Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg

Gabor Wiese[1]
gabor.wiese@uni.lu

Version du 14 janvier 2016

[1]Je remercie Agnès David pour sa collaboration à une version antérieure.

Table des matières

Préface

L'algèbre, qu'est-ce que c'est ? Historiquement, on entend par « algèbre » l'étude des équations polynomiales. Au cours des 2000 ans de cette étude, les gens se sont aperçus que certaines structures revenaient très souvent, et de plus, dans des contextes tout à fait différents ! Depuis, les algébristes s'occupent aussi de l'étude et du développement de ces structures, ainsi que, évidemment, de leurs applications dans d'autres domaines en sciences, ingénierie et mathématiques. Le cours *Algèbre 1* sera consacré à une introduction aux structures algébriques fondamentales : les groupes, les anneaux, les corps, ainsi qu'aux espaces vectoriels (d'un point de vue plus général que dans le cours d'algèbre linéaire). Ces structures seront illustrées par des exemples et, parfois, des applications. Les règles et les méthodes les plus importantes concernant les démonstrations mathématiques seront enseignées et pratiquées.
En *Algèbre 2*, nous approfondirons la théorie des anneaux et traiterons quelques compléments au cours d'algèbre linéaire. En *Algèbre 3*, nous traiterons la théorie des corps. Le cours culminera au quatrième semestre par la *Théorie de Galois*, qui nous permettra de démontrer la constructibilité ou inconstructibilité à la règle et au compas de certains problèmes de l'Antiquité et l'impossibilité de résoudre l'équation générale de degré au moins 5 par radicaux.

Littérature

Pour le début, qui est sans doute la partie la plus difficile, je recommande les livres suivants qui devraient être disponibles dans la bibliothèque au Kirchberg.

- Schichl, Steinbauer : *Einführung in das mathematische Arbeiten*.
- Scharlau : *Schulwissen Mathematik : Ein Überblick*, Vieweg, 3rd ed., 2001.
- Cramer : *Vorkurs Mathematik : Arbeitsbuch zum Studienbeginn in Bachelor-Studiengängen*, Springer, 2012.
- Fritzsche : *Mathematik für Einsteiger Spektrum*.

Voici quelques références : ces livres devraient également être disponibles dans la bibliothèque au Kirchberg.

- Lelong-Ferrand, Arnaudiès : *Cours de mathématiques, Tome 1, Algèbre*. Dunod. Ce livre est très complet et très détaillé. On peut l'utiliser comme ouvrage de référence.
- Siegfried Bosch : *Algebra* (en allemand), Springer-Verlag. Ce livre est très complet et bien lisible.
- Serge Lang : *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre ; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.
- Siegfried Bosch : *Lineare Algebra*, Springer-Verlag.
- Jens Carsten Jantzen, Joachim Schwermer : *Algebra*.

- Christian Karpfinger, Kurt Meyberg : *Algebra : Gruppen - Ringe - Körper*, Spektrum Akademischer Verlag.
- Gerd Fischer : *Lehrbuch der Algebra : Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern*, Vieweg+Teubner Verlag.
- Gerd Fischer : *Lineare Algebra : Eine Einführung für Studienanfänger*, Vieweg+Teubner Verlag.
- Gerd Fischer, Florian Quiring : *Lernbuch Lineare Algebra und Analytische Geometrie : Das Wichtigste ausführlich für das Lehramts- und Bachelorstudium*, Springer Vieweg.
- Perrin : *Cours d'algèbre*, Ellipses.
- Guin, Hausberger : *Algèbre I. Groupes, corps et théorie de Galois*, EDP Sciences.
- Fresnel : *Algèbre des matrices*, Hermann.
- Tauvel : *Algèbre*.
- Combes : *Algèbre et géométrie*.
- Godement : *Cours d'algèbre*.

Chapitre I

Introduction aux mathématiques à l'université

1 Les démonstrations et les premiers mots du langage mathématique

Objectifs de cette section :

- Comprendre le concept de démonstration ;
- comprendre les concepts de définition, lemme, proposition, théorème ;
- faire connaissance avec des exemples de démonstrations directes et indirectes ;
- faire connaissance avec des exemples de définitions, lemmes, propositions, théorèmes ;
- maîtriser la manipulation d'équations simples ;
- maîtriser l'utilisation des indices, des sommes et des produits ;
- maîtriser les démonstrations par récurrence.

Une grande partie du contenu de cette section a déjà été traitée dans le cours de M. Schlenker pendant la semaine préparatoire. On donnera donc parfois moins de détails au cours.

Quelques mots au début – Aller Anfang ist schwer... und leicht

Le début des études de mathématiques est (comme Schichl et Steinbauer l'écrivent dans *Einführung in das mathematische Arbeiten*)

- **très difficile**, du fait de l'abstraction (définition, proposition, démonstration) et de l'utilisation d'un langage particulier, le langage mathématique,
- **facile**, car une grande partie des sujets a déjà été traitée au lycée.

Les mathématiques à l'université sont caractérisées par la **certitude absolue** de leurs résultats. Il ne suffit plus – comme souvent au lycée – d'expliquer un phénomème par beaucoup d'exemples ou d'apprendre une technique de calcul ; à l'université, il s'agit de le **démontrer**, c'est-à-dire d'écrire une **démonstration** (aussi appelée une **preuve**) qui, par une chaîne d'arguments faciles à suivre et compréhensibles pour tous, ne laisse aucun doute sur la vérité d'une assertion.
Pour pouvoir dire qu'une assertion est vraie avec une certitude absolue, il faut que tous les mots qui sont utilisés aient une signification très précise qui est la même pour tous. Par exemple, la phrase « La maison est haute » a certainement une signification différente pour quelqu'un de New York et pour quelqu'un venant d'un petit village en Sibérie.
Le langage mathématique diffère du langage du quotidien par :

- sa **précision**, tout terme a une définition précise ;
- son **formalisme**, souvent, on utilise des symboles et des formules.

Ce cours d'algèbre commencera donc par des exemples de preuves et l'introduction du langage mathématique.
On vous conseille fortement de vous **procurer des livres** (dans la bibliothèque sur support papier ou dans les répertoires électroniques) :

- spécialisés pour le grand pas entre l'école et l'université (comme Schichl/Steinbauer : *Einführung in das mathematische Arbeiten*) ;
- d'introduction à l'algèbre et à l'algèbre linéaire.

Un mot d'explication sur « l'algèbre » et « l'algèbre linéaire » : à l'Université du Luxembourg, ces deux cours sont enseignés au premier semestre, tandis qu'en France et en Allemagne, les cours d'algèbre ne commencent qu'en deuxième année et reposent sur les cours d'algèbre linéaire. Ne soyez pas choqués par ce fait (mais gardez-le à l'esprit quand vous regardez des livres – il vous faut aussi des livres sur l'algèbre linéaire). Le cours d'algèbre linéaire à l'UL est en commun avec d'autres filières du Bachelor et le cours d'algèbre est destiné uniquement aux étudiants en mathématiques. En cours d'algèbre, nous allons faire une grande partie de ce qui se fait habituellement dans les cours d'algèbre linéaire dans d'autres pays, sauf que vous allez très bien vous entraîner aux calculs importants de matrices dans votre cours d'algèbre linéaire ; cela nous permettra d'aller un tout petit peu plus loin que l'algèbre linéaire dans notre cours.

Définition, proposition, démonstration

On utilise les notations suivantes (connues de l'école) :

- $\mathbb{N}$, les entiers naturels : $0, 1, 2, 3, \ldots$;
- $\mathbb{Z}$, les entiers relatifs : $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$;
- $\mathbb{Q}$, les nombres rationnels ;
- $\mathbb{R}$, les nombres réels ;

- $\mathbb{C}$, les nombres complexes.

On rappelle la notion de *divisibilité* dans les entiers relatifs. On dit qu'un entier relatif $q \neq 0$ divise un entier relatif n (et que q est un diviseur de n) si le reste de la division de n par q est zéro, ou, dit autrement, s'il existe un entier relatif m tel que $n = mq$.
En fait, les phrases précédentes signifient que nous avons donné un nom (« diviseur ») à une propriété mathématique. C'est un exemple de **définition**. Pour souligner le rôle essentiel des définitions en mathématiques, nous les formulons comme suit.

Définition 1.1. *Soient $n, q \in \mathbb{Z}$.*
On dit que q est un diviseur *de n et que q* divise *n s'il existe $m \in \mathbb{Z}$ tel que*

$$n = mq.$$

On utilise le symbole $q \mid n$ pour signifier que q divise n.

Définition 1.2. *Soit $n \in \mathbb{Z}$. On dit que n est* pair *si 2 divise n (en symboles : $2 \mid n$).*

Une définition n'est pas vraie ou fausse. C'est seulement un nom qu'on donne à une propriété pour pouvoir mieux l'utiliser. Mais les définitions sont d'une importance fondamentale pour les mathématiques parce qu'elles « définissent » les objets avec lesquels nous allons travailler, donc sur lesquels nos propositions vont porter.

Proposition 1.3. *Le carré d'un nombre pair est pair.*

Vocabulaire :

- Une **proposition** est une assertion qui est vraie avec une certitude absolue, c'est-à-dire qui a été démontrée.
- Un **théorème** est un autre mot pour une assertion qui est vraie avec une certitude absolue. On utilise habituellement le mot « théorème » pour les assertions les plus importantes.
- Un **lemme** est encore un autre mot pour une assertion qui est vraie avec une certitude absolue. Les lemmes ont souvent une fonction secondaire et auxiliaire ; on les utilise pour démontrer des propositions ou des théorèmes.
- Un **corollaire** est encore un autre mot pour désigner une assertion. On l'utilise pour des énoncés qui se déduisent facilement d'un autre résultat, en général une proposition ou un théorème. Le contenu d'un corollaire peut être très important, mais sa démonstration à partir de la proposition ou du théorème initial est rapide.

Démonstration de la proposition 1.3. Soit $n \in \mathbb{Z}$ pair. D'après les définitions précédentes, cela veut dire qu'il existe $m \in \mathbb{Z}$ tel que

$$n = 2m.$$

Cela implique que

$$n^2 = (2m)^2 = 4m^2.$$

Donc

$$n^2 = 2 \cdot (2m^2).$$

Alors, n^2 est divisible par 2, donc pair. □

Cette démonstration est la première dans ce cours. On voit que c'est une suite d'arguments, et chaque étape est facile à vérifier pour tous. Donc, on peut en effet dire que la proposition est vraie avec une certitude absolue.
Cette preuve est un exemple d'une **démonstration directe** : nous avons commencé par **l'hypothèse** (n est un entier relatif pair) et nous avons terminé par l'assertion recherchée.
Il est habituel de signaler la fin d'une preuve par un symbole spécial ou par une abbréviation standard. La fin des preuves dans ces notes sera toujours marquée par le symbole □. D'autres professeurs utilisent d'autres symboles. Une abbréviation très courante est « q.e.d. » (quod erat demonstrandum – ce qui a été à démontrer).

