Sous la direction de Jean-Pierre Ramis et André Warusfel
Xavier Buff · Emmanuel Halberstadt · François Moulin · Monique Ramis · Jacques Sauloy

Mathématiques

Tout-en-un pour la Licence 2

3e édition

DUNOD

Jean-Pierre Ramis, ancien élève de l'École Normale Supérieure de la rue d'Ulm, membre de l'Institut (Académie des Sciences), membre de l'Institut Universitaire de France, membre de l'Académie des Sciences, Inscriptions et Belles-Lettres de Toulouse, professeur émérite à l'Institut de Mathématique de Toulouse (Université Paul Sabatier), a été directeur de l'Institut de Recherches Mathématiques Avancées de Strasbourg et de l'Institut de Mathématiques de Toulouse.

André Warusfel, ancien élève de l'École Normale Supérieure de la rue d'Ulm, a été professeur de mathématiques spéciales au Lycée Louis-le-Grand à Paris et inspecteur général de Mathématiques.

Xavier Buff, ancien élève de l'École Normale Supérieure de la rue d'Ulm, professeur à l'Institut de Mathématiques de Toulouse, ancien directeur de l'Institut de Recherches sur l'Enseignement des Mathématiques de Toulouse.

Emmanuel Halberstadt, a été maître de conférences à l'Université Paris 6 Pierre et Marie Curie, ancien chargé de cours d'agrégation aux Écoles Normales Supérieures d'Ulm et de Cachan.

François Moulin, ancien élève de l'École Normale Supérieure de la rue d'Ulm, professeur de chaires supérieures au Lycée sainte-Geneviève (spéciales MP*).

Monique Ramis, ancienne élève de l'École Normale Supérieure de Sèvres, a été professeur de chaires supérieures (à Paris, Strasbourg, Toulouse).

Jacques Sauloy, ancien élève de l'École Normale Supérieure de Saint-Cloud, maître de conférences à l'Institut de Mathématiques de Toulouse.

Les éditions Dunod remercient Jean-Marie Monier, professeur de mathématiques en classes préparatoires au lycée La Martinière-Monplaisir (Lyon), pour sa relecture attentive de l'ouvrage.

Illustration de couverture : © Photo gallery – Adobestock.com

© Dunod, Paris, 2007, 2014, 2020
ISBN 978-2-10-080058-2
11 rue Paul Bert, 92240 Malakoff
www.dunod.com

Préface

Les mathématiques constituent l'ossature de la science moderne et sont une source intarissable de concepts nouveaux d'une efficacité incroyable pour la compréhension de la réalité matérielle qui nous entoure. Ainsi l'apprentissage des mathématiques est devenu indispensable pour la compréhension du monde par la science. Les nouveaux concepts eux-mêmes sont le résultat d'un long processus de distillation dans l'alambic de la pensée. Essayer de justifier les mathématiques par leurs applications pratiques n'a guère de sens, tant ce processus de création est sous-tendu par la soif de connaître et non l'intérêt immédiat.
Les mathématiques restent l'un des domaines dans lequel la France excelle et ceci malgré la mutilation des programmes dans le secondaire et l'influence néfaste d'un pédagogisme dont l'effet principal est de compliquer les choses simples.
Vues de loin les mathématiques apparaissent comme la réunion de sujets distincts comme la géométrie, qui a pour objet la compréhension du concept d'espace, l'algèbre, art de manipuler les symboles, l'analyse, science de l'infini et du continu, la théorie des nombres etc. Cette division ne rend pas justice à l'un des traits essentiels des mathématiques qui est leur unité profonde de sorte qu'il est impossible d'en isoler une partie sans la priver de son essence. En ce sens les mathématiques ressemblent à un être biologique qui ne peut survivre que comme un tout et serait condamné à périr si on le découpait en morceaux en oubliant son unité fondamentale.
L'une des caractéristiques de l'apprentissage des mathématiques, c'est la possibilité donnée à tout étudiant de devenir son propre maître et en ce sens il n'y a pas d'autorité en mathématiques. Seules la preuve et la rigueur y font la loi. L'étudiant peut atteindre par le travail une maîtrise suffisante pour pouvoir s'il le faut tenir tête au maître. La rigueur, c'est être sûr de soi, et à l'âge où l'on construit sa personnalité, se confronter au monde mathématique est le moyen le plus sûr de construire sur un terrain solide. Il faut, si l'on veut avancer, respecter un équilibre entre les connaissances qui sont indispensables et le « savoir-faire » qui l'est autant. On apprend les maths en faisant des exercices, en apprenant à calculer sans l'aide de l'ordinateur, en se posant des questions et en ne lâchant pas prise facilement devant la difficulté. Seule la confrontation réelle à la difficulté a une valeur formatrice, en rupture avec ce pédagogisme qui complique les choses simples et mélange l'abstraction mathématique avec le jeu qui n'a vraiment rien à voir. Non, les mathématiques ne sont pas un jeu et l'on n'apprend pas les mathématiques en s'amusant.
L'ouvrage qui suit est un cours soigné et complet idéal pour apprendre toutes les Mathématiques qui sont indispensables au niveau de la Licence. Il regorge d'exercices (700) qui

incitent le lecteur à réfléchir et ne sont pas de simples applications de recettes, et respecte parfaitement l'équilibre nécessaire entre connaissances et savoir-faire, permettant à l'étudiant de construire des images mentales allant bien au-delà de simples connaissances mémorisées. Il s'agit d'un ouvrage de référence pour la Licence, non seulement pour les étudiants en mathématiques mais aussi pour tous ceux qui s'orientent vers d'autres disciplines scientifiques. Il insiste sur la rigueur et la précision et va au fond des notions fondamentales les plus importantes sans mollir devant la difficulté et en respectant constamment l'unité des mathématiques qui interdit tout cloisonnement artificiel. Il répond à une demande de tant de nos collègues d'un ouvrage qui les aide à « redresser la barre », mais sera aussi un atout merveilleux pour l'étudiant travaillant seul par la cohérence et la richesse de son contenu.
Il est l'œuvre d'une équipe qui rassemble des mathématiciens de tout premier plan ayant une véritable passion pour l'enseignement. Il était grand temps !

Alain Connes,
Médaille Fields 1982,
Professeur au Collège de France.

Table des matières

II Analyse

Avant-propos

Cet ouvrage est le deuxième d'une série de trois, conçue pour couvrir les programmes de mathématiques de la plupart des Licences scientifiques.
Dans cette nouvelle édition nous avons, pour certains sujets (en particulier l'intégration), choisi une pédagogie plus progressive. Nous avons ainsi tenu compte, d'une part, de la mise en place des nouveaux programmes de l'enseignement secondaire et des modifications corrélatives des enseignements universitaires et, d'autre part, des remarques de nos lecteurs et de nos collègues enseignants. Cette présentation étant plus détaillée, certains sujets habituellement enseignés au niveau de la deuxième année de licence sont maintenant traités dans le troisième volume de la série, qui couvre par ailleurs un « tronc commun » des programmes de mathématiques au niveau de la troisième année.

Ce cours est illustré d'exemples et applications, il propose de plus au fil du texte de nombreux exercices corrigés qui permettront à l'étudiant de s'entraîner au fur et à mesure de son apprentissage, des notices historiques et un index très complet. On trouvera aussi à la fin de chaque « module » des exercices supplémentaires[1] avec des indications de solutions. Une correction détaillée d'une grande partie de ces exercices est accessible sur le site de l'éditeur.

Nos livres sont conçus comme une aide à l'enseignement oral dispensé par nos collègues dans les cours et travaux dirigés. L'ordre de lecture n'est pas complètement imposé et chaque étudiant peut se concentrer sur tel ou tel aspect en fonction de son programme et de son travail personnel.
Ce livre peut aussi être utilisé par un enseignant comme ouvrage de base pour son cours, dans l'esprit d'une pédagogie encore peu utilisée en France, mais qui a largement fait ses preuves ailleurs. Nous avons aussi pensé à l'étudiant travaillant seul, sans appui d'un corps professoral.

