$ définie par

$$h \mapsto ((a+b\mathrm{i}) + (c+d\mathrm{i}) \cdot \mathrm{j}) \cdot h.$$

En effet, les formules de Broom Bridge impliquent également les relations

$$\mathrm{ij} = \mathrm{k},\ \mathrm{ik} = -\mathrm{j},\ \mathrm{ji} = -\mathrm{k},\ \mathrm{jk} = \mathrm{i},\ \mathrm{ki} = \mathrm{j},\ \mathrm{kj} = -\mathrm{i},$$

ce qui permet de compléter la « table de multiplication » de $\{1, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$. Tout quaternion h peut donc s'écrire comme une combinaison linéaire à coefficients réels des vecteurs de la base $(1, \mathrm{i}, \mathrm{j}, \mathrm{k})$ de $\mathbb{H}$ sur $\mathbb{R}$, soit $h = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ avec $(a, b, c, d) \in \mathbb{R}^4$, ou bien comme une combinaison linéaire à coefficients complexes des vecteurs de la base $(1, \mathrm{j})$ de $\mathbb{H}$ sur $\mathbb{C}$, soit $h = z + w\mathrm{j}$ avec $(z, w) \in \mathbb{C}^2$.

Il est essentiel ici de considérer $\mathbb{H}$ comme un espace vectoriel sur $\mathbb{C}$ *à droite* sinon la multiplication ainsi définie n'est pas $\mathbb{C}$-linéaire. En particulier, pour identifier la première colonne, on utilisera la relation

$$(a + b\mathrm{i}) + (c + d\mathrm{i})\mathrm{j} = (a + b\mathrm{i}) + \mathrm{j}(c - d\mathrm{i}).$$

Cette découverte démontra la nécessité de travailler aussi avec des lois non commutatives, une avancée radicale pour l'époque. Il faut se rappeler que vecteurs et matrices faisaient encore partie du futur, mais Hamilton venait en quelque sorte d'introduire avant l'heure le produit vectoriel et le produit scalaire des vecteurs.

On sait à présent que bien avant Hamilton, en 1748, le mathématicien et physicien suisse Leonhard Euler (1707-1783) connaissait la règle de multiplication des quaternions, sous la forme du théorème des quatre carrés, ainsi que le mathématicien, astronome et physicien allemand Carl Friedrich Gauss (1777-1855) en 1819. Hamilton quant à lui passa le reste de sa vie à explorer cette notion car il pensait que sa découverte allait révolutionner la physique mathématique. La postérité démentit ce pronostic et porta un regard souvent sévère sur son invention. D'après le physicien mathématicien et ingénieur écossais William Thomson alias Lord Kelvin (1824-1907) par exemple (oui, le Kelvin des degrés Kelvin) :

> Quaternions came from Hamilton after his really good work had been done, and though beautifully ingenious, have been an unmixed evil to those who have touched them in any way.

3.3 Les idéaux d'Emmy Noether

La théorie des anneaux et de leurs idéaux est un des nombreux produits de la réflexion sur les équations diophantiennes, et leur cas particulier le plus célèbre, le Dernier Théorème de Fermat. Au XIX$^{\mathrm{e}}$ siècle, on se rendit compte que pour étudier l'équation $x^p + y^p = z^p$ et bien d'autres, il serait utile d'étendre à d'autres ensembles de nombres que $\mathbb{Z}$ le théorème fondamental de l'arithmétique selon lequel on peut décomposer tout nombre en produit de facteurs premiers. En premier lieu, viennent les ensembles d'entiers cyclotomiques. Si p est un nombre premier, un *entier cyclotomique* est une combinaison linéaire à coefficients entiers des racines p-ièmes de l'unité. Par exemple pour $p = 3$:

$$4 - 5\left(-\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}\right) + 2\left(-\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}\right) .$$

Le rapport avec Fermat ? Tout simplement le fait que si $z^p = x^p + y^p$ et x, y, z sont entiers, alors z^p, x^p et y^p sont des produits d'entiers cyclotomiques. Par exemple :

$$x^p = z^p - y^p = \prod_{k=1}^{p} (z - r_k\, y) \ ,$$

où les r_k sont les racines p-ièmes de l'unité. En 1847, Lamé annonça avoir démontré le théorème de Fermat, mais il supposait que tous les entiers cyclotomiques possédaient une décomposition unique. Or en 1844, Kummer avait montré que ce n'était pas le cas. Interprétant le fait que la décomposition ne soit pas unique comme l'absence de certains facteurs premiers, il eut l'idée de les rajouter en les baptisant « nombres idéaux ». La théorie des idéaux, formalisée plus tard par Dedekind, vise donc à étendre dans un anneau quelconque la notion de facteur premier dans $\mathbb{Z}$. Qu'est-ce qu'un idéal I dans un anneau commutatif A ? C'est un sous-groupe pour l'addition, possédant en plus une propriété de stabilité :

$$\forall a \in A\ ,\ \forall x \in I\ , \quad ax \in I\ .$$

Dans $\mathbb{Z}$, les idéaux sont les ensembles de multiples d'un même nombre. Petit à petit les propriétés des anneaux permettant d'étendre les opérations de l'arithmétique prirent forme, et la théorie des idéaux permit de généraliser à des ensembles de nombres quelconques les outils de l'arithmétique.