Voici une autre définition.

Définition 1.4. *Un entier relatif $p \in \mathbb{Z}$ est appelé* nombre premier *si $p > 1$ et les seuls diviseurs positifs de p sont 1 et p.*

Nous avons donné cette définition et maintenant nous voulons en savoir autant que possible sur cette nouvelle notion que nous avons définie. Pour commencer, les nombres premiers inférieurs à 20 sont : 2, 3, 5, 7, 11, 13, 17, 19. Vous connaissez certainement d'autres nombres premiers. Une question vient donc immédiatement à l'esprit : existe-t-il une infinité de nombres premiers ?
La réponse a déjà été donnée par Euclide il y a plus de 2200 ans.

Théorème 1.5 (Euclide)**.** *Il existe une infinité de nombres premiers.*

La démonstration donnée par Euclide est souvent considérée comme l'exemple d'une preuve belle et élégante. C'est une **démonstration indirecte** ou, plus précisement, **démonstration par l'absurde**. On donne d'abord la démonstration et on expliquera ces termes juste après.

Démonstration. Supposons pour l'instant le contraire de ce que nous voulons démontrer : il n'existe qu'un nombre fini (disons n) de nombres premiers. On peut alors les numéroter :

$$p_1, p_2, p_3, \ldots, p_n.$$

Considérons l'entier positif

$$m := p_1 p_2 p_3 \cdots p_n + 1. \tag{1.1}$$

Nous allons maintenant utiliser le fait que tout entier positif ≥ 2 s'écrit comme produit de nombres premiers. Cette assertion doit être démontrée ! Nous le faisons dans le lemme 1.6 qui suit.
Il existe alors un nombre premier p qui divise m. Le nombre premier p doit appartenir à notre liste complète des nombres premiers, donc $p = p_i$ pour un certain i entre 1 et n.
L'équation (1.1) montre que la division de m par p_i laisse le reste 1.
Nous avons trouvé qu'en même temps p_i divise m et laisse le reste 1. Ceci est **absurde**, c'est une **contradiction**.
Donc, notre hypothèse faite au début de cette preuve ne peut pas être vraie. Alors, son contraire est vrai : il existe une infinité de nombres premiers. □

Le principe de cette preuve indirecte est de supposer vrai le contraire de l'assertion recherchée. Puis, on donne une suite d'arguments, comme avant, pour arriver à une assertion, dont on sait qu'elle est fausse, **absurde** et **contradictoire** (dans notre preuve : le reste de la division de m par p est à la fois 0 et 1). Nous savons alors que le contraire de l'assertion recherchée est faux. Cela signifie que l'assertion est vraie, car une assertion est soit vraie soit fausse. Ce fait est souvent écrit en latin « Tertium non datur » et s'appelle en français « Principe du tiers exclu ». On en reparlera plus tard.

Lemme 1.6. *Soit $n \geq 2$ un entier relatif. Alors il existe des nombres premiers $p_1, \ldots, p_k$ tels que*

$$n = p_1 p_2 \cdots p_k.$$

Remarquons que dans l'énoncé du lemme, les nombres premiers ne sont pas nécessairement distincts. Remarquons également que, pour être encore plus précis, on aurait du écrire : « Alors il existe un entier $k \geq 1$ et il existe des nombres premiers $p_1, \ldots, p_k$ tels que $n = p_1 p_2 \cdots p_k$ ». Il est habituel de formuler l'enoncé comme nous l'avons fait, mais il faut toujours être conscient que l'existence de k est implicite.
La preuve de ce lemme est un autre exemple d'une démonstration par l'absurde.

Démonstration (par l'absurde). Supposons que l'énoncé du lemme est faux. Dans ce cas, il existe un entier positif ≥ 2 qui ne s'écrit pas comme un produit de nombres premiers. Soit n le plus petit entier ayant cette propriété.
Nous distinguons des cas.
1er cas : n est premier. Dans ce cas, on prend $k = 1$ et $p_1 = n$, donc on a $n = p_1$.
2ème cas : n n'est pas un nombre premier. Alors, n possède un diviseur positif d différent de 1 et n. Par définition (de diviseur) il existe $m \in \mathbb{Z}$ tel que

$$n = md.$$

Notons que $1 < d < n$ et $1 < m < n$.
Comme n est le plus petit entier positif qui ne s'écrit pas comme un produit de nombres premiers et m, d sont strictement plus petits, ces deux nombres s'écrivent sous la forme

$$m = p_1 p_2 \cdots p_k \quad \text{et} \quad d = q_1 q_2 \cdots q_\ell$$

avec des nombres premiers $p_1, \ldots, p_k$ et $q_1, \ldots, q_\ell$.
Cela donne :

$$n = md = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell.$$

Nous avons donc obtenu que n s'écrit comme produit de nombres premiers. Ceci contredit notre hypothèse que l'énoncé du lemme est faux. Alors, c'est faux que le lemme est faux ; donc, le lemme est vrai. □

Assertions

Nous allons regarder la structure des écrits mathématiques de plus près. Le rôle central est occupé par les assertions. Par exemple, une preuve est une suite d'assertions de telle sorte que la **vérité** d'une assertion **implique** la vérité de l'assertion suivante.

Une **assertion** est une phrase (en mathématiques, ou ailleurs) qui est **soit vraie**, **soit fausse**, mais pas les deux en même temps.[1]

Il n'y a donc pas de troisième possibilité (en latin : *tertium non datur*). Nous avons déjà vu des exemples :

- *Le carré d'un entier relatif pair est pair.*

  Cette assertion est vraie comme nous l'avons vu dans la proposition 1.3.

- *Il n'y a qu'un nombre fini de nombres premiers.*

  Cette assertion est fausse (voir le théorème 1.5).

D'autres exemples d'assertions :

- $x = 1$

  La véracité ou non de cette assertion dépend du contexte, car nous n'avons pas précisé ce qu'était x.

  - Soit x une solution de l'équation $2x = 2$. Dans ce contexte, l'assertion « $x = 1$ » est vraie (on le démontre en divisant par 2).
  - Soit x une solution de l'équation $2x = 4$. Dans ce contexte, l'assertion « $x = 1$ » est fausse.
  - Soit x une solution de l'équation $x^2 = 1$. Dans ce contexte, nous ne pouvons rien dire quant à la vérité de l'assertion « $x = 1$ » car x peut être 1 ou -1.

- Pour illustrer, on peut aussi prendre des assertions de notre vie quotidienne, par exemple :

  - Il pleut.
  - La rue est mouillée.
  - etc.

Implication

Si la véracité d'une assertion entraîne celle d'une autre, on parle d'une *implication* que nous notons $\Rightarrow$ (ou $\Leftarrow$ selon la situation). Le symbole $\Rightarrow$ se lit comme : « implique », « alors », « en conséquence », « donc », « est suffisant pour » etc. Nous allons formaliser ces concepts dans la prochaine section ; maintenant nous allons regarder des exemples.

(1) Assertion A : « Il pleut. »

Assertion B : « La rue est mouillée. »

Nous pouvons les combiner pour obtenir l'assertion :
« S'il pleut, alors la rue est mouillée. »
En symboles : Il pleut. $\Rightarrow$ La rue est mouillée.

[1] Il y a des subtilités concernant cette phrase que nous n'évoquerons pas (il faut que l'assertion soit formulée convenablement) car vous ne les rencontrerez dans aucun cours de vos études, sauf si vous suivez un cours de logique mathématique.

Cette assertion est certainement vraie. Notez que nous n'avons pas dit que l'assertion A est vraie. Nous avons seulement fait une remarque sur la *relation* entre les deux assertions. Cela ne devrait pas vous choquer : La phrase « S'il pleut, alors la rue est mouillée. » est vraie même s'il ne pleut pas en ce moment.

On peut aussi écrire la même chose comme ça :
La rue est mouillée. $\Leftarrow$ Il pleut.

Nous avons donc seulement échangé les deux côtés, mais le contenu reste le même. En mots, on pourrait dire :
« La rue est mouillée s'il pleut. »

Voici une formulation plus sophistiquée pour encore dire la même chose :
« Il suffit qu'il pleuve pour que la rue soit mouillée. »

Noter que l'assertion
« Si la rue est mouillée, il pleut. »
est fausse car il peut y avoir d'autres raisons pour une rue mouillée (par ex., lavage).

(2) Assertion A : « Je réussis l'examen. »

Assertion B : « Je reçois les points ECTS. »

On peut les combiner ainsi :
« Si je réussis l'examen, alors je reçois les points ECTS. »
en symboles : Je réussis l'examen. $\Rightarrow$ Je reçois les points ECTS.

C'est également une assertion vraie.

(3) Assertion A : « $x = 1$ »

Assertion B : « $2x = 2$ »

Nouvelle assertion vraie : « $x = 1 \Rightarrow 2x = 2.$ »
On pourrait aussi écrire : « $2x = 2 \Leftarrow x = 1.$ »

Répétons que nous n'avons rien dit sur la vérité des assertions A et B. Nous avons seulement constaté une relation entre les deux assertions.

(4) Assertion A : « $x = 1$ »

Assertion B : « $x^2 = 1$ »

Nouvelle assertion vraie : « $x = 1 \Rightarrow x^2 = 1.$ »
On pourrait aussi écrire : « $x^2 = 1 \Leftarrow x = 1.$ »

(5) (Juste pour montrer qu'on peut aussi obtenir des assertions fausses :)

Assertion A : « $x = 1$ »

Assertion B : « $2x = 4$ »

Nouvelle assertion (fausse !) : « $x = 1 \Rightarrow 2x = 4.$ »

« $A \Rightarrow B$ » et « $A \Leftarrow B$ » doivent être bien distingués !

Voici un exemple d'une utilisation incorrecte :

S'il fait nuit, alors les phares des voitures sont allumés. Les phares de cette voiture sont allumés, donc il fait nuit.

Equivalence

Si une assertion est vraie si et seulement si une autre est vraie, on parle de *l'équivalence* des deux assertions, notée $\Leftrightarrow$. Le symbole $\Leftrightarrow$ indique l'équivalence ; il veut dire que les deux implications $\Rightarrow$ et $\Leftarrow$ sont vraies en même temps. Il se dit « est équivalent à », « si et seulement si », etc.
Exemples :

(1) Je reçois les points ECTS si et seulement si je réussis l'examen.
En symboles : Je reçois les points ECTS. $\Leftrightarrow$ Je réussis l'examen.