Dans les mathématiques d'aujourd'hui, un certain nombre de théories puissantes sont au premier plan. Leur maniement, au moins à un certain niveau dépendant de la filière choisie, devra évidemment être acquis par l'étudiant à la fin de ses années de licence. Mais celui-ci devra aussi avoir appris à calculer, sans s'appuyer exagérément sur les ordinateurs et les logiciels, à « se débrouiller » devant un problème abstrait ou issu des applications. Nous avons, à cette fin, mis en place une approche adaptée. Nous insistons aussi sur les exigences de rigueur (définitions précises, démonstrations rigoureuses), mais les choses sont mises

[1] Les plus difficiles sont marqués d'une ou deux étoiles.

en place de façon progressive et pragmatique, et nous proposons des exemples riches, dont l'étude met souvent en œuvre des approches multiples. Nous aidons progressivement le lecteur à acquérir le maniement d'un outillage abstrait puissant, sans jamais nous complaire dans l'abstraction pour elle même, ni un formalisme sec et gratuit : le cœur des mathématiques n'est sans doute pas un corpus de théories, si profondes et efficaces soient-elles, mais un certain nombre de problèmes dans toute leur complexité, souvent issus d'une réflexion sur le monde qui nous entoure.

Historiquement, les mathématiques se sont développées pendant des siècles en relation avec les autres sciences. De nos jours, leurs interactions se poursuivent vigoureusement (avec la physique, l'informatique, la mécanique, la chimie, la biologie, l'économie...). Nous souhaitons accompagner ce mouvement au niveau de l'enseignement des premières années d'université et aider à la mise en place, ici ou là, de filières scientifiques pluridisciplinaires contenant une composante mathématique pure ou appliquée. En particulier nous avons introduit de solides initiations aux probabilités et statistique ainsi qu'à l'algorithmique.

Malgré tout le soin apporté à cet ouvrage il est inévitable que quelques erreurs subsistent. Nous prions le lecteur, qui pourra les signaler à l'éditeur ou à l'un d'entre nous pour correction lors d'un nouveau tirage, de nous en excuser.

Jean-Pierre Ramis, André Warusfel

Vous pouvez accéder aux corrigés des exercices supplémentaires à partir de la page de présentation de l'ouvrage sur le site de l'éditeur `www.dunod.com`*. Les corrigés sont au format pdf et permettent une recherche classique par mots clef. Ils peuvent être lus, enregistrés ou imprimés en partie comme en totalité.*

Algèbre

Partie I

L'algèbre au sens moderne a deux visages : d'une part l'étude des structures indépendamment de leurs réalisations concrètes et d'autre part celle d'algorithmes performants permettant des calculs effectifs sur ordinateur.
Elle est issue de l'arithmétique, déjà bien présente chez les anciens Grecs (notamment Euclide), qui a connu de grands développements au XVII^{e} siècle (Fermat), au XVIII^{e} (Euler) et au XIX^{e} (Gauß, Hermite), et joue toujours un rôle très important, central dans un certain nombre de conjectures très célèbres comme celle de Riemann. Vers le milieu du XX^{e} siècle, l'algèbre a permis d'unifier arithmétique et géométrie algébrique, et d'établir aujourd'hui de fascinantes convergences entre arithmétique et physique théorique. Algèbre et arithmétique ont aussi d'importantes applications (cryptographie, codes correcteurs d'erreurs, secret bancaire, communications).
Les « recettes » pour équations du premier et du second degré remontent à une lointaine antiquité : à Babylone (vers 1800 avant Jésus-Christ), en Grèce grâce à Euclide et Diophante, suivis au Moyen Âge par des mathématiciens de langue arabe. Il faudra attendre le XVI^{e} siècle italien pour connaître les formules de résolution par radicaux des équations de degré trois et quatre (Del Ferro, Cardan, Ferrari). Un siècle plus tard, Viète et Descartes essaieront de dépasser ce stade, ce qui conduira ce dernier à inventer au passage la géométrie analytique. Au début du XIX^{e}, Gauß, Abel puis surtout Galois mettront un terme aux recherches vaines de leurs prédécesseurs : « il n'y a plus de formule » à partir du degré cinq. Après avoir joué un très grand rôle dans la construction des mathématiques, le sujet perdait presque tout intérêt ; toutefois les outils inventés pour le clore (groupes, théorie de Galois) restaient centraux dans les mathématiques et certaines de leurs applications.
Dans une perspective plus appliquée, Gauß, au XIX^{e} siècle, a développé des techniques « effectives » d'algèbre linéaire pour l'astronomie (trajectoire de Ceres en 1801). Au XX^{e} les groupes et l'algèbre linéaire interviennent de manière centrale en mécanique quantique et en chimie (cristallographie, chimie quantique). L'algèbre linéaire est aujourd'hui également omniprésente dans de nombreux problèmes industriels (contrôle, optimisation, robotique...).
Ce cours de seconde année approndit nettement deux aspects fondamentaux de l'algèbre, d'une part l'algèbre générale en systématisant les structures quotients (par exemple à propos des anneaux et des polynômes), et d'autre part en traitant l'algèbre linéaire et bilinéaire qui constitue le fonds classique d'une seconde année d'université. Il faut également signaler un important module consacré à la récursivité, complétant l'initiation à l'algorithmique du premier volume.

Compléments d'algèbre

I.1

Nous approfondissons ici, en vue d'applications dans ce volume, les notions d'algèbre de base de [L1] concernant les groupes, les anneaux, les espaces vectoriels et les polynômes.

1 Quotients

Cette section fait appel au vocabulaire de la section « Relations d'équivalence » du module « Fondements » de [L1], qu'il est donc nécessaire de bien maîtriser.

1.1 Quotient d'un ensemble par une relation d'équivalence

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. On notera indifféremment $x\mathcal{R}y$ ou $x \equiv y \pmod{\mathcal{R}}$, ou encore, pour alléger l'écriture, $x \sim y$. Pour certains raisonnements ou calculs portant sur les éléments de E, il n'y a pas lieu de distinguer entre deux éléments équivalents, le résultat obtenu (ou les propriétés étudiées) ne dépendant pas du choix d'un élément particulier dans une classe d'équivalence donnée. Le but de cette section est de se donner des moyens (vocabulaire et méthodes) de raisonner et de calculer sur des objets considérés *à équivalence près*.

Exemple. Pour « vérifier » l'opération $54\,321 \times 6\,789 = 368\,785\,269$, on considère chaque entier naturel n comme « équivalent » à la somme $s(n)$ de ses chiffres. Ainsi, $54\,321 \sim 15 \sim 6$ et $6\,789 \sim 30 \sim 3$. On effectue le calcul sur les équivalents plus simples : $6 \times 3 = 18 \sim 9$. Par ailleurs, $368\,785\,269 \sim 54 \sim 9$. On estime alors que le résultat est plausible : il n'a pas été réfuté par le test dit de la « preuve par neuf ». L'idée sous-jacente est qu'il existe une relation d'équivalence $\sim$ telle que, d'une part, $\forall n \in \mathbb{N}\ ,\ n \sim s(n)$ et que, d'autre part, $a \sim a'$ et $b \sim b' \Rightarrow aa' \sim bb'$. Alors $54\,321 \sim 6$ et $6\,789 \sim 3 \Rightarrow 54\,321 \times 6\,789 \sim 6 \times 3 = 18 \sim 9$. C'est, bien entendu, la relation $\equiv_9$ de congruence modulo 9 qui convient.

Théorème et définition 1. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$, également notée $\sim$. Il existe alors un ensemble $\overline{E}$ et, pour chaque élément x de E, un élément $\overline{x}$ de $\overline{E}$ de telle sorte que l'application $\pi : x \mapsto \overline{x}$ soit surjective de E sur $\overline{E}$ et que l'on ait l'équivalence suivante : $\forall x, y \in E\ ,\ \pi(x) = \pi(y) \Leftrightarrow x \sim y$.
L'ensemble $\overline{E}$ est appelé *ensemble quotient de E par la relation d'équivalence $\mathcal{R}$*, et il est noté $E/\mathcal{R}$. L'application π est appelée *projection canonique* de E sur $\overline{E}$. L'élément $\overline{x}$ de $\overline{E}$ est appelé *classe de x* (dans $\overline{E}$) ; on dit que l'élément x est un *représentant* de $\overline{x}$ (dans E).