Emmy Noether [1] naît à Erlangen en 1882, d'un père mathématicien. Elle fait ses études à Erlangen et y soutient une thèse sur la théorie des invariants en 1907. Après sa thèse, personne ne s'oppose à ce qu'elle enseigne à Erlangen... à condition que ce soit sous le nom de son père et sans recevoir de salaire ! Au printemps 1915, Hilbert et Klein la font venir à Göttingen pour travailler sur les problèmes mathématiques liés à la théorie de la relativité générale d'Einstein. Elle réfléchit aussi à des questions d'algèbre plus théoriques, qui conduisent en 1921 à la publication de sa « Théorie des idéaux dans les anneaux ». Elle y atteint une généralité, une simplicité, une efficacité exceptionnelles, et ouvre la voie à une foule de travaux ultérieurs, au point qu'elle est considérée comme la mère de l'algèbre moderne. Sa capacité exceptionnelle à abstraire et à généraliser pour simplifier en se débarrassant des détails inessentiels allait de pair avec une caractéristique profonde de sa personnalité. Elle ne s'est jamais préoccupée ni de sa condition sociale, ni de ses revenus, ni de son confort matériel, ni même semble-t-il de son aspect extérieur. À Göttingen, Hilbert et Klein étaient bien convaincus que Emmy Noether méritait un poste de professeur. Hilbert disait : « Je ne vois pas en quoi le sexe d'un candidat pourrait être un argument contre son recrutement en tant qu'enseignant ; après tout, nous sommes une université, pas un établissement de bains ! » Il fallut trois tentatives et l'intervention d'Albert Einstein lui-même, pour qu'on lui accorde en 1922 le titre de plus bas niveau que l'on ait pu inventer, celui de « professeur non officiel et extraordinaire », avec un salaire minimal. Certains glosèrent

1. Paul Dubreil : Emmy Noether *Cahiers du séminaire d'histoire des mathématiques 7, pp. 15–27 (1986)*

sur le fait qu'un professeur extraordinaire ne savait rien d'ordinaire et un professeur ordinaire ne savait rien d'extraordinaire.

Mais en 1932 les nazis arrivent au pouvoir, et les juifs sont bientôt chassés de l'université ; parmi eux bien sûr Emmy Noether. Lors d'un banquet à l'été 1933, le nouveau ministre de l'éducation nazi demande à Hilbert : « Comment vont les mathématiques à Göttingen maintenant qu'elles ont été débarrassées de leur influence juive ? ». Après un instant de réflexion, Hilbert répond : « Des mathématiques à Göttingen ? Il n'y en a plus. » Après avoir vainement tenté d'obtenir un travail à Moscou et Oxford, Emmy Noether finit par obtenir un poste provisoire dans un « college » américain. Vu l'afflux de scientifiques européens aux États-Unis, embaucher une femme, aux opinions libérales et pacifistes de surcroît, ne coulait pas de source. Heureusement elle était bien défendue, en particulier par Norbert Wiener :

> She is one of the ten or twelve leading mathematicians of the present generation in the entire world... Of all the cases of German refugees, whether in this country or elsewhere, that of Miss Noether is without doubt the first to be considered.

Aux États-Unis, Emmy Noether poursuit son activité mathématique avec un rayonnement encore accru. Malheureusement elle décéde en avril 1935 d'une infection postopératoire. Voici le bel éloge paru le 4 mai 1935 dans le New York Times, sous le nom d'Albert Einstein.

> The efforts of most human-beings are consumed in the struggle for their daily bread, but most of those who are, either through fortune or some special gift, relieved of this struggle are largely absorbed in further improving their worldly lot. Beneath the effort directed toward the accumulation of worldly goods lies all too frequently the illusion that this is the most substantial and desirable end to be achieved ; but there is, fortunately, a minority composed of those who recognize early in their lives that the most beautiful and satisfying experiences open to humankind are not derived from the outside, but are bound up with the development of the individual's own feeling, thinking and acting. The genuine artists, investigators and thinkers have always been persons of this kind. However inconspicuously the life of these individuals runs its course, none the less the fruits of their endeavors are the most valuable contributions which one generation can make to its successors.
>
> Within the past few days a distinguished mathematician, Professor Emmy Noether, formerly connected with the University of Göttingen and for the past two years at Bryn Mawr College, died in her fifty-third year. In the judgment of the most competent living mathematicians, Fräulein Noether was the most significant creative mathematical genius thus far produced since the higher education of women began. In the realm of algebra, in which the most gifted mathematicians have been busy for centuries, she

discovered methods which have proved of enormous importance in the development of the present-day younger generation of mathematicians. Pure mathematics is, in its way, the poetry of logical ideas. One seeks the most general ideas of operation which will bring together in simple, logical and unified form the largest possible circle of formal relationships. In this effort toward logical beauty spiritual formulas are discovered necessary for the deeper penetration into the laws of nature.

Born in a Jewish family distinguished for the love of learning, Emmy Noether, who, in spite of the efforts of the great Göttingen mathematician, Hilbert, never reached the academic standing due her in her own country, none the less surrounded herself with a group of students and investigators at Göttingen, who have already become distinguished as teachers and investigators. Her unselfish, significant work over a period of many years was rewarded by the new rulers of Germany with a dismissal, which cost her the means of maintaining her simple life and the opportunity to carry on her mathematical studies. Farsighted friends of science in this country were fortunately able to make such arrangements at Bryn Mawr College and at Princeton that she found in America up to the day of her death not only colleagues who esteemed her friendship but grateful pupils whose enthusiasm made her last years the happiest and perhaps the most fruitful of her entire career.