(2) Soit x un nombre réel. On a $2x = 2$, si et seulement si $x = 1$.
En symboles : $2x = 2 \ \Leftrightarrow \ x = 1$

(3) Soit x un nombre réel. On a $x^2 = 1$, si et seulement si $x = 1$ ou $x = -1$.
En symboles : $x^2 = 1 \ \Leftrightarrow \ (x = 1$ ou $x = -1)$

Discutons d'abord pourquoi il n'y a pas d'exemple avec une rue mouillée : L'assertion : « La rue est mouillée. $\Rightarrow$ Il pleut. » est fausse (car quelqu'un pourrait nettoyer sa voiture) ! Alors, il ne s'agit pas d'une équivalence. Aussi l'assertion : « $x^2 = 1 \Leftrightarrow x = 1$ » est fausse, car l'assertion « $x^2 = 1 \Rightarrow x = 1$ » est fausse, parce que $x = -1$ est une autre solution.
Voici un autre exemple de proposition.

Proposition 1.7. *Soient n, m des entiers relatifs. Alors les assertions suivantes sont équivalentes :*

(i) n *est pair.*

(ii) $n + 2m$ *est pair.*

Si on démontre une équivalence, il faut démontrer les deux assertions $\Rightarrow$ et $\Leftarrow$.

Démonstration. « (i) $\Rightarrow$ (ii) » : On suppose que (i) est vrai : que n est pair. Il existe donc $q \in \mathbb{Z}$ tel que $n = 2q$. Alors, $n + 2m = 2q + 2m = 2(q + m)$. Donc $n + 2m$ est pair.
« (i) $\Leftarrow$ (ii) » : On suppose que (ii) est vrai : $n + 2m$ est pair. Il existe donc $q \in \mathbb{Z}$ tel que $n + 2m = 2q$. Alors, $n = 2q - 2m = 2(q - m)$. Donc n est pair. □

Comment manipuler des équations

On commence cette petite partie par un avertissement :

Faites bien attention au symbole $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ à utiliser.

C'est une grande source d'erreur au début.
Nous allons insister sur l'utilisation des symboles $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ dans les manipulations des équations.

Voici un exemple. Soit x un nombre réel.

$$\begin{array}{lrl} & x^2+3=4x-1 & |-(4x-1) \\ \Rightarrow & x^2-4x+4=0 & \\ \Rightarrow & (x-2)^2=0 & |\sqrt{\ } \\ \Rightarrow & x-2=0 & |+2 \\ \Rightarrow & x=2 & \end{array}$$

Notre calcul montre : si $x \in \mathbb{R}$ est une solution de l'égalité $x^2+3=4x-1$, alors $x=2$. Elle ne montre pas que $x=2$ est une solution. Mais cette dernière assertion est aussi correcte : $2^2+3=4\cdot 2-1$. Nous pouvons rajouter une autre ligne en bas de notre calcul :

$$\Rightarrow x^2+3=4x-1.$$

Nous avons fermé le cercle : on peut déduire de la vérité de n'importe laquelle des assertions dans le calcul la vérité des autres en suivant les flèches d'implication. Donc, toutes les manipulations que nous avons faites sont en effet des équivalences : on aurait pu écrire $\Leftrightarrow$ au lieu de $\Rightarrow$ à chaque fois. On pourrait aussi vérifier que chacune des implications que nous avons écrites est en fait une équivalence. Vous pensez peut-être que les remarques précédentes ne sont que des subtilités sans importance. Considérons encore une fois un nombre réel x et faisons le calcul suivant :

$$\begin{array}{lrl} & x^2=-9 & |\text{ carré} \\ \Rightarrow & x^4=81 & |\sqrt[4]{\ } \\ \Rightarrow & x=3 \text{ ou } x=-3 & \end{array}$$

Les manipulations sont correctes et ce calcul montre : si $x \in \mathbb{R}$ est une solution de l'égalité $x^2=-9$, alors $x=3$ ou $x=-3$. Mais, ni l'un ni l'autre n'est une solution de l'équation de départ ! Pourquoi ? Parce que notre équation du début ne possède aucune solution dans $\mathbb{R}$. Donc, attention à vérifier que vos calculs donnent une solution au problème initial.

Que pensez-vous des arguments suivants ? Soient n, m deux nombres réels.

$$\begin{array}{lrl} & n=m & |\cdot n \\ \Rightarrow & n^2=nm & |+n^2 \\ \Rightarrow & n^2+n^2=n^2+nm & \\ \Rightarrow & 2n^2=n^2+nm & |-2nm \\ \Rightarrow & 2n^2-2nm=n^2+nm-2nm & \\ \Rightarrow & 2n^2-2nm=n^2-nm & \\ \Rightarrow & 2(n^2-nm)=1\cdot(n^2-nm) & |:(n^2-nm) \\ \Rightarrow & 2=1 & \end{array}$$

Nous avons donc démontré : Si $n=m$, alors $2=1$. L'égalité $n=m$ peut être facilement satisfaite, par exemple par $n=m=1$. Alors l'assertion $2=1$ est vraie. Quoi ? ? ? ? ? ? ?

La faute se passe dans la dernière implication. Elle est fausse si $n^2 - nm = 0$ (c'est d'ailleurs le cas quand $n = m$), parce que dans ce cas, nous divisons par zéro. Notez que quelle que soit la valeur de $n^2 - nm$, multiplier par cette expression donne une implication :

$$a(n^2 - nm) = b(n^2 - nm) \Leftarrow a = b.$$

Nous avons donc mis $\Rightarrow$ où $\Leftarrow$ aurait été correct. Mais $\Leftarrow$ dans la dernière ligne ne nous permet plus de déduire que l'assertion $2 = 1$ est vraie. Ouf, sauvés.

Encore un autre... Soient n, m deux nombres réels.

$$\begin{aligned}
& m = n + 1 && | - m \\
\Rightarrow \quad & 0 = n + 1 - m && | \cdot 4 \\
\Rightarrow \quad & 0 = 4n + 4 - 4m && | + (n^2 - 2mn + m^2) \\
\Rightarrow \quad & n^2 - 2mn + m^2 = n^2 + 4n + 4 - 2mn - 4m + m^2 && \\
\Rightarrow \quad & (n - m)^2 = (n + 2)^2 - 2(n + 2)m + m^2 && \\
\Rightarrow \quad & (n - m)^2 = (n + 2 - m)^2 && |\sqrt{\ } \\
\Rightarrow \quad & n - m = n + 2 - m && | + (m - n) \\
\Rightarrow \quad & 0 = 2 &&
\end{aligned}$$

Nous avons donc démontré : Si $m = n + 1$, alors $0 = 2$. L'égalité $m = n + 1$ peut être facilement satisfaite, par exemple par $m = 1$ et $n = 0$. Alors l'assertion $0 = 2$ est vraie. Nous avons donc encore une fois « démontré » une assertion évidement fausse. Pourquoi ? ? ? ? ?

Indices, sommes et produits

Si nous avons une fonction qui dépend de deux variables, par exemple $f(x, y) = x^2 + 2y$, on peut les numéroter en utilisant des indices x_1, x_2 (dans notre exemple : $f(x_1, x_2) = x_1^2 + 2x_2$). Cela est surtout utile si le nombre des variables n'est pas fixe, par exemple $f(x_1, x_2, \ldots, x_n)$. Nous avons aussi déjà utilisé des indices dans les sections précédentes, par ex. $p_1, p_2, \ldots, p_n$.
Vous connaissez peut-être aussi les polynômes. Un polynôme de degré n à coefficients rationnels est une expression :

$$p(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n$$

avec $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ et $a_n \neq 0$ (pour que le degré soit vraiment n et pas inférieur). Évidemment, on peut faire la même chose pour des coefficients dans un autre ensemble que $\mathbb{Q}$ (par exemple $\mathbb{R}$ ou $\mathbb{C}$).
Il est possible d'avoir deux indices. Par exemple, on peut numéroter les entrées d'une matrice A de taille $n \times m$ comme suit :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \ldots & a_{1,m} \\ a_{2,1} & a_{2,2} & a_{2,3} & \ldots & a_{2,m} \\ a_{3,1} & a_{3,2} & a_{3,3} & \ldots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \ldots & a_{n,m} \end{pmatrix}.$$

On peut, par exemple, définir une matrice de taille 3×3 par la formule :

$$a_{i,j} := 3 \cdot (i-1) + j \text{ pour } 1 \leq i \leq 3 \text{ et } 1 \leq j \leq 3.$$

Cela donne

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

Il peut même nous arriver d'avoir des indices qui ont aussi des indices eux-mêmes, par exemple :
$A_{1,1}, A_{1,2}, \dots A_{1,e_1}$
$A_{2,1}, A_{2,2}, \dots A_{2,e_2}$
$\dots$
$A_{n,1}, A_{n,2}, \dots A_{n,e_n}$
On peut imaginer cet exemple comme une matrice, sauf que la longueur des lignes varie d'une ligne à l'autre.

Définition 1.8. *Le symbole* delta de Kronecker *est défini comme*

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Par exemple, nous avons pour $n \in \mathbb{N}$

$$A = \begin{pmatrix} \delta_{1,1} & \delta_{1,2} & \delta_{1,3} & \dots & \delta_{1,n} \\ \delta_{2,1} & \delta_{2,2} & \delta_{2,3} & \dots & \delta_{2,n} \\ \delta_{3,1} & \delta_{3,2} & \delta_{3,3} & \dots & \delta_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \delta_{n,1} & \delta_{n,2} & \delta_{n,3} & \dots & \delta_{n,n} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

c'est la matrice « identité ».

Nous avons souvent utilisé les trois points « $\dots$ ». C'est une écriture suggestive, mais pas précise ! Vous pensez que $3, 5, 7, \dots$ est la suite des nombres impairs supérieurs ou égaux à 3 ? Mais non, on pourrait aussi vouloir parler des nombres premiers impairs. Donc, il vaut mieux être précis. Pour cela on introduit les symboles $\sum$ et $\prod$ pour les sommes et les produits.
Voici des exemples :

- Notre polynôme ci-dessus s'écrit :

$$p(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i.$$

  Cette notation dit que l'indice i parcourt les $n+1$ entiers entre 0 et n (avec 0 et n inclus).

- $\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15.$
- $\prod_{i=1}^{5} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$

- $\sum_{i=1}^{5} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$.
- $\prod_{i=1}^{5} i^2 = 1^2 \cdot 2^2 \cdot 3^2 \cdot 4^2 \cdot 5^2 = 14400$.
- Cas spécial de la somme vide : Soient $b < a$ des entiers relatifs. Alors

$$\sum_{i=a}^{b} a_i = 0$$

  pour n'importe quel a_i.