Autrement dit, on demande que soient vérifiés les axiomes suivants :

- Deux éléments quelconques de E ont la même classe si, et seulement s'ils sont équivalents : $\forall x, y \in E\ ,\ \overline{x} = \overline{y} \Longleftrightarrow x \sim y$.
- Tout élément de $\overline{E}$ est la classe d'un élément de E ; noter cependant que l'on ne requiert *pas* l'unicité du représentant $x \in E$ de $\overline{x} \in \overline{E}$.

Remarquons d'ailleurs qu'en toute rigueur, c'est l'ensemble $\overline{E}$ *muni de la projection canonique* π que l'on devrait appeler le quotient.

Démonstration. Il y a aux moins deux méthodes pour construire l'ensemble quotient $\overline{E} = E/\mathcal{R}$ et la projection canonique $\pi : E \to \overline{E}$. Dans la première méthode, on choisit, dans chaque classe d'équivalence, un élément arbitraire que l'on note $\overline{x}$. C'est possible grâce à l'axiome du choix (module « Fondements » de [L1]). L'ensemble $\overline{E} := \{\overline{x} \mid x \in E\}$ est donc, dans ce cas, un *ensemble de représentants.*
Dans la deuxième méthode, on pose $\overline{x} := \mathrm{cl}(x)$. L'objet $\overline{x}$ est donc *l'ensemble des éléments de E équivalents à x*, donc un sous-ensemble de E, et un représentant de $\overline{x}$ en est un élément. Dans ce cas : $\overline{E} = E/\mathcal{R} := \{\mathrm{cl}(x) \mid x \in E\} \subset \mathcal{P}(E)$. Pour chacune de ces deux constructions, le lecteur vérifiera sans peine que l'application $\pi : E \to \overline{E}$ est surjective et que $\pi(x) = \pi(y) \Leftrightarrow x \sim y$. ∎

L'avantage de la première construction est que les symboles $\overline{x}$ désignent des objets « concrets ». L'avantage de la deuxième construction est qu'elle ne fait pas jouer un rôle privilégié à un élément particulier de $\mathrm{cl}(x)$, ceux-ci sont vraiment équivalents ! L'inconvénient (surtout psychologique) est que le symbole $\overline{x}$ peut être parfois vu comme désignant un *élément* de $\overline{E}$, parfois comme désignant un *sous-ensemble* de E.

Corollaire 2. Soient $a \in \overline{E}$ et $x \in \pi^{-1}(a)$ un représentant de a dans E. Alors l'ensemble $\pi^{-1}(a)$ de tous les représentants de a dans E est la classe d'équivalence $\mathrm{cl}(x)$.

Démonstration. Notons que x existe bien puisque π est surjective. De plus, on a les équivalences logiques : $y \in \pi^{-1}(a) \Leftrightarrow \pi(y) = a = \pi(x) \Leftrightarrow y \sim x$, de sorte que, par définition de la classe d'équivalence de x, $\pi^{-1}(a) = \{y \in E \mid y \sim x\} = \mathrm{cl}(x)$. ∎

Exemple. Pour la relation $\equiv_9$, on a $\overline{E} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\}$. Selon la première construction, on prend, par exemple, $\overline{n} := n \mod 9$ (reste de la division euclidienne) ; dans ce cas, $\overline{E} = [\![0, 8]\!]$ et $\overline{54321} = 6$. Selon la seconde construction, $\overline{n}$ est l'ensemble $\{n + 9k \mid k \in \mathbb{Z}\}$. Ainsi, $\overline{54321} = \overline{15} = \overline{6}$ est-il à la fois une sorte de nombre et une partie de $\mathbb{Z}$.

1.1.1 Passage au quotient d'une application

On reprend les notations précédentes E, $\mathcal{R}$, $\sim$ et $\pi : E \to \overline{E}$. Soit de plus $f : E \to F$ une application dont l'ensemble d'arrivée F est quelconque.

Théorème et définition 3 (Théorème de factorisation pour les applications).
Les assertions suivantes sont équivalentes :
(i) Deux éléments équivalents de E ont même image par f :

$$x \sim y \Rightarrow f(x) = f(y).$$

De manière équivalente, l'application f est constante sur chaque classe $\mathrm{cl}(x)$.
(ii) Il existe $\overline{f} : \overline{E} \to F$ telle que $\overline{f} \circ \pi = f$, c'est-à-dire : $\forall x \in E\ ,\ \overline{f}(\overline{x}) = f(x)$.
L'application $\overline{f}$ est alors unique. Nous dirons que la relation $\mathcal{R}$ est *compatible* avec l'application f, et que l'application $\overline{f}$ a été obtenue à partir de l'application f par *passage au quotient* par la relation $\mathcal{R}$.

Démonstration. S'il existe une application $\overline{f}$ satisfaisant (ii), on a les implications logiques : $x \sim y \Rightarrow \overline{x} = \overline{y} \Rightarrow f(x) = \overline{f}(\overline{x}) = \overline{f}(\overline{y}) = f(y)$.
Supposons réciproquement (i) vérifiée. On définit alors l'application $\overline{f}$ de la manière suivante. Pour tout $a \in \overline{E}$, on choisit un représentant arbitraire $x \in E$ de a et l'on est obligé (pour respecter la condition requise) de poser $\overline{f}(a) = f(x)$, ce qui entraîne d'ailleurs l'unicité de $\overline{f}$. Le point crucial est que *cette définition ne dépend pas du choix du représentant* : pour tout autre représentant y, on a $\overline{x} = a = \overline{y}$, donc $x \sim y$, donc $f(x) = f(y)$.
Par construction, on a alors bien $\forall x \in E\ ,\ \overline{f}(\overline{x}) = f(x)$, autrement dit, $\overline{f} \circ \pi = f$. ∎

Pratiquement, on procède comme suit : soit $a \in \overline{E}$. Pour définir $\overline{f}(a)$, on choisit tout d'abord un représentant arbitraire $x \in E$ de a et l'on pose $\overline{f}(a) := f(x) \in F$; dans un deuxième temps, *il faut vérifier que $f(x)$ ne dépend pas du représentant x choisi.*

Corollaire 4. On suppose E et F respectivement munis des relations d'équivalence $\mathcal{R}$ et $\mathcal{S}$, abrégées en $\sim$ et en $\equiv$. Soit $f : E \to F$ une application telle que deux éléments équivalents de E ont des images équivalentes : $x \sim y \Rightarrow f(x) \equiv f(y)$.
Il existe alors une unique application $\overline{f} : \overline{E} := E/\mathcal{R} \to \overline{F} := F/\mathcal{S}$ telle que :

$$\forall x \in E\ ,\ \overline{f}(\overline{x}) = \overline{f(x)}.$$

Démonstration. On applique le théorème à l'application $x \mapsto \overline{f(x)}$ de E dans $\overline{F}$. ∎

Exemple. Prenons $E = \mathbb{R}$ muni de la relation $\equiv_{2\pi}$ de congruence modulo 2π ; l'ensemble quotient est alors noté $\mathbb{R}/2\pi\mathbb{Z}$ (module sur les nombres complexes de [L1]).
La relation $\equiv_{2\pi}$ est compatible avec l'application $\theta \mapsto e^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$ de $\mathbb{R}$ dans $\mathbb{C}$, car les fonctions cosinus et sinus sont 2π-périodiques. On peut donc en déduire, par passage au quotient, une application $\overline{\theta} \mapsto e^{\mathrm{i}\theta}$ de $\mathbb{R}/2\pi\mathbb{Z}$ dans $\mathbb{C}$. En revanche, l'application $\theta \mapsto e^{\mathrm{i}\theta/2}$ ne passe pas au quotient et l'application $\overline{\theta} \mapsto e^{\mathrm{i}\theta/2}$ de $\mathbb{R}/2\pi\mathbb{Z}$ dans $\mathbb{C}$ *n'est pas définie* : on ne saurait en effet décider si $\overline{0} = \overline{2\pi}$ a pour image $e^{\mathrm{i}0/2} = 1$ ou $e^{\mathrm{i}2\pi/2} = -1$ (voir également l'exercice I.1.1 de la page 50).