- Cas spécial du produit vide : Soient $b < a$ des entiers relatifs. Alors

$$\prod_{i=a}^{b} a_i = 1$$

  pour n'importe quel a_i.

Définition 1.9. *Pour un entier naturel n on définit n* factorielle *comme*

$$n! = \prod_{i=1}^{n} i.$$

Noter le cas spécial $0! = 1$ qui correspond au produit vide. Nous avons déjà vu le cas spécial $5! = 120$ plus haut.

Récurrence

Une méthode de preuve très souvent utilisée est la **démonstration par récurrence**. Nous commençons par un exemple qui – selon la légende – est dû à Gauß quand il était enfant. Son professeur voulait occuper les enfants et leur a demandé de calculer la somme des entiers naturels jusqu'à 100, c'est-à-dire $1 + 2 + \cdots + 100 = \sum_{i=1}^{100} i$. Gauß a trouvé la réponse tout de suite : 5050. On peut s'imaginer que son professeur n'était pas content car il lui fallait alors trouver d'autres choses pour occuper les enfants.

Proposition 1.10 (« Petit Gauß »)**.** *Pour tout nombre naturel $n \geq 1$, on a la formule :*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Démonstration.

(1) On commence toujours par une vérification de la formule au cas minimal, ici $n = 1$:

$$\sum_{i=1}^{1} i = 1 \overset{!}{=} \frac{1(1+1)}{2}.$$

(2) Supposons que nous savons déjà que la formule est vraie pour $n = m$ (par ex. $m = 1$). Nous allons la démontrer pour $n = m + 1$:

$$\sum_{i=1}^{m+1} i = \big(\sum_{i=1}^{m} i\big) + (m+1) \overset{\text{cas} n=m}{=} \frac{m(m+1)}{2} + (m+1)$$
$$= \frac{m(m+1) + 2(m+1)}{2} = \frac{(m+1)(m+2)}{2}.$$

(3) Ce que nous avons fait suffit déjà pour conclure que la formule est vraie pour tout $n \geq 1$:

Pour le cas $n = 1$ on utilise (1).
Puis on utilise (2) pour conclure du cas $n = 1$ le cas $n = 1 + 1 = 2$.
Puis on utilise (2) pour conclure du cas $n = 2$ le cas $n = 2 + 1 = 3$.
Puis on utilise (2) pour conclure du cas $n = 3$ le cas $n = 3 + 1 = 4$.
On se convainc que par ce processus on traite tous les $n \geq 1$.

□

Le principe de la démonstration précédente s'appelle « démonstration par récurrence ».
Nous formalisons ce principe maintenant. Soit $A(n)$ une assertion (pour n un entier), par exemple

$$A(n) : \ 1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Les trois étapes dans la preuve sont appelées ainsi :

Initialisation Démontrer que l'assertion $A(0)$ est vraie.

Hérédité Pour tout n dans $\mathbb{N}$, démontrer que l'assertion $A(n)$ implique l'assertion $A(n+1)$.

Conclusion Pour tout n dans $\mathbb{N}$, l'assertion $A(n)$ est vraie.

Un autre exemple :

Proposition 1.11 (Somme des premiers nombres impairs)**.** *Pour tout nombre naturel $n \geq 1$, on a la formule*

$$1 + 3 + 5 + \cdots + (2n-1) = \sum_{i=1}^{n} (2i-1) = n^2.$$

Démonstration. Nous voulons démontrer l'assertion

$$A(n) : \ 1 + 3 + 5 + \cdots + (2n-1) = \sum_{i=1}^{n} (2i-1) = n^2$$

pour tout nombre naturel $n \geq 1$.

Initialisation : Pour $n = 1$ on a $1 = 1^2$, donc $A(1)$ est vraie.

Hérédité : « $A(n) \Rightarrow A(n+1)$ » : Supposons donc que pour $n \in \mathbb{N}$ l'assertion $A(n)$ est vraie.

$$\sum_{i=1}^{n+1}(2i-1) = \big(\sum_{i=1}^{n}(2i-1)\big) + (2n+1) \overset{A(n)}{=} n^2 + (2n+1) = (n+1)^2,$$

donc $A(n+1)$ est vraie.

Conclusion : Pour tout $n \in \mathbb{N}_{>0}$ on a $\sum_{i=1}^{n}(2i-1) = n^2$.

□

Pour simplifier, nous allons utiliser les notations suivantes.

Notation 1.12. *Soit n_0 un entier naturel ; on note $\mathbb{N}_{\geq n_0}$ l'ensemble des entiers naturels supérieurs ou égaux à n_0 et $\mathbb{N}_{>n_0}$ l'ensemble des entiers naturels strictement supérieurs à n_0.*

Le principe de récurrence a plusieurs variantes.

Proposition 1.13 (Variantes du principe de récurrence)**.**

Changement d'initialisation *Soient n_0 dans $\mathbb{N}$ et, pour tout n dans $\mathbb{N}$ supérieur ou égal à n_0, une assertion $A(n)$. Alors :*

$$(A(n_0) \wedge (\forall n \in \mathbb{N}_{\geq n_0}, A(n) \Rightarrow A(n+1))) \Rightarrow (\forall n \in \mathbb{N}_{\geq n_0}, A(n)).$$

Récurrence forte *Soit, pour tout n dans $\mathbb{N}$, une assertion $A(n)$. Alors*

$$(A(0) \wedge (\forall n \in \mathbb{N}, (A(0) \text{ et } A(1) \dots \text{ et } A(n)) \Rightarrow A(n+1))) \Rightarrow (\forall n \in \mathbb{N}, A(n)).$$

Récurrence finie *Soient N et M dans $\mathbb{N}$, avec $N < M$ et pour tout entier n dans $\{N, \dots, M\}$, une assertion $A(n)$. Alors*

$$(A(N) \wedge (\forall n \in \{N, \dots, M-1\}, A(n) \Rightarrow A(n+1))) \Rightarrow (\forall n \in \{N, \dots, M\}, A(n)).$$

Récurrence finie descendante *Soient N et M dans $\mathbb{N}$, avec $N < M$ et pour tout entier n dans $\{N, \dots, M\}$, une assertion $A(n)$. Alors*

$$(A(M) \wedge (\forall n \in \{N+1, \dots, M\}, A(n) \Rightarrow A(n-1))) \Rightarrow (\forall n \in \{N, \dots, M\}, A(n)).$$

Nous connaissons maintenant les principes les plus importants des démonstrations :

- démonstration directe ;
- démonstration de la contraposée (c'est une démonstration indirecte) ;
- démontration par l'absurde (c'est une démonstration indirecte) ;
- démonstration qu'une assertion est fausse par un contrexemple ;
- démonstration par récurrence.

Développement du binôme de Newton

Définition 1.14. *Soient $n \in \mathbb{N}$ et $k \in \mathbb{Z}$ Pour $0 \leq k \leq n$, nous définissons le* coefficient binomial *comme*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Pour $k > n$ ou $k < 0$ on définit

$$\binom{n}{k} = 0.$$

En allemand on prononce : « n über k » ou « k aus n ». En anglais on dit : « n choose k ». En français on note aussi C_n^k (pour « combinaison de n parmi k »).

Exemple 1.15.

- *Pour tout n dans $\mathbb{N}$, on a* $\binom{n}{0} = \binom{n}{n} = 1.$
- *Pour tout n dans $\mathbb{N}_{>0}$, on a* $\binom{n}{1} = \binom{n}{n-1} = n.$

Lemme 1.16. *Pour $n, k \in \mathbb{N}$ et $k \leq n$ nous avons :*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Lemme 1.17. *Pour $n, k \in \mathbb{N}$ et $k \leq n$ nous avons :*

$$\binom{n}{k} = \prod_{i=1}^{k} \frac{n+1-i}{i}.$$

Démonstration. Exercice. □

Proposition 1.18 (Formule de Pascal)**.** *Pour tout $k, n \in \mathbb{N}$ on a :*

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Démonstration. On vérifie immédiatement l'égalité recherchée si $k \leq 0$ ou $k > n$. On peut donc

supposer $1 \leq k \leq n$. La formule se vérifie par le calcul suivant :

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!(n+1-k)}{k!(n+1-k)!} + \frac{n!k}{k!(n+1-k)!} \\ &= \frac{n!(n+1-k+k)}{k!(n+1-k)!} \\ &= \frac{(n+1)!}{k!(n+1-k)!} \\ &= \binom{n+1}{k}.\end{aligned}$$

□

Nous donnons maintenant l'explication combinatoire du coefficient binomial.

Proposition 1.19. *Pour tous n et k dans $\mathbb{N}_{\geq 1}$, le coefficient binomial $\binom{n}{k}$ exprime le nombre de possibilités pour choisir k entiers parmi $1, 2, \ldots, n$ (l'ordre ne jouant aucun rôle).*

Démonstration. Par récurrence sur n.

Initialisation : Pour $n = 1$ et $k = 1$ il n'existe qu'une seule possibilité et $\binom{1}{1} = 1$, donc l'assertion est vraie.

Hérédité : « $n \Rightarrow n+1$ » : On cherche à sélectionner k entiers parmi $1, \ldots, n+1$. On distingue selon deux cas : soit on sélectionne $n+1$, soit on ne le sélectionne pas.

Si on choisit $n+1$, il nous reste $k-1$ entiers à choisir, parmi $1, \ldots, n$. Par hypothèse de récurrence, il existe $\binom{n}{k-1}$ possibilités de choisir $k-1$ nombres parmi $1, 2, \ldots, n$. Donc, il existe $\binom{n}{k-1}$ possibilités de choisir k éléments parmi $1, 2, \ldots, n+1$ à la condition que $n+1$ est choisi.

Si on ne choisit pas $n+1$, cela signifie qu'on va choisir nos k entiers parmi $1, \ldots, n$. Encore par l'hypothèse de récurrence, il existe $\binom{n}{k}$ possibilités de choisir k éléments parmi $1, 2, \ldots, n$; c'est-à-dire qu'il existe $\binom{n}{k}$ possibilités de choisir k entiers parmi $1, 2, \ldots, n+1$ à la condition que $n+1$ n'est pas choisi.

Donc, le nombre de possibilités de choisir k entiers parmi $1, 2, \ldots, n+1$ est

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k},$$

par la formule de Pascal (proposition 1.18).

□

Par exemple, le nombre de possibilités de choisir 6 nombres parmi $1, 2, \ldots, 49$ (Lotto allemand) est $\binom{49}{6} = 13983816$.

Théorème 1.20 (Formule du binôme de Newton)**.** *Soit $n \in \mathbb{N}$. Pour tout a, b (nombres réels, rationnels, complexes, entiers, etc.) nous avons :*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration. Par récurrence.

Initialisation : Pour $n = 0$ on a $(a+b)^0 = 1$ et $\sum_{k=0}^{0} \binom{n}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 1$, donc l'assertion est vraie.

Hérédité : « $n \Rightarrow n+1$ » : Nous supposons que pour $n \in \mathbb{N}$ l'égalité $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ a déjà été démontrée. Nous faisons le calcul suivant :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n \cdot (a+b) \\
&= \Big(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\Big) \cdot (a+b) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-(k-1)} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= a^0 b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + a^{n+1} b^0 \\
&= a^0 b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + a^{n+1} b^0 \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}$$

Nous avons utilisé la formule de Pascal (proposition 1.18).

□

2 Logique élémentaire

Objectifs :

- Maîtriser la conjonction, disjonction, négation d'assertions ainsi que les implications, l'équivalence et la contraposée ;
- maîtriser les quantificateurs $\forall$ et $\exists$;
- maîtriser le calcul avec les tables de vérité.

Une grande partie du contenu de cette section a déjà été traitée dans le cours de M. Schlenker pendant la semaine préparatoire. On donnera donc parfois moins de détails au cours.
Dans la section précédente, nous avons déjà considéré le concept des assertions et nous avons introduit d'un point de vue intuitif les implications et l'équivalence. Nous allons maintenant étudier d'autres opérations sur les assertions et formaliser les implications.

Et et ou ou ou et et

Si on a une assertion, son contraire en est une autre, appelée sa **négation** (par ex. « Il pleut. » Négation : « Il ne pleut pas. »). On peut aussi combiner deux assertions par un « **et** » ou un « **ou** » (par ex. « x est pair **et** x est positif. » ; « $x = 2$ **ou** x est impair. »).
Nous allons étudier ces trois constructions de plus près. Pour cela nous allons utiliser les tables de vérité. Pour ceux qui aiment bien l'informatique, cela peut aider d'utiliser le modèle des circuits électriques comme dans le livre de Schichl/Steinbauer.

Définition 2.1. *Soient A et B des assertions.*

(a) **La conjonction « et » (symbole : $\wedge$)**

« Et » en mathématiques a la même signification qu'au quotidien :

L'assertion A et *B (en symboles : $A \wedge B$) est vraie si et seulement si A et B sont vraies.*

(b) **La disjonction « ou » (symbole : $\vee$)**

« Ou » en mathématiques a la signification suivante :

L'assertion « A ou B » (en symboles : $A \vee B$) est vraie si au moins une des assertions A, B est vraie.

(c) **La négation (symbole : $\neg$)**

La négation de A est l'assertion « non A » (en symboles : $\neg A$) qui est vraie si et seulement si A est faux.

Introduisons maintenant le formalisme (facile !) des tables de vérité (v= vrai, f = faux) à l'exemple de la conjonction.

A	B	$A \wedge B$	Explication
v	v	v	Si A est vrai et B est vrai, alors $(A \wedge B)$ est vrai.
v	f	f	Si A est vrai et B est faux, alors $(A \wedge B)$ est faux.
f	v	f	Si A est faux et B est vrai, alors $(A \wedge B)$ est faux.
f	f	f	Si A est faux et B est faux, alors $(A \wedge B)$ est faux.

(1) P est étudiant(e) de ce cours **et** P habite à Luxembourg.
(2) $x^2 = 1$ **et** $x > 0$

Regardons (2) de plus près. Soit A l'assertion « $x^2 = 1$ » et B l'assertion « $x > 0$ ».

- $x = 1$: c'est le cas de la rangée 1 ; alors, l'assertion est vraie.
- $x = -1$: c'est le cas de la rangée 2 ; alors, l'assertion est fausse.
- $x \neq 1$ et $x > 0$: c'est le cas de la rangée 3 ; alors, l'assertion est fausse.
- $x \neq -1$ et $x \leq 0$: c'est le cas de la rangée 4 ; alors, l'assertion est fausse.

Voici, la table de vérité pour la disjonction :

A	B	$A \vee B$
v	v	v
v	f	v
f	v	v
f	f	f

(1) P est étudiant(e) de ce cours **ou** P habite à Luxembourg.
(2) $x^2 = 1$ **ou** $x > 0$

Regardons (2) de plus près. Soit A l'assertion « $x^2 = 1$ » et B l'assertion « $x > 0$ ».

- $x = 1$: c'est le cas de la rangée 1 ; alors, l'assertion est vraie.
- $x = -1$: c'est le cas de la rangée 2 ; alors, l'assertion est vraie.
- $x \neq 1$ et $x > 0$: c'est le cas de la rangée 3 ; alors, l'assertion est vraie.
- $x \neq -1$ et $x \leq 0$: c'est le cas de la rangée 4 ; alors, l'assertion est fausse.

Notez que « ou » au quotidien est souvent utilisé de manière exclusive : « Voulez vous du café ou du thé ? » ; « Allez-vous à droite ou à gauche ? ». C'est soit l'un, soit l'autre. Pas en maths : Si A et B sont vraies, alors l'assertion $(A \vee B)$ est vraie. Mais, aussi au quotidien on peut utiliser « ou » comme en maths : « Si c'est votre anniversaire ou si vous réussissez l'examen, je vous félicite. » Je vous félicite même si vous réussissez votre examen le jour de votre anniversaire.
Pour être comlet, nous donnons la table de vérité de la négation qui est facile.

A	$\neg A$
v	f
f	v

Voici, des exemples de négations :

(1) Il pleut.
Négation : Il ne pleut pas.

(2) $x = 1$
Négation : $x \neq 1$

(3) Il est luxembourgeois **et** il étudie à l'Université du Luxembourg.
Négation : Il n'est pas luxembourgeois **ou** il n'étudie pas à l'Université du Luxembourg.

(4) $x^2 = 1$ **et** $x > 0$
Négation : $x^2 \neq 1$ **ou** $x \leq 0$

Soulignons ce que nous avons vu dans les exemples (3) et (4) :

Lors de la négation, « et » et « ou » sont à échanger !

Voici la proposition qui exprime cela.

Proposition 2.2 (De Morgan)**.** *Soient A, B des assertions. Alors :*

(a) $\neg(A \wedge B) = (\neg A) \vee (\neg B)$,

(b) $\neg(A \vee B) = (\neg A) \wedge (\neg B)$.

Démonstration. L'assertion (a) se voit par l'égalité de la 3ème et la dernière colonne dans la table de vérité :

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$(\neg A) \vee (\neg B)$
v	v	v	f	f	f	f
v	f	f	v	f	v	v
f	v	f	v	v	f	v
f	f	f	v	v	v	v

La démonstration de (b) est similaire. □

Mentionnons encore la **double négation** : on vérifie immédiatement que $\neg(\neg A) = A$; donc la négation de la négation d'une assertion est égale à l'assertion du début : s'il est faux que l'assertion A est fausse, alors A est vraie. Voici, quelques exemples :

- Il n'est pas vrai que le Luxembourg n'appartient pas à l'UE.
- Je ne vais pas m'abstenir de voter.
- « $\neg(x \neq 1)$ » est une façon compliquée pour écrire « $x = 1$ ».

Pour finir, nous donnons un théorème qui résume quelques règles pour le calcul avec les symboles $\vee, \wedge, \neg$. La démonstration se fait par tables de vérité.

Théorème 2.3. *Soient A, B, C des assertions. Alors les égalités suivantes sont vraies.*

(a) $A \vee B = B \vee A$,
$A \wedge B = B \wedge A$ *(commutativité) ;*

(b) $A \vee (B \vee C) = (A \vee B) \vee C$,
$A \wedge (B \wedge C) = (A \wedge B) \wedge C$ *(associativité) ;*

(c) $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$,
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ *(distributivité) ;*

(d) $A \vee (B \wedge A) = A$,
$A \wedge (B \vee A) = A$ *;*

(e) $A \vee A = A$,
$A \wedge A = A$ *;*

(f) $A \vee f = A$,
$A \wedge v = A$ *; ici, v et f sont les assertions qui sont toujours vraies/fausses.*

(g) $A \vee v = v$,
$A \wedge f = f$ *;*

(h) $A \vee (\neg A) = v$,
$A \wedge (\neg A) = f$ *;*

(i) $\neg(\neg A) = A$ *;*

(j) $\neg(A \vee B) = (\neg A) \wedge (\neg B)$,
$\neg(A \wedge B) = (\neg A) \vee (\neg B)$ *(règles de de Morgan).*

De l'existence pour tout

Il y a peut-être une personne parmi vous qui a deux frères. Est-ce que cette personne dit la vérité quand elle dit : « J'ai un frère » ? Evidemment que oui ! Si on a deux frères, on en a aussi un. Un mathématicien ayant un frère et pas deux dirait : « J'ai un frère et un seul » ou « J'ai précisement un frère. »
Une autre personne n'a pas de frère du tout. A-t-elle raison si elle dit : « Tous mes frères ont les cheveux verts » ? La réponse est encore : oui.

« Il existe » veut dire : il existe au moins un. Il peut y en avoir plus d'un. Souvent on utilise le symbole $\exists$ pour « il existe ». S'il existe un, mais pas deux ou plus, alors on dit que « il existe un et un seul » ou « il existe un unique ». Dans ce cas, on écrit souvent « $\exists!$ ». Les deux points « : » possèdent la signification « tel(s) que ».
Exemples :

(1) (vrai) Il y a un étudiant dans cette salle.

(2) (vrai) Il existe un nombre rationnel x tel que $2x = 2$ (en symboles : $\exists\, x \in \mathbb{Q} : 2x = 2$).

(3) (vrai) Il existe un et un seul nombre rationnel x tel que $2x = 2$ (en symboles : $\exists!\, x \in \mathbb{Q} : 2x = 2$).

(4) (vrai) Il existe un nombre rationnel x tel que $x^2 = 1$ (en symboles : $\exists\, x \in \mathbb{Q} : x^2 = 1$).

(5) (vrai) Il existe un et un seul nombre rationnel x tel que $x^2 = 1$ et $x > 0$ (en symboles : $\exists!\, x \in \mathbb{Q} : (x^2 = 1 \wedge x > 0)$).

(6) (faux) Il existe un et un seul nombre rationnel x tel que $x^2 = 1$ (en symboles : $\exists!\, x \in \mathbb{Q} : x^2 = 1$).

(7) (vrai) L'équation $a^2 + b^2 = c^2$ possède une solution en entiers positifs non nuls.
Démonstration. $3^2 + 4^2 = 5^2$.

(8) (vrai) Tous les étudiants dans cette salle étudient à l'Université du Luxembourg.