Exercice 1.
Soit $f : E \to F$ une application. On définit sur E la relation $x \sim y \Leftrightarrow f(x) = f(y)$. Démontrer que c'est une relation d'équivalence compatible avec l'application f et que l'application $\overline{f} : \overline{E} \to F$ est injective. Elle induit donc une bijection de $\overline{E}$ sur $\operatorname{Im} f$.
Solution. On a vu dans [L1] que $\sim$ est une relation d'équivalence dont les classes d'équivalence sont exactement les ensembles de la forme $f^{-1}(y)$, où $y \in F$. Selon la deuxième construction de $\overline{E}$, on peut identifier l'élément $\overline{x}$ de $\overline{E}$ à $f^{-1}(y)$, où $y = f(x)$; on a alors $\overline{f}(\overline{x}) = y$. L'unique antécédent de y par $\overline{f}$ est donc la classe $\overline{x}$ de n'importe quel antécédent x de y par f.

1.2 Passage au quotient d'une loi de composition interne

On reprend les notations précédentes E, $\mathcal{R}$, $\sim$ et $\pi : E \to \overline{E}$. Soit de plus $\star$ une loi de composition interne sur E. On souhaite munir $\overline{E}$ d'une loi de composition interne $\diamond$ telle que π soit un morphisme, autrement dit : $\forall x, y \in E\ ,\ \overline{x} \diamond \overline{y} = \overline{x \star y}$. Pour que cela soit possible, il est évidemment *nécessaire* que $\overline{x \star y}$ ne change pas si l'on remplace x, y par x', y' tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$.

Définition 1. On dit que la relation $\sim$ est *compatible avec la loi* $\star$, ou encore que c'est une *congruence* si : $\forall x, y, x', y' \in E\ ,\ x \sim x'$ et $y \sim y' \Longrightarrow x \star y \sim x' \star y'$.

Il suffit en fait de vérifier séparément deux propriétés un peu plus faibles, la *compatibilité à gauche* : $y \sim y' \Rightarrow x \star y \sim x \star y'$, et la *compatibilité à droite* : $x \sim x' \Rightarrow x \star y \sim x' \star y$. En effet, des hypothèses $x \sim x'$ et $y \sim y'$, on peut alors déduire respectivement $x \star y \sim x' \star y$ et $x' \star y \sim x' \star y'$, d'où, par transitivité, $x \star y \sim x' \star y'$. Si la loi $\star$ est commutative, ces deux compatibilités partielles sont bien sûr équivalentes.

Proposition et définition 5. Si la relation $\sim$ est compatible avec la loi $\star$, l'ensemble quotient $\overline{E}$ peut être muni d'une unique loi de composition interne $\diamond$ telle que la projection canonique π est un morphisme de $(E, \star)$ dans $(\overline{E}, \diamond)$. La loi $\diamond$ est appelée *loi quotient* (de la loi $\star$ par la relation d'équivalence $\sim$).

Notons que la conclusion traduit l'équation $\overline{x} \diamond \overline{y} = \overline{x \star y}$.

Démonstration. Soient $a, b \in \overline{E}$ et soient $x, y \in E$ des représentants respectifs de a, b. Pour que π soit un morphisme, $\diamond$ doit être définie par la formule $a \diamond b = \overline{x \star y}$, d'où l'unicité de la loi $\diamond$. Il reste à voir que cette définition en est bien une, c'est-à-dire qu'elle ne dépend pas du choix des représentants. Si $a = \overline{x} = \overline{x'}$ et $b = \overline{y} = \overline{y'}$, on a $x \sim x'$ et $y \sim y'$, d'où, par hypothèse, $x \star y \sim x' \star y'$ et $\overline{x \star y} = \overline{x' \star y'}$. ∎

Exemple. La relation $\equiv_9$ est compatible avec l'addition et la multiplication dans $\mathbb{Z}$; on peut donc additionner et multiplier des classes. Par exemple, comme $\overline{4} = \overline{13}$ et $\overline{17} = \overline{-1}$,on peut indifféremment calculer $\overline{4}+\overline{17} = \overline{21}$ ou $\overline{13}+\overline{-1} = \overline{12}$ et obtenir le même résultat $\overline{21} = \overline{12}$.

Exercice 2.

Montrer que la relation $\equiv_{2\pi}$ est compatible avec l'addition dans $\mathbb{R}$. Donner un exemple d'addition de classes. Cette relation est-elle compatible avec la multiplication dans $\mathbb{R}$?

Solution. Soient x, x', y, y' des réels tels que $x' \equiv_{2\pi} x$ et $y' \equiv_{2\pi} y$. Il existe donc des entiers relatifs a, b tels que $x' - x = a \times 2\pi$ et $y' - y = b \times 2\pi$, d'où $(x' + y') - (x + y) = (a + b) \times 2\pi$, d'où $x' + y' \equiv_{2\pi} x + y$: la relation $\equiv_{2\pi}$ est bien compatible avec l'addition. On reconnaît dans $(\mathbb{R}/\equiv_{2\pi}, +)$ le groupe $\mathbb{R}/2\pi\mathbb{Z}$ rencontré dans l'étude des nombres complexes. Par exemple, comme $\overline{\pi} = \overline{-\pi}$ et $\overline{3\pi/2} = \overline{-\pi/2}$, on peut indifféremment calculer $\overline{\pi} + \overline{3\pi/2} = \overline{5\pi/2}$ ou $\overline{-\pi} + \overline{-\pi/2} = \overline{-3\pi/2}$ et obtenir le même résultat : $\overline{5\pi/2} = \overline{-3\pi/2}$.

Avec les notations ci-dessus, aucun calcul ne permet de conclure que $x'y' - xy$ est un multiple entier de 2π. De fait, si $x = y = 0$, $x' = a \times 2\pi$ et $y' = b \times 2\pi$, on a $x'y' - xy = (2\pi ab) \times 2\pi$ et $2\pi ab$ n'est en général pas un entier. La relation $\equiv_{2\pi}$ n'est donc pas compatible avec la multiplication. Ainsi, on ne saurait dire ce que vaut $\overline{\pi} \times \overline{3\pi/2}$ ou $\overline{-\pi} \times \overline{-\pi/2}$ car $\overline{3\pi^2/2}$ et $\overline{\pi^2/4}$ ne sont pas égaux.

PROPRIÉTÉS HÉRITÉES PAR LA LOI QUOTIENT. *Avec les mêmes notations, les propriétés qui suivent se déduisent de la surjectivité du morphisme* $\pi : (E, \star) \to (\overline{E}, \diamond)$ *:*

1. *Si* $\star$ *est commutative (resp. associative),* $\diamond$ *est commutative (resp. associative).*
2. *Si* e *est un élément neutre (resp. neutre à gauche, resp. neutre à droite, resp. absorbant) pour* $\star$*, alors* $\overline{e}$ *est un élément neutre (resp. neutre à gauche, resp. neutre à droite, resp. absorbant) pour* $\diamond$*.*
3. *Si* y *est inverse de* x *(resp. inverse à droite, resp. inverse à gauche) pour* $\star$*, alors* $\overline{y}$ *est inverse de* $\overline{x}$ *(resp. inverse à droite, resp. inverse à gauche) pour* $\diamond$*.*
4. *En particulier, si* $\star$ *est une loi de groupe, la loi quotient* $\diamond$ *est une loi de groupe.*
5. *Dans le cas d'une relation d'équivalence compatible avec deux lois* $\star$ *et* $\top$*, telle que* $\top$ *est distributive (resp. à gauche, resp. à droite) par rapport à* $\star$*, la loi quotient* $\overline{\top}$ *est distributive (resp. à gauche, resp. à droite) par rapport à* $\overline{\star}$*.*
6. *La régularité ne s'hérite pas :* exercice I.1.3 de la page 50.

Théorème 6 (Théorème de factorisation pour les morphismes).
Soit $\sim$ une relation d'équivalence sur E compatible avec la loi $\star$. Notons $\overline{E}$ et $\overline{\star}$ le quotient et la loi quotient et $\pi : E \to \overline{E}$ la projection canonique.
Soit par ailleurs $f : (E, \star) \to (F, \diamond)$ un morphisme. Pour que f soit compatible avec $\sim$, il faut, et il suffit, qu'il existe un morphisme $\overline{f} : (\overline{E}, \overline{\star}) \to (F, \diamond)$ tel que $f = \overline{f} \circ \pi$.
Le morphisme $\overline{f}$ est alors unique.