(9) (vrai) Pour tout nombre rationnel x, on a $x^2 \geq 0$ (en symboles : $\forall\, x \in \mathbb{Q} : x^2 \geq 0$)).

(10) (vrai) Le carré de tout entier relatif pair est divisible par 4 (en symboles : $\forall\, n \in \mathbb{Z} : (2 \mid n \Rightarrow 4 \mid n^2)$).

Démonstration : Soit $n \in \mathbb{Z}$ (arbitraire) tel que $2 \mid n$. Alors, $n = 2m$ pour un $m \in \mathbb{Z}$ et donc $n^2 = 4m^2$ est divisible par 4.

(11) (vrai) Tout nombre réel non-négatif est le carré d'un nombre réel non-négatif (en symboles : $\forall\, x \in \mathbb{R}_{\geq 0}, \exists\, y \in \mathbb{R}_{\geq 0} : y^2 = x$ où $\mathbb{R}_{\geq 0}$ est l'ensemble de tous les nombres réels non-négatifs).

Démonstration : Soit $x \in \mathbb{R}_{\geq 0}$ (arbitraire). On prendra $y = \sqrt{x}$, sa racine carrée.

(12) (faux) Le carré de tout nombre réel est supérieur à 0 (en symboles : $\forall\, x \in \mathbb{Q} : x^2 > 0$).

Démonstration : L'assertion est fausse pour $x = 0$.

Pour démontrer une assertion d'existence, il suffit de donner un exemple. Pour démontrer une assertion de la forme « $\forall\, x \in E : A(x)$ », on se donne un $x \in E$ (arbitraire) et on démontre $A(x)$ pour ce x. Pour démontrer qu'une assertion de la forme « $\forall\, x \in E : A(x)$ » est fausse, il suffit de donner un contre-exemple.

Le dernier point suit en fait du premier par les règles de négation que nous regardons maintenant.

(1) Tous les étudiants ont les cheveux blonds.
Négation : Il existe un étudiant qui n'a pas les cheveux blonds.

(2) Il existe x tel que $f(x) = 0$.
Négation : Pour tout x : $f(x) \neq 0$.

Si on fait la négation d'une assertion, il faut échanger $\forall$ et $\exists$, et il faut échanger « $\wedge$ » et « $\vee$ ».

La table de vérité de l'implication

Nous définissons maintenant l'implication $A \Rightarrow B$ par la table de vérité :

A	B	$A \Rightarrow B$
v	v	v
v	f	f
f	v	v
f	f	v

Voici une explication du choix de cette définition. Supposons que $A \Rightarrow B$ est vraie. Alors :

- Si A est vraie, B est vraie aussi. Ceci exprime « l'implication ».
- Si A est fausse, on ne peut rien dire sur B : B peut être vraie ou fausse.

En fait, si on exige ces deux propriétés, la table de vérité de $A \Rightarrow B$ ne peut être que celle en haut, comme on le vérifie directement. Il peut apparaître contre-intuitif que les dernières deux lignes expriment : « D'une fausse assertion A on peut conclure que toute assertion B est vraie et qu'elle est fausse. »

Proposition 2.4. *Soient A, B des assertions. Alors :*

(a) $(A \Rightarrow B) = ((\neg A) \vee B)$.

(b) $(A \Rightarrow B) = (\neg(A \wedge (\neg B)))$.

(c) $(A \Rightarrow B) = ((\neg A) \Leftarrow (\neg B))$.

La démonstration se fait par une table de vérité.
La partie (b) de la proposition 2.4 donne une explication formelle pour les démonstrations par l'absurde : si l'assertion « l'hypothèse A est vraie et la conclusion B est fausse » est fausse (par exemple, parce qu'on trouve une contradiction), alors $A \Rightarrow B$ est vrai.
Elle justifie aussi (encore une fois) la table de vérité définissant l'implication (« On ne peut pas avoir à la fois A vraie et B fausse »).

La contraposée

Soient A et B deux assertions. On appelle l'assertion « $(\neg A) \Leftarrow (\neg B)$ » la *contraposée de $(A \Rightarrow B)$*. La partie (c) de la proposition 2.4 nous dit que l'assertion « $A \Rightarrow B$ » est vraie, si et seulement si « $(\neg A) \Leftarrow (\neg B)$ » est vraie.

(1) Il pleut. $\Rightarrow$ La rue est mouillée.
Formulation équivalente : Il ne pleut pas. $\Leftarrow$ La rue n'est pas mouillée.

(2) P est un point sur le cercle de rayon r et de centre C. $\Rightarrow$ La distance entre P est C est égale à r.
Formulation équivalente : P n'est pas un point sur le cercle de rayon r et de centre C. $\Leftarrow$ La distance entre P est C est différente de r.

(3) $x = 1 \Rightarrow x^2 = 1$
Formulation équivalente : $x \neq 1 \Leftarrow x^2 \neq 1$
(4) $x^2 = 1$ et $x > 0 \Leftrightarrow x = 1$
Formulation équivalente : ($x^2 \neq 1$ ou $x \leq 0$) $\Leftrightarrow x \neq 1$

Quelquefois il est plus facile de démontrer la contraposée d'une assertion que l'assertion elle-même.

Proposition 2.5. *Si* $x^7 + x + 1 = 0$*, alors* $x \neq 1$.

Démonstration. Nous ne cherchons pas à calculer les solutions de cette équation car elles ne sont pas demandées. Il est plus facile de démontrer la contraposée : « Si $x = 1$ alors $x^7 + x + 1 \neq 0$. » On voit immédiatement que cette assertion est vraie car $1^7 + 1 + 1 = 3 \neq 0$. □

Ne pas confondre la contraposée $(\neg A) \Leftarrow (\neg B)$ avec $(\neg A) \Rightarrow (\neg B)$.

Voici un exemple d'une utilisation erronnée (!) :

> Les voitures ayant eu un accident sont cassées. Cette voiture n'a pas eu d'accident, alors elle n'est pas cassée.

3 Ensembles

Objectifs :

- Maîtriser la notion intuitive d'ensemble, union, intersection, complément, etc.
- savoir démontrer des propriétés simples.

Cette section provient du cours préparatoire. Elle ne sera traitée que brièvement.

Introduction

Les ensembles sont un outil indispensable en mathématiques. Nous en avons notamment besoin pour décrire des fonctions. Notre approche des ensembles sera celle du 19ème et du début du 20ème siècle. Une théorie plus rigoureuse ne peut pas être enseignée au début des études.

On peut décrire un ensemble en écrivant ses éléments. Par exemple :

- $\mathcal{A} = \{A, B, C, D, \ldots, X, Y, Z\}$, l'alphabet.
- $\mathcal{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, l'ensemble des chiffres.

On utilise les accolades pour indiquer qu'il s'agit d'un ensemble. Les 'objets' dans un ensemble sont appelés *éléments*.
Vous connaissez déjà des ensembles de l'école :

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ l'ensemble des nombres naturels/entiers non-négatifs,
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ l'ensemble des entiers relatifs,

- $\mathbb{Q}$, l'ensemble des nombres rationnels (les fractions),
- $\mathbb{R}$, l'ensemble des nombres réels,
- $\mathbb{C}$, l'ensemble des nombres complexes (voir le cours à ce sujet).

Nous utiliserons les notations suivantes :

- $\emptyset$ pour l'ensemble vide ;
- $\in$ pour indiquer l'appartenance d'un élément à un ensemble ;
- $\notin$ pour indiquer qu'un élément n'appartient pas à un ensemble ;
- $\#M$ pour indiquer le nombre d'éléments (le cardinal) d'un ensemble.

Par exemple :

- $7 \in \mathbb{R}$
- $7 \in \mathbb{N}$
- $7 \in \mathbb{Z}$
- $-1 \notin \mathbb{N}$
- $1/2 \in \mathbb{Q}$
- $1/2 \notin \mathbb{Z}$
- $A \in \mathcal{A}$ (A est élément de l'ensemble $\mathcal{A}$, l'alphabet.)
- $A \notin \mathcal{Z}$ (A n'est pas un élément de l'ensemble des chiffres $\mathcal{Z}$.)
- $\#\mathcal{A} = 26$
- $\#\mathcal{Z} = 10$

Nous exigeons que les ensembles satisfassent les deux propriétés fondamentales suivantes :

- Les éléments d'un ensemble sont tous deux-à-deux distincts, c'est-à-dire qu'un seul objet n'est pas deux fois élément d'un seul ensemble : $\{1, 2, 2, 3\}$ n'est qu'une écriture (non-minimale) de $\{1, 2, 3\}$.
- Les éléments d'un ensemble ne sont pas ordonnés, c'est-à-dire qu'un ensemble ne dépend pas de l'ordre dans lequel on écrit ses éléments : $\{1, 2, 3\} = \{2, 3, 1\}$.

Une autre façon d'écrire un ensemble est de le définir par des propriétés de ses éléments. Par exemple :

- $\mathcal{X} = \{ \underbrace{xy}_{\text{éléments}} \mid \underbrace{x \in \mathcal{Z}, y \in \mathcal{Z}}_{\text{propriétés}} \} = \{00, 01, 02, 03, \ldots, 99\}$.

- $\mathcal{E} = \{P \mid P$ est étudiant(e) de ce cours $\}$, l'ensemble des étudiants de ce cours.
- $\mathcal{L} = \{P \mid P$ est un/une Luxembourgeois(e) $\}$, l'ensemble de tous les Luxembourgeois.
- $\mathcal{B} = \{ABC \mid A \in \mathcal{A}, B \in \mathcal{A}, C \in \mathcal{A}\}$, l'ensemble de tous les mots de trois lettres. Noter que la virgule dans la description doit être comprise comme « et » et pourrait être remplacée par « $\wedge$ ».
- $\mathcal{G} = \{n \mid n \in \mathbb{N}, n$ est pair $\}$, l'ensemble des nombres naturels pairs.
- Soient $a, b \in \mathbb{R}$. L'ensemble

$$[a, b] := \{x \mid x \in \mathbb{R}, a \leq x \leq b\}$$

  est appelé *l'intervalle fermé entre a et b*. (Pour les intervalles ouverts (semi-ouverts), on utilise la notation $]a, b[$ ($]a, b]$).)

La notion d'ensemble de Georg Cantor

La notion d'ensemble utilisée dans ce cours (et pendant la plupart de vos études) est celle de Georg Cantor :

> Par ensemble, nous entendons toute collection M d'objets m de notre intuition ou de notre pensée, définis et distincts, ces objets étant appelés les éléments de M.

Interprétation :

- objet : « objet mathématique » ;
- collection : l'ensemble sera un nouvel objet mathématique ;
- définis : les objets doivent être clairement définis ;
- distincts : il doit être clair si deux objets sont égaux ou distincts.

Il y a des subtilités avec les ensembles que vous n'allez pas rencontrer pendant vos études (sauf dans un cours de logique mathématique). C'est à cause de cela qu'il faut en fait utiliser une notion plus moderne. Pour les mathématiques que nous allons faire, cela ne fera aucune différence.
Voici un problème avec la notion de Cantor : le paradoxe de Russell. Il en suit qu'il n'existe pas d'ensemble de tous les ensembles.
En effet, supposons par l'absurde que l'ensemble de tous les ensembles existe ; appelons le Ω. Nous pouvons alors considérer le sous-ensemble A de Ω formé des ensembles X tels que X n'est pas un élément de l'ensemble X :

$$A = \{X \in \Omega | X \notin X\}.$$

Qu'en est-il alors de A ? Si A est un élément de A ($A \in A$), alors par définition de A, A n'est pas un élément de A ($A \notin A$). Et si A n'est pas un élément de A ($A \notin A$), alors par définition de A, A est un élément de A ($A \in A$). Aucune de ces deux options n'est donc possible.

Sous-ensembles et opérations sur les ensembles

Définition 3.1. *Soient A, B des ensembles.*

- *B est appelé* sous-ensemble/partie de *A si pour tout $b \in B$ on a $b \in A$. Notation : $B \subseteq A$.*
- *A et B sont appelés* égaux *si $A \subseteq B$ et $B \subseteq A$. Notation : $A = B$.*
- *On appelle l'ensemble*
$$A \setminus B := \{a \mid a \in A, a \notin B\}$$
le complément ou la différence de B dans A.
- *On appelle l'ensemble*
$$A \cup B := \{a \mid a \in A \vee a \in B\}$$
la réunion de A et B.
- *On appelle l'ensemble*
$$A \cap B := \{a \mid a \in A \wedge a \in B\}$$
l'intersection de A et B.
- *Si on a $A \cap B = \emptyset$, on appelle $A \cup B$ la* réunion disjointe de A et B. *Notation : $A \dot\cup B$ ou $A \sqcup B$.*
- *On appelle l'ensemble*
$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$
le produit cartésien de A et B. *Ses éléments sont aussi appelés* couples.

Par exemple :

- $\{A, D, Z\} \subseteq \mathcal{A}$.
- $\{1, 2, 3, 4\} \subseteq \mathcal{Z}$; aussi : $\{1, 2, 3, 4\} \subseteq \mathbb{N}$.
- $\mathcal{G} \subseteq \mathbb{N}$
- $[1, 2] \subseteq \mathbb{R}$
- $\mathcal{Z} \setminus \{1, 2, 3, 4\} = \{0, 5, 6, 7, 8, 9\}$.
- $\{1, 2, 3, 4\} \setminus \{2, 3, 4, 5\} = \{1\}$.
- $\{1, 2, 3\} \setminus \mathcal{Z} = \emptyset$.
- $[1, 3] \setminus [2, 3] = [1, 2[$.
- $\{1, 2\} \cup \{8, 9\} = \{1, 2, 8, 9\} = \{1, 2\} \dot\cup \{8, 9\}$
- $\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$. (Tout élément n'appartient qu'une fois à l'ensemble !)
- $[1, 3] \cap [2, 4] = [2, 3]$

- $\mathcal{L} \cap \mathcal{E} = \{A \mid A$ est Luxembourgeois et étudiant de ce cours $\}$.
- $\mathbb{N} \times \mathbb{N}$ est l'ensemble de tous les couples (a, b) avec $a, b \in \mathbb{N}$.
- $\mathcal{A} \times \mathcal{Z} = \{(A,0),(A,1),\ldots,(A,9),(B,0),(B,1),\ldots,(B,9),(C,0),\ldots,(Z,9)\}$.
- $\{n \mid n \in \mathbb{Z}, 2$ divise $n\} \cap \{n \mid n \in \mathbb{Z}, 3$ divise $n\} = \{n \mid n \in \mathbb{Z}, 6$ divise $n\}$.

Quelques propriétés

Lemme 3.2. *Soient A, B, C des ensembles. Alors, les assertions suivantes sont vraies :*

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Démonstration. (a) Nous nous souvenons que deux ensembles sont égaux si l'un est sous-ensemble de l'autre et réciproquement. Nous allons alors montrer les deux inclusions :

(1) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

(2) $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$

Par définition de $\subseteq$ il faut montrer :

(1) $x \in A \cap (B \cup C) \Rightarrow x \in (A \cap B) \cup (A \cap C)$.

(2) $x \in (A \cap B) \cup (A \cap C) \Rightarrow x \in A \cap (B \cup C)$.

(1) Soit $x \in A \cap (B \cup C)$.
$\Rightarrow x \in A \wedge x \in (B \cup C)$
$\Rightarrow x \in A \wedge (x \in B \vee x \in C)$
$\Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$
$\Rightarrow x \in A \cap B \vee x \in A \cap C$
$\Rightarrow x \in (A \cap B) \cup (A \cap C)$
Nous avons démontré (1). Dans les calculs on s'est servi des règles pour le calcul avec les symboles « $\vee$, $\wedge$ » du théorème2.3.
(2) Soit $x \in (A \cap B) \cup (A \cap C)$
$\Rightarrow x \in A \cap B \vee x \in A \cap C$
$\Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$
$\Rightarrow x \in A \wedge (x \in B \vee x \in C)$
$\Rightarrow x \in A \cap (B \cup C)$.
Nous avons démontré (2), et donc (a).
(b) Exercice 3.5. □

Nous avons vu que l'intersection correspond au « et/$\wedge$ » et la réunion au « ou/$\vee$ ». Dans le prochain lemme nous voyons que le complément correspond à la négation.

Lemme 3.3. *Soient E un ensemble, A et B des parties de E et $\overline{A} = E \setminus A$ et $\overline{B} = E \setminus B$, les complémentaires de A et B dans E ; on a :*

(a) $A \cap \overline{A} = \emptyset$ *et* $A \cup \overline{A} = E$ *(autrement dit* $A \sqcup \overline{A} = E$*) ;*

(b) $E \setminus (E \setminus A) = A$ *(autrement dit* $\overline{\overline{A}} = A$*) ;*

(c) $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$ *;*

(d) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ *;*

(e) $\overline{A \cap B} = \overline{A} \cup \overline{B}$*.*

Démonstration.

(a) Supposons par l'absurde que l'intersection $A \cap \overline{A}$ est non vide. Soit alors x un élément dans $A \cap \overline{A}$. On a : $x \in A \wedge x \notin A$. Ceci est impossible, donc $A \cap \overline{A}$ est vide.

Comme A et $\overline{A}$ sont des sous-ensembles de E, leur union l'est aussi : on a $A \cup \overline{A} \subseteq E$. Démontrons maintenant que E est inclus dans l'union $A \cup \overline{A}$. Pour cela, soit x un élément de E. On a : $x \in A \vee x \notin A$. Ceci prouve que x appartient à $A \cup \overline{A}$. Ainsi, on a $E \subseteq A \cup \overline{A}$, et finalement l'égalité.

(b) Soit x dans E ; on a :

$$x \in E \setminus (E \setminus A) \Leftrightarrow x \notin E \setminus A \Leftrightarrow \neg(x \in E \setminus A) \Leftrightarrow \neg(x \notin A) \Leftrightarrow x \in A.$$

Ceci prouve l'égalité des deux ensembles.

(c) La clé dans cette démonstration est la contraposée. Par définition, l'inclusion $\overline{B} \subseteq \overline{A}$ signifie

$$\forall\, x \in E : (x \notin B \Rightarrow x \notin A).$$

On reconnaît que l'assertion entre paranthèses est la contraposée de l'assertion entre paranthèses de

$$\forall\, x \in E : (x \in A \Rightarrow x \in B),$$

qui signifie précisement $A \subseteq B$.

(d) Soit x dans E ; on a :

$$x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow \neg(x \in A \cup B) \Leftrightarrow \neg(x \in A \vee x \in B)$$

$$\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \Leftrightarrow x \in \overline{A} \wedge x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B}.$$

Ceci prouve l'égalité des deux ensembles.

(e) On a, d'après (b) et (d) :

$$\overline{A \cap B} = \overline{\overline{\overline{A}} \cap \overline{\overline{B}}} = \overline{\overline{\overline{A} \cup \overline{B}}} = \overline{A} \cup \overline{B}.$$

□

Exercices sur les ensembles

Exercice 3.4. *Soient*

$$A = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 2\} \text{ et } B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 5\}.$$

(a) Décrire l'intersection $A \cap B$.

(b) Décrire la réunion $A \cup B$.

(c) Décrire le complément $B \setminus A$.

(d) Décrire le complément $A \setminus B$.

(e) Donner le cardinal de $[12, 27] \cap A$ et de $[12, 27] \cap B$.

Exercice 3.5. *(Deuxième partie du lemme 3.2.) Soient A, B et C des ensembles. Démontrer :*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Exercice 3.6. *(a) Soient A et B des ensembles. Démontrer :*

(1) $A \subseteq B \iff A = A \cap B \iff B = A \cup B$;
(2) $A \cap B = \emptyset \iff A \setminus B = A$.

(b) Soient E un ensemble et A, B des sous-ensembles de E. Démontrer :

(1) $A \cap B = \emptyset \iff B \subseteq E \setminus A \iff A \subseteq E \setminus B$;
(2) $A \cup B = E \iff E \setminus A \subseteq B \iff E \setminus B \subseteq A$.

Corrigé des exercices sur les ensembles

Exercice 3.4. Soient

$$A = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 2\} \text{ et } B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 5\}.$$

(a) $A \cap B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 10\}$.

Raison : un entier relatif n est divisible par 10 si et seulement s'il est divisible par 2 et 5.

(b) $A \cup B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 5 \text{ ou par } 2\}$.

(c) $B \setminus A = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 5 \text{ et n'est pas divisible par } 10\}$.

(d) $A \setminus B = \{n \mid n \in \mathbb{N}, n \text{ est divisible par } 2 \text{ et n'est pas divisible par } 5\}$.

(e) $[12, 27] \cap A = \{12, 14, 16, 18, 20, 22, 24, 26\}$, donc son cardinal est 8.
$[12, 27] \cap B = \{15, 20, 25\}$, donc son cardinal est 3.

Exercice 3.5. Soient A, B et C des ensembles. On a :

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Avec la même argumentation que pour (a) du lemme 3.2, nous devons démontrer :

(1) $x \in A \cup (B \cap C) \Rightarrow x \in (A \cup B) \cap (A \cup C)$.