Démonstration. On applique la proposition 3 de la page 5, ce qui fournit l'application $\overline{f}$ (qui est unique). Il reste à voir que f est un morphisme si, et seulement si, $\overline{f}$ l'est.
Dans le sens direct, c'est évident (composé de deux morphismes). Réciproquement, si f est un morphisme, on a, avec des notations évidentes :

$$\overline{f}(\overline{x}\ \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Comme π est surjective, $\overline{x}$ et $\overline{y}$ sont arbitraires dans $\overline{E}$ et $\overline{f}$ est un morphisme. ∎

Théorème 7 (Théorème d'isomorphisme). (i) Soit $f : (E, \star) \to (F, \diamond)$ un morphisme. La relation $\sim$ sur E définie par $x \sim y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence compatible avec la loi $\star$. On notera $\overline{E}$ l'ensemble quotient, $\overline{\star}$ la loi induite et $\overline{f} : \overline{E} \to F$ l'application obtenue par passage au quotient.
(ii) Le sous-ensemble $F' = \operatorname{Im} f$ de F est stable pour la loi $\diamond$.
(iii) L'application $\overline{f}$ induit un isomorphisme de $(\overline{E}, \overline{\star})$ sur $(F', \diamond)$.

Démonstration. (i) D'après l'exercice 1 de la page 6, $\sim$ est une relation d'équivalence.
Si $x \sim y$ et $x' \sim y'$, alors $f(x) = f(y)$ et $f(x') = f(y')$, donc

$$f(x \star x') = f(x) \diamond f(x') = f(y) \diamond f(y') = f(y \star y'),$$

d'où $x \star x' \sim y \star y'$: on a bien la compatibilité.
(ii) Deux éléments quelconques de F' sont de la forme $f(x), f(y)$ et leur composé est $f(x) \diamond f(y) = f(x \star y) \in F'$: cet ensemble est bien un sous-ensemble stable.
(iii) Le morphisme $\overline{f} : \overline{E} \to F$ induit par corestriction un morphisme $\overline{f} : \overline{E} \to F'$, qui est bijectif d'après l'exercice 1 de la page 6. ∎

Exemple. L'application $t \mapsto e^{it}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$ et la relation $\sim$ associée est $\equiv_{2\pi}$. L'image est le cercle unité $\mathbb{U}$ et l'on obtient par passage au quotient un isomorphisme de $(\mathbb{R}/\equiv_{2\pi}, +) = \mathbb{R}/2\pi\mathbb{Z}$ sur $(\mathbb{U}, \times)$. D'après les propriétés d'héritage de la page précédente, il s'agit d'un isomorphisme de groupes.

1.2.1 Retour sur la construction de $\mathbb{Z}$

Soit M un ensemble non vide muni d'une loi de composition interne associative et commutative notée additivement, et disposant d'un élément neutre 0. On dit alors que $(M, +)$ est un *monoïde*

commutatif. Notons additivement la loi produit sur $M \times M$: $(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2)$. Ainsi $(M \times M, +)$ est un monoïde commutatif d'élément neutre $(0, 0)$. Définissons sur $M \times M$ une relation $\sim$ par : $(a, b) \sim (a', b') \Leftrightarrow \exists c \in M \ : \ a + b' + c = a' + b + c$. Par exemple, $(a, a) \sim (0, 0)$ pour tout a. On démontre alors que $\sim$ est une relation d'équivalence compatible avec l'addition de $M \times M$. Notons G l'ensemble quotient et $+$ la loi quotient ; alors $(G, +)$ est un groupe commutatif, dans lequel l'élément neutre est $\overline{(0, 0)}$ et l'opposé de la classe $\overline{(a, b)}$ est $\overline{(b, a)}$. L'application $i : a \mapsto \overline{(a, 0)}$ est un morphisme de $(M, +)$ dans $(G, +)$. Deux éléments $a, b \in M$ ont même image si, et seulement si, $\exists c \in M \ : \ a + c = b + c$. En particulier, si tous les éléments de M sont simplifiables, le morphisme i est injectif. Le groupe G est appelé *groupe des fractions du monoïde* M. Dans le cas du monoïde $(\mathbb{N}, +)$, on obtient ainsi le groupe $G = \mathbb{Z}$ et le morphisme injectif $\mathbb{N} \to \mathbb{Z}$ ([L1], module « Arithmétique »).

1.2.2 Retour sur la construction du corps des fractions

Soient A un anneau commutatif et S une partie *multiplicative* de A, autrement dit : S est stable pour la multiplication et $1 \in S$; ainsi, $(S, \times)$ est (en un sens évident) un sous-monoïde du monoïde commutatif $(A, \times)$. On suppose de plus que $0 \notin S$ (il en résulte d'ailleurs que S ne contient aucun élément nilpotent). On définit sur $A \times S$ deux lois de composition interne, notées additivement et multiplicativement : $(a_1, s_1)+(a_2, s_2) = (a_1 s_2+a_2 s_1, s_1 s_2)$ et $(a_1, s_1) \times (a_2, s_2) = (a_1 a_2, s_1 s_2)$. La deuxième loi est simplement la loi produit définie à partir des monoïdes commutatifs $(A, \times)$ et $(S, \times)$. La première loi, plus compliquée, est modelée sur le calcul des fractions. On définit également sur $A \times S$ une relation $\sim$ comme suit : $(a, s) \sim (a', s') \iff \exists t \in S \ : \ t(as' - a's) = 0$. On démontre alors que $\sim$ est une relation d'équivalence compatible avec les lois $+$ et $\times$ sur $A \times S$. Notons B l'ensemble quotient et $+$ et $\times$ les lois quotients. Alors $(B, +, \times)$ est un anneau commutatif dont les éléments neutres sont $\overline{(0, 1)}$ (pour l'addition) et $\overline{(1, 1)}$ (pour la multiplication). L'opposé de $\overline{(a, s)}$ est $\overline{(-a, s)}$. L'application $i : a \mapsto \overline{(a, 1)}$ est un morphisme d'anneaux de A dans B, de noyau : $\operatorname{Ker} i = \{a \in A \mid \exists s \in S \ : \ sa = 0\}$. Si S ne contient aucun diviseur de zéro dans A, en particulier si A est intègre, le morphisme i est injectif. L'anneau B est noté $S^{-1}A$ et l'on dit que c'est un *anneau de fractions de* A. L'image de $(a, s) \in A \times S$ dans $S^{-1}A$ est notée $s^{-1}a$ ou $\dfrac{a}{s}$. Lorsque A est intègre, en prenant $S = A \setminus \{0\}$, on reconnaît dans $S^{-1}A$ le corps des fractions de A ([L1], module « Groupes, anneaux, corps »).

1.3 Groupes quotients

1.3.1 Relations compatibles et sous-groupes distingués

Lemme 8. (i) Soient G un groupe et H un sous-groupe de G. Alors la relation $\sim$ définie par $a \sim b \Leftrightarrow a^{-1}b \in H$ (resp. $ab^{-1} \in H$) est une relation d'équivalence sur G compatible à gauche (resp. à droite) avec la loi interne ; la classe d'équivalence de $a \in G$ est sa *classe à gauche* aH (resp. sa *classe à droite* Ha).
(ii) Réciproquement, toutes les relations d'équivalence sur G compatibles à gauche (resp. à droite) avec la loi interne sont obtenues de cette manière.

Démonstration. (i) Nous ne traiterons que le cas des classes à gauche, l'autre côté étant entièrement similaire. De l'équivalence logique $a^{-1}b \in H \Leftrightarrow aH = bH$ (dont la preuve facile est laissée au lecteur), on déduit que $\sim$ est une relation d'équivalence et que la classe

d'équivalence de $a \in G$ est aH. De l'implication évidente $aH = bH \Rightarrow caH = cbH$, on déduit que $\sim$ est compatible à gauche avec la loi interne.
(ii) Soit $\sim$ une relation d'équivalence sur G compatible à gauche avec la loi interne. Soit H la classe de l'élément neutre e. Le sous-ensemble H contient e et l'on a les implications :

$$(a, b \in H) \Longrightarrow (a \sim e \text{ et } b \sim e) \Longrightarrow (a^{-1}b \sim a^{-1}e \sim a^{-1}a = e) \Longrightarrow (a^{-1}b \in H),$$

ce qui entraîne que H est un sous-groupe de G. On a maintenant les équivalences logiques :

$$a \sim b \Longleftrightarrow a^{-1}a \sim a^{-1}b \Longleftrightarrow a^{-1}b \in H,$$

ce qui achève la démonstration. ∎

Théorème et définition 9. Les propriétés suivantes sont équivalentes :
(i) Les relations d'équivalence sur G respectivement définies par $a^{-1}b \in H$ et par $ab^{-1} \in H$ coïncident.
(ii) Pour tout $a \in G$, la classe à gauche et la classe à droite coïncident : $aH = Ha$.
(iii) Le sous-groupe H est invariant par les *automorphismes intérieurs* $x \mapsto axa^{-1}$ ($a \in G$) : quel que soit $a \in G$, on a $aHa^{-1} = H$.
Le sous-groupe H de G est alors dit *distingué* dans G. On parle également de sous-groupe *invariant* ou de sous-groupe *normal*. On note alors : $H \lhd G$.

Démonstration. C'est immédiat en vertu du lemme 8 de la page précédente. ∎

Précisons le sens de la troisième propriété. Pour tout $a \in G$ fixé, l'application $x \mapsto axa^{-1}$ est un automorphisme de G ([L1], module « Groupes, anneaux, corps »); c'est ce que l'on appelle un automorphisme intérieur. Pratiquement, il suffit de vérifier que, pour tout $a \in G$, on a l'inclusion $aHa^{-1} \subset H$. En effet, l'inclusion correspondante pour a^{-1} s'écrit $a^{-1}Ha \subset H$, qui entraîne $H \subset aHa^{-1}$ et l'on obtient finalement l'égalité.
Les sous-groupes G et $\{e\}$ de G sont évidemment distingués. Si G est commutatif, tout automorphisme intérieur est égal à l'identité et tout sous-groupe est distingué.

Exercice 3.

Montrer que le centre Z du groupe G en est un sous-groupe distingué.
Solution. Rappelons ([L1]) que $Z = \{a \in G \mid \forall b \in G\ ,\ ab = ba\}$. Tout élément de Z est fixé par tout automorphisme intérieur, *a fortiori*, le sous-groupe Z est globalement invariant par tout automorphisme intérieur.

Proposition 10. Le noyau $\operatorname{Ker} f$ d'un morphisme de groupes $f : G \to G'$ est distingué. La relation associée est définie par $a \sim b \Leftrightarrow f(a) = f(b)$.

Démonstration.
Si $x \in \operatorname{Ker} f$, alors $f(x) = e'$ (neutre de G'), donc $f(axa^{-1}) = f(a)e'f(a)^{-1} = e'$, donc $axa^{-1} \in \operatorname{Ker} f$: c'est bien un sous-groupe distingué. De plus, on a les équivalences :

$$a^{-1}b \in \operatorname{Ker} f \Longleftrightarrow f(a^{-1}b) = e' \Longleftrightarrow f(a) = f(b).$$

∎

Corollaire 11. Soit $n \in \mathbb{N}^*$. Le groupe alterné $\mathfrak{A}_n$ est distingué dans le groupe symétrique $\mathfrak{S}_n$. Soit E un ensemble fini non vide. Le groupe alterné $\mathfrak{A}(E)$ est distingué dans le groupe symétrique $\mathfrak{S}(E)$.

Démonstration. C'est le noyau du morphisme signature. ∎

Définition 2. Soit $n \in \mathbb{N}^*$. On appelle *groupe spécial linéaire d'ordre* n, et l'on note $SL_n(K)$ le sous-groupe du groupe linéaire $GL_n(K)$ formé des matrices de déterminant 1. De même, si E est un K-espace vectoriel de dimension finie, on appelle *groupe spécial linéaire de* E, et l'on note $\mathcal{SL}(E)$ le sous-groupe du groupe linéaire $\mathcal{GL}(E)$ formé des automorphismes de déterminant 1.

Corollaire 12. Le groupe spécial linéaire $SL_n(K)$ est un sous-groupe distingué du groupe linéaire $GL_n(K)$. Le groupe spécial linéaire $\mathcal{SL}(E)$ est un sous-groupe distingué du groupe linéaire $\mathcal{GL}(E)$.

Démonstration. C'est, dans chaque cas, le noyau du morphisme déterminant. ∎

1.3.2 Quotient par un sous-groupe distingué

Théorème 13. (i) Soit $H \lhd G$ un sous-groupe distingué. Les égalités $a^{-1}b \in H$ et $ab^{-1} \in H$ définissent une même relation, notée $a \equiv b \pmod{H}$, qui est une relation d'équivalence sur G compatible (à gauche et à droite) avec la loi interne ; la classe d'équivalence de $a \in G$ est $aH = Ha$. Réciproquement, toutes les relations d'équivalence sur G compatibles (à gauche et à droite) avec la loi interne sont obtenues de cette manière à partir d'un sous-groupe distingué H.
(ii) La loi quotient fait de l'ensemble quotient $\overline{G}$ un groupe.
La projection canonique $\pi : G \to \overline{G}$ est un morphisme surjectif de noyau H.

Démonstration.
(i) C'est immédiat à partir du lemme 8 de la page 9 et du théorème 9 de la page ci-contre.
(ii) On sait déjà que la projection canonique est un morphisme surjectif, et, d'après les propriétés d'héritage de la de la page 7, $\overline{G}$ est un groupe. Le noyau de π est la classe de l'élément neutre, c'est-à-dire H. ∎

Définition 3. La relation $a \equiv b \pmod{H}$ est appelée *congruence modulo* H.
Le groupe $\overline{G}$ est appelé *groupe quotient de* G *par* H et noté G/H, ou, parfois $\dfrac{G}{H}$.

Théorème 14 (Théorème de factorisation pour les groupes).
Soient $H \lhd G$ un sous-groupe distingué et $\pi : G \to G/H$ la projection canonique.
Soit $f : G \to G'$ un morphisme de groupes.
Alors, pour que H soit inclus dans $\operatorname{Ker} f$, il faut, et il suffit, qu'il existe un morphisme de groupes : $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ \pi$.

Démonstration.
L'inclusion $H \subset \operatorname{Ker} f$ équivaut à l'implication $a^{-1}b \in H \Rightarrow f(a) = f(b)$, c'est-à-dire à la compatibilité de la congruence modulo H avec f : on peut donc appliquer le théorème 6 de la page 8. ∎

Théorème 15 (Premier théorème d'isomorphisme pour les groupes). Soit $f : G \to G'$ un morphisme de groupes. Soit $\pi : G \to G/\operatorname{Ker} f$ la projection canonique. Il existe alors un unique morphisme de groupes $\overline{f} : G/\operatorname{Ker} f \to G'$ tel que $f = \overline{f} \circ \pi$. Ce morphisme est injectif et induit par corestriction un isomorphisme $\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$.

Démonstration. On peut, au choix, appliquer le théorème 7 de la page 8 au cas des groupes ou bien appliquer le théorème 14 de la page précédente au cas de $H = \operatorname{Ker} f$. ∎

Proposition 16. Soient $H \lhd G$ et $\pi : G \to G/H$ la projection canonique. On définit une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H de la manière suivante : à tout sous-groupe G' de G contenant H, on associe son image $\pi(G') \subset G/H$; à tout sous-groupe K de G/H, on associe son image réciproque $G' = \pi^{-1}(K) \subset G$. Avec ces notations, on a alors : $\overline{G'} := \pi(G') = G'/H$.

Démonstration. L'inclusion $G' \subset \pi^{-1}\big(\pi(G')\big)$ est vraie pour toute partie G' de G. Pour un sous-groupe G' contenant H, on montre l'inclusion réciproque : si $x \in \pi^{-1}\big(\pi(G')\big)$, alors $\pi(x) \in \pi(G')$, donc $\pi(x) = \pi(g)$ avec $g \in G'$; alors $x^{-1}g \in \operatorname{Ker}\pi = H \subset G'$, d'où $x^{-1}g \in G'$, d'où $x \in G'$ (car $g \in G'$). On a donc $\pi^{-1}\big(\pi(G')\big) \subset G'$, d'où $G' = \pi^{-1}\big(\pi(G')\big)$. Puisque π est surjective, l'égalité $F = \pi\big(\pi^{-1}(F)\big)$ est vraie pour toute partie F de G/H. Pour tout sous-groupe G' de G contenant H, $F := \pi(G')$ est un sous-groupe de G/H. Pour tout sous-groupe F de G/H, $G' := \pi^{-1}(F)$ est un sous-groupe de G contenant $\pi^{-1}(e) = H$.
Ainsi, les applications $F \mapsto \pi^{-1}(F)$ et $G' \mapsto \pi(G')$ sont des bijections réciproques l'une de l'autre entre les sous-groupes de G/H et les sous-groupes de G contenant H. La restriction-corestriction de π à $G' \to \overline{G'}$ est surjective de noyau H, donc (théorème 15) induit un isomorphisme $G'/H \simeq \overline{G'}$ qui permet l'identification. ∎

Théorème 17 (Deuxième théorème d'isomorphisme pour les groupes). La correspondance de la proposition 16 induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de G/H.
Si $G' \lhd G$, G' contenant H, on a de plus un isomorphisme : $\dfrac{G/H}{G'/H} \simeq \dfrac{G}{G'}$.

Démonstration. Si G' est distingué, l'égalité $aG'a^{-1} = G'$ donne, par application du morphisme π, l'égalité $bFb^{-1} = F$, où $F := \pi(G')$ et où $b := \overline{a}$ est un élément quel-

conque de G/H (puisque π est surjective); F est donc distingué. Si $F = G'/H$ est distingué dans $\overline{G} = G/H$, le morphisme composé $G \to \overline{G} = G/H \to \overline{G}/F$ est surjectif de noyau G', qui est donc distingué; on applique alors le premier théorème d'isomorphisme. ∎

Exercice 4.
Quels sont les sous-groupes de $GL_n(K)$ (resp. de $\mathfrak{S}_n$) contenant $SL_n(K)$ (resp. $\mathfrak{A}_n$)?
Solution. Les premiers sont en bijection avec les sous-groupes de $GL_n(K)/SL_n(K)$. Or, $SL_n(K)$ est le noyau du morphisme surjectif $\det : GL_n(K) \to K^*$. Pour tout sous-groupe F de K^*, on définit donc un sous-groupe $G' := \det^{-1}(F)$, et tous les sous-groupes de $GL_n(K)$ contenant $SL_n(K)$ s'obtiennent de cette façon. Comme K^* est commutatif, ils sont distingués. Un argument analogue s'applique à la seconde question, avec la signature ε à la place du déterminant. Comme $\operatorname{Im}\varepsilon = \{+1, -1\}$ n'admet comme sous-groupes que $\{+1\}$ et lui-même, les seuls sous-groupes de $\mathfrak{S}_n$ contenant $\mathfrak{A}_n$ sont $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

1.3.3 Le cas d'un groupe commutatif

Dans le cas d'un groupe commutatif G, tout sous-groupe H est distingué et l'on peut former le quotient G/H, qui est commutatif d'après les propriétés d'héritage de la de la page 7. Pratiquement tous les quotients que nous rencontrerons cette année sont de ce type : cela concerne en particulier les anneaux et les espaces vectoriels (sections suivantes). Décrivons rapidement le mode d'emploi d'un tel quotient; on suppose que les groupes sont notés additivement. Lorsque l'on veut additionner deux éléments quelconques a et b de G/H, on en choisit des *représentants*, c'est à dire des éléments x et y dans G tels que $a = \overline{x}$ et $b = \overline{y}$. On a alors $a+b = \overline{x+y}$. Cette somme ne dépend pas du choix des représentants x, y. Nous avons déjà rencontré deux exemples de tels calculs : le calcul des congruences modulo n (il correspond au cas du sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$; le théorème 18 l'explicite); et le calcul des congruences modulo 2π, pour les arguments de nombres complexes (il correspond au cas du sous-groupe $2\pi\mathbb{Z}$ de $\mathbb{R}$, le groupe quotient étant $\mathbb{R}/2\pi\mathbb{Z}$).

Théorème 18. (i) Soit $n \in \mathbb{N}^*$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les groupes $d\mathbb{Z}/n\mathbb{Z}$, où $d \in \mathbb{N}^*$ est un diviseur de n. Le quotient de $\mathbb{Z}/n\mathbb{Z}$ par $d\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Le nombre de ces sous groupes est donc le nombre de diviseurs de n dans $\mathbb{N}^*$.
(ii) Soit G un groupe cyclique d'ordre n. Pour tout diviseur d de n, G admet un unique sous-groupe H d'ordre d, celui-ci est cyclique ainsi que le quotient G/H. Tous les sous-groupes de G s'obtiennent ainsi. Dans le cas où G est le groupe μ_n des racines $n^{\text{èmes}}$ de l'unité dans $\mathbb{C}$, le sous-groupe d'ordre d est μ_d.

Démonstration. (i) Puisque tous les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $m\mathbb{Z}/n\mathbb{Z}$, où m est un diviseur de n (proposition 16 de la page 12). Selon le théorème 17 de la page précédente, le quotient de $\mathbb{Z}/n\mathbb{Z}$ par $m\mathbb{Z}/n\mathbb{Z}$ s'identifie à $\mathbb{Z}/m\mathbb{Z}$. L'assertion (ii) est alors immédiate. ∎

1.4 Anneaux quotients

Nous ne considérerons que des anneaux commutatifs.

Théorème 19. (i) Soit I un idéal de l'anneau commutatif A. La congruence modulo le sous-groupe I est compatible avec la multiplication de A. Soit réciproquement $\sim$ une relation d'équivalence sur A compatible avec l'addition et la multiplication. Alors la classe de 0 est un idéal I et $\sim$ est la congruence modulo I.
(ii) La loi quotient de la multiplication de I fait alors du groupe quotient $(A/I, +)$ un anneau commutatif. La projection canonique $\pi : A \to A/I$ est un morphisme surjectif d'anneaux, de noyau I.

On dit que l'image $\overline{a} := \pi(a) \in A/I$ s'obtient par *réduction modulo* I de $a \in A$.
Démonstration. Presque tout cet énoncé fait partie du théorème 13 de la page 11.
(i) Notons $\sim$ la congruence modulo l'idéal I. Alors, si $a \sim b$ et si c est quelconque, $a-b \in I \Rightarrow c(a-b) \in I$ (car I est un idéal), donc $ca \sim cb$, ce qui suffit par commutativité. Si $\sim$ est une relation d'équivalence sur A compatible avec l'addition et la multiplication, on sait déjà que la classe I de 0 est un sous-groupe et que $\sim$ est la congruence modulo I. Reste à voir que c'est un idéal. Si $a \in I$ et $c \in A$, alors $a \sim 0 \Rightarrow ca \sim c0 \Rightarrow ca \in I$.
(ii) Les propriétés d'héritage de la de la page 7 entraînent que $(A/I, +, \times)$ est un anneau commutatif, et il est immédiat que π est un morphisme surjectif d'anneaux, de noyau I. ∎

Exemples. Si l'idéal est trivial : $I = 0$ (notation abusive abrégée pour $I := \{0\}$), alors $A/I = A$. Si $I = A$, le quotient est l'anneau trivial 0 (notation abusive abrégée pour $\{0\}$). Si $A = \mathbb{Z}$ et $I = n\mathbb{Z}$ ($n \in \mathbb{N}^*$), le quotient est l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exercice 5.
Décrire tous les anneaux quotients de l'anneau $\mathbb{Z}$ et ceux de l'anneau $K[X]$.
Solution. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$. Les anneaux quotients de $\mathbb{Z}$ sont donc les anneaux de classes de congruence $\mathbb{Z}/n\mathbb{Z}$ (donc $\mathbb{Z}$ si $n = 0$).
De même, les idéaux de $K[X]$ sont tous principaux et de la forme $<P>$, où P est soit 0 soit un polynôme unitaire. Si $P = 0$, l'idéal est nul et le quotient est $K[X]$. Si $P = 1$, l'idéal est $K[X]$ et le quotient est trivial. Supposons que P est de degré n. De la division euclidienne, on déduit que tout polynôme de $K[X]$ est congru modulo P à un unique polynôme de $K_{n-1}[X]$. Comme on le verra à la section 1.5, de la décomposition $K[X] = <P> \oplus K_{n-1}[X]$ ([L1], module sur les polynômes), on peut déduire l'isomorphisme des *espaces vectoriels*, donc des *groupes* $K[X]/<P>$ et $K_{n-1}[X]$ (proposition 28 de la page 17). Cependant, la multiplication dans $K_{n-1}[X]$ doit alors s'effectuer modulo P : pour multiplier A et B selon la loi quotient, on calcule AB puis on prend le reste $AB \mod P$. Ce type de calcul est illustré dans l'exercice 6 de la page suivante.

Théorème 20 (Théorème de factorisation pour les anneaux). Soient I un idéal de A et $\pi : A \to A/I$ la projection canonique. Soit $f : A \to A'$ un morphisme d'anneaux. Alors, pour que I soit inclus dans $\mathrm{Ker}\, f$, il faut, et il suffit, qu'il existe un morphisme d'anneaux : $\overline{f} : A/I \to A'$ tel que $f = \overline{f} \circ \pi$.

Démonstration. On invoque le théorème 14 de la page 11 ; il ne reste qu'à vérifier que $\overline{f}$ est bien un morphisme pour la multiplication, ce qui est facile.

Exemple. L'application $P \mapsto P(\mathrm{i})$ de $\mathbb{R}[X]$ dans $\mathbb{C}$ est un morphisme surjectif d'anneaux. Son noyau contient l'idéal $<X^2+1>$. D'après le théorème, on a donc par passage au quotient un morphisme surjectif d'anneaux $\mathbb{R}[X]/<X^2+1> \to \mathbb{C}$ (voir également l'exercice 6 ci-dessous).

Corollaire 21. Soit $f : A \to B$ un morphisme d'anneaux et soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A et l'on a un morphisme injectif : $A/f^{-1}(J) \to B/J$. En particulier, si $A \subset B$ est un sous-anneau et J un idéal de B, alors $A \cap J$ est un idéal de A et l'on a un morphisme injectif : $A/(A \cap J) \to B/J$.

Démonstration. Le noyau du morphisme composé $A \to B \to B/J$ est l'idéal $f^{-1}(J)$. Si $A \subset B$ et si f est l'inclusion de A dans B, $f^{-1}(J) = A \cap J$.

Théorème 22 (Premier théorème d'isomorphisme pour les anneaux). Soient $f : A \to A'$ un morphisme d'anneaux et $\pi : A \to A/\operatorname{Ker} f$ la projection canonique. Il existe alors un unique morphisme d'anneaux $\overline{f} : A/\operatorname{Ker} f \to A'$ tel que $f = \overline{f} \circ \pi$. Ce morphisme est injectif et induit un isomorphisme de $A/\operatorname{Ker} f$ sur $\operatorname{Im} f$.

Démonstration. On invoque le théorème 15 de la page 12 ; il ne reste qu'à vérifier que $\overline{f}$ est bien un morphisme pour la multiplication, ce qui est facile.

Exercice 6.

Appliquer ce qui précède au morphisme $P \mapsto P(\mathrm{i})$ de $\mathbb{R}[X]$ dans $\mathbb{C}$ et à l'image de $\mathbb{Q}[X]$.

Solution. De la division euclidienne $P = (X^2+1)Q + (a+bX)$, on déduit les équivalences $P(\mathrm{i}) = 0 \Leftrightarrow a + b\mathrm{i} = 0 \Leftrightarrow a = b = 0$. Le noyau est donc l'idéal $<X^2+1>$, d'où un isomorphisme $\mathbb{R}[X]/<X^2+1> \simeq \mathbb{C}$. On peut donc décrire $\mathbb{C}$ comme le groupe $\mathbb{R}_1[X] = \mathbb{R} + \mathbb{R}X$, muni de la multiplication pour laquelle le produit de $a+bX$ et de $c+dX$ est le reste de la division de $(a+bX)(c+dX)$ modulo X^2+1. On vérifie sans peine que ce reste vaut $(ac-bd)+(ad+bc)X$. C'est donc la classe de X modulo X^2+1 qui joue le rôle de i. L'image de $\mathbb{Q}[X]$ est évidemment $\mathbb{Q}[\mathrm{i}]$.

En prenant, dans le corollaire 21, $A := \mathbb{Q}[X]$, $B := \mathbb{R}[X]$ et $J := (X^2+1)\mathbb{R}[X]$, on trouve $A \cap J = (X^2+1)\mathbb{Q}[X]$ (pourquoi ?) et un morphisme injectif

$$\mathbb{Q}[X]/<X^2+1> \to \mathbb{R}[X]/<X^2+1>,$$

qui s'identifie à l'inclusion $\mathbb{Q}[\mathrm{i}] \subset \mathbb{C}$.

Théorème 23 (Deuxième théorème d'isomorphisme pour les anneaux). Soient A un anneau, I un idéal de A et $\pi : A \to A/I$ la projection canonique. La correspondance du théorème 17 de la page 12 établit une bijection entre les idéaux de A contenant I et les idéaux de A/I. Si $J \subset A$ est un idéal contenant I et si $\pi(J) = J/I$ est l'idéal de A/I qui lui correspond, on a un isomorphisme d'anneaux : $\dfrac{A/I}{J/I} \simeq \dfrac{A}{J}$.

Démonstration. Il suffit de vérifier que les constructions correspondantes pour les sous-groupes distingués sont bien compatibles avec la multiplication, ce qui est facile. ∎

Exercice 7.
Décrire les idéaux et les anneaux quotients de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (où $n \in \mathbb{N}$). On détaillera le cas particulier $n := 6$. Décrire de même les idéaux et les anneaux quotients de l'anneau $A := K[X]/<P>$ (où $P \in K[X]$ est un polynôme unitaire de degré $n \in \mathbb{N}^*$). On détaillera le cas $n := 2$ (en admettant que la caractéristique de K n'est pas 2).

Solution. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $m\mathbb{Z}/n\mathbb{Z}$, où m divise n, et les quotients correspondants sont les anneaux $\mathbb{Z}/m\mathbb{Z}$. Par exemple, les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont tous ses sous-groupes : $1\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$, $3\mathbb{Z}/6\mathbb{Z}$ et $6\mathbb{Z}/6\mathbb{Z} = \{0\}$; et les anneaux quotients correspondants sont les anneaux $\mathbb{Z}/1\mathbb{Z} = \{0\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

Les idéaux de A sont les $<Q>/<P>$, où Q est un polynôme unitaire qui divise P, et les quotients correspondants sont les $K[X]/<Q>$. Si $P = X^2 + pX + q$, les diviseurs $Q = 1$ et $Q = P$ donnent respectivement les idéaux $K[X]/<P> = A$ et $<P>/<P> = 0$, et les quotients correspondants sont 0 et A. Pour d'éventuels autres idéaux et quotients, une discussion est nécessaire :

1. Si $\Delta := p^2 - 4q$ n'est pas un carré dans K, le polynôme P est irréductible et A n'admet pas d'autre idéal que 0 et lui-même. Nous verrons plus loin qu'en fait, A est un corps (exemple de la page 20).
2. Si $\Delta = 0$, P admet pour seul diviseur unitaire non trivial $X + p/2$, et A admet un seul idéal autre que 0 et lui-même.
3. Si Δ est un carré non nul, $P = (X - a)(X - b)$ avec $a \neq b$ et l'anneau A admet deux idéaux et deux quotients non triviaux. De plus, comme aucun des deux facteurs de P ne divise l'autre, ces deux idéaux ne sont pas contenus l'un dans l'autre. Nous verrons plus loin que A est le produit de deux corps (exercice I.1.25 de la page 53).

1.5 Espaces vectoriels quotients

Théorème et définition 24. Soit W un sous–espace vectoriel d'un K-espace vectoriel V. Le groupe V/W admet une unique structure d'espace vectoriel telle que l'application $\pi : V \to V/W$ soit linéaire. On définit ainsi *l'espace vectoriel quotient* V/W et la *projection canonique* π.

Démonstration. Puisque l'on veut avoir $\forall x \in V\ ,\ \pi(\lambda x) = \lambda\pi(x)$, on doit définir la loi externe sur V/W en posant $\lambda a := \overline{\lambda x}$, où $x \in V$ est un représentant de a. D'après les