(2) $x \in (A \cup B) \cap (A \cup C) \Rightarrow x \in A \cup (B \cap C)$.

(1) Soit $x \in A \cup (B \cap C)$
$\Rightarrow x \in A \vee x \in (B \cap C)$
$\Rightarrow x \in A \vee (x \in B \wedge x \in C)$
$\Rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
$\Rightarrow x \in A \cup B \wedge x \in A \cup C$
$\Rightarrow x \in (A \cup B) \cap (A \cup C)$
Nous avons démontré (1).
(2) Soit $x \in (A \cup B) \cap (A \cup C)$
$\Rightarrow x \in A \cup B \wedge x \in A \cup C$
$\Rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
$\Rightarrow x \in A \vee (x \in B \wedge x \in C)$
$\Rightarrow x \in A \vee x \in (B \cap C)$
$\Rightarrow x \in A \cup (B \cap C)$
Nous avons démontré (2) et donc l'assertion demandée.

Exercice 3.6.

(a) Soient A et B des ensembles. On a :

(1) $A \subseteq B \iff A = A \cap B \iff B = A \cup B$.
Raison : Il y a plusieures manières pour démontrer cela. Nous en donnons une.
Commençons par les équivalences suivantes :

$$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B) \Leftrightarrow (x \in A \Leftrightarrow (x \in A \wedge x \in B)) \Leftrightarrow A = A \cap B.$$

Regardons maintenant les équivalences suivantes :

$$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B) \Leftrightarrow (x \in B \Leftrightarrow (x \in A \vee x \in B)) \Leftrightarrow B = A \cup B.$$

(2) $A \cap B = \emptyset \iff A \setminus B = A$.
Raison :

$$A \cap B = \emptyset \Leftrightarrow (x \in A \Rightarrow x \notin B) \Leftrightarrow A \setminus B = \{x \mid x \in A \wedge x \notin B\} = \{x \mid x \in A\} = A.$$

(b) Soient E un ensemble et A, B des sous-ensembles de E. On a :

(1) $A \cap B = \emptyset \iff B \subseteq E \setminus A \iff A \subseteq E \setminus B$.
Raison : D'abord nous avons les équivalences

$$A \cap B = \emptyset \Leftrightarrow \forall\, x \in E : (x \in A \Rightarrow x \notin B) \Leftrightarrow A \subseteq E \setminus B.$$

Pour voir le reste il suffit de prendre la contraposée de l'assertion $\forall\, x \in E : (x \in A \Rightarrow x \notin B)$ est $\forall\, x \in E : (x \in B \Rightarrow x \notin A)$ qui équivaut à l'inclusion $B \subseteq E \setminus A$.

(2) $A \cup B = E \iff E \setminus A \subseteq B \iff E \setminus B \subseteq A$.
Ces équivalences peuvent être démontrées avec des arguments similaires. Mais il est aussi possible d'appliquer les règles pour les compléments dans le lemme 3.3 à l'assertion (1).

4 Applications et fonctions

Objectifs :

- Maîtriser les notions d'application, d'image, d'image réciproque, etc. ;
- maîtriser les notions d'injectivité, de surjectivité et de bijectivité ;
- savoir démontrer des propriétés simples.

Cette section provient du cours préparatoire. Elle ne sera traitée que brièvement.
Dans ce cours, nous utilisons les mots « application » et « fonction » comme des synonymes.

La notion d'une application/fonction

Commençons par des exemples :

- Considérons l'application $f : \underbrace{\mathbb{R}}_{\text{source}} \to \underbrace{\mathbb{R}}_{\text{but}}$ donnée par la règle $f(x) = x^2$ pour tout $x \in \mathbb{R}$.

  On dit que x^2 est l'image de x par f. Par exemple : 4 est l'image de 2 par f.

  On dit aussi que 2 est une image réciproque/un antécédant de 4 par f. Noter que -2 est un autre antécédant, donc les antécédants ne sont pas uniques.

  Si une application est donnée par une règle comme f, on écrit la règle aussi comme $x \overset{f}{\mapsto} x^2$ ou $x \mapsto x^2$ tout court.

  L'image de f est la partie du but dans laquelle tout élément possède au moins un antécédant. Dans notre cas on a $\mathrm{Im}(f) = \{x \mid x \in \mathbb{R}, x \geq 0\} = \mathbb{R}_{\geq 0}$.

- $A = \{1, 2, 3\}$, $B = \{X, Y\}$. On voudrait définir une application $g : \underbrace{A}_{\text{source}} \to \underbrace{B}_{\text{but}}$. Nous pouvons simplement le faire en posant $g(1) = X$, $g(2) = Y$, $g(3) = X$.

  Une autre possibilité serait $g(1) = X$, $g(2) = Y$, $g(3) = Y$, et encore une autre $g(1) = Y$, $g(2) = Y$, $g(3) = Y$ (c'est une fonction constante).

  Par contre, il n'est ni permis de poser $g(1) = X$, $g(1) = Y$, $g(2) = X$, $g(3) = Y$, ni suffisant de poser $g(1) = X$ et $g(2) = Y$ car :

Dans la définition d'une application/fonction, tout élément de la source doit posséder une et une unique image dans le but.

- On peut définir l'application $S : \mathcal{L} \to \{\text{homme, femme}\}$ par la règle $S(P) = \text{homme}$ si la personne P de l'ensemble $\mathcal{L}$ de tous les Luxembourgeois est un homme, et $S(P) = \text{femme}$ sinon.

Nous allons formaliser cette notion maintenant.

Définition 4.1. *Soient A, B des ensembles. Une* application $f : A \to B$ *est une règle qui associe à tout élément $a \in A$ un unique élément $f(a) \in B$.*
On appelle A l'ensemble de départ ou la source de f *et B* l'ensemble d'arrivée ou but de f.
Les applications sont aussi appelées fonctions.
Soit $f : A \to B$ une application.

- *Si $a \in A$, on appelle $f(a)$* l'image de a par f.
- *Soit $S \subseteq A$ un sous-ensemble. L'ensemble*

$$f(S) = \{f(s) \mid s \in S\} \subseteq B$$

est appelé l'image (directe) de S par f.

L'ensemble $f(A) = \mathrm{Im}(f)$ est appelé l'image de f *(tout court).*

- *Soit $b \in B$. Tout $a \in A$ tel que $f(a) = b$ est appelé* une image réciproque (ou préimage ou antécédant) de b *(Un tel élément n'existe pas toujours et lorsqu'il existe, il n'est pas unique en général !).*
- *Soit $T \subseteq B$ un sous-ensemble. L'ensemble*

$$f^{-1}(T) = \{a \mid a \in A, f(a) \in T\} \subseteq A$$

est appelé l'image réciproque (ou préimage ou antécédant) de T par f.

- *On appelle l'ensemble*

$$\{(a, f(a)) \mid a \in A\} \subseteq A \times B$$

le graphe de f.

Le graphe de f est comme vous le connaissez (le dessiner).

Injectivité, surjectivité, bijectivité

Définition 4.2. *Soient A, B des ensembles et $f : A \to B$ une application.*

- *L'application f est appelée* injective *si pour tout $x, y \in A$ l'assertion*

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

est vraie. Noter la formulation équivalente : f est injectif si et seulement si pour tout $x, y \in A$ distincts $x \neq y$ leurs images sont aussi distinctes $f(x) \neq f(y)$.

- *L'application f est appelée* surjective *si pour tout $b \in B$ il existe $a \in A$ tel que $f(a) = b$. Noter que f est surjectif si et seulement si $f(A) = B$.*
- *L'application f est appelée* bijective *si elle est injective et surjective.*

Regardons ce que ces notions veulent dire dans des exemples.

- Considérons encore l'application $f : \mathbb{R} \to \mathbb{R}$ donnée par $x \mapsto x^2$.

  Alors, f n'est pas surjective car, par exemple, -1 ne possède pas d'antécédant. Elle n'est pas injective non plus, puisque $f(-1) = 1 = f(1)$.

- Faisons une petite modification et considérons l'application

$$\begin{array}{rccc} f_1 : & \mathbb{R} & \to & \mathbb{R}_{\geq 0} \\ & x & \mapsto & x^2. \end{array}$$

  Elle est surjective mais pas injective.

- Modifions-la encore un peu et considérons l'application

$$\begin{array}{rccc} f_2 : & \mathbb{R}_{\geq 0} & \to & \mathbb{R} \\ & x & \mapsto & x^2. \end{array}$$

  Maintenant, ell est injective mais pas surjective.

- Finalement, considérons l'application

$$\begin{array}{rccc} f_3 : & \mathbb{R}_{\geq 0} & \to & \mathbb{R}_{\geq 0} \\ & x & \mapsto & x^2. \end{array}$$

  Maintenant elle est injective et surjective, donc bijective.

- Regardons maintenant le deuxième exemple du début avec $A = \{1, 2, 3\}$, $B = \{X, Y\}$ et l'application $g : A \to B$ par $g(1) = X$, $g(2) = Y$, $g(3) = X$.

  Cette application est surjective. Il suffit qu'il existe une image réciproque pour chaque élément de l'ensemble d'arrivée. Vérifions ceci : une image réciproque de X est 1 (une autre est 3) et une image réciproque de Y est 2.

  Elle n'est pas injective, car 1 et 3 sont deux éléments distincts de A qui ont la même valeur $g(1) = X = g(3)$.

- L'application S est surjective : il existe au moins un Luxembourgeois et au moins une Luxembourgeoise (probablement présentes dans cette salle). Elle n'est pas injective : il y a plus qu'une Luxembourgeoise ou il y a plus qu'un Luxembourgeois (probablement aussi présents dans cette salle).

- Considérons l'application $f : \mathbb{Z} \to \mathbb{Z}$ donnée par la règle $f(n) = 2n$ pour tout $n \in \mathbb{Z}$.

  Son image $f(\mathbb{Z})$ est l'ensemble de tous les entiers relatifs pairs. Alors, elle n'est pas surjective. Mais f est injective : si $f(n) = 2n$ et $f(m) = 2m$ sont égaux, alors, $n = m$.

- Considérons l'application $f : \mathbb{Z} \to \{n \mid n \in \mathbb{Z}, n \text{ est pair }\}$ donnée par la règle $f(n) = 2n$ pour tout $n \in \mathbb{Z}$.

  Elle est bijective.

- Pour tout ensemble A on considère l'application *identité* $\mathrm{id}_A : A \to A$ donnée par la règle $\mathrm{id}_A(a) = a$ pour tout $a \in A$.

  Elle est bijective.

Pour des ensembles finis (c'est-à-dire, de cardinal fini), la proposition suivante est parfois très utile :

Proposition 4.3. *Soient A, B deux ensembles et $f : A \to B$ une application.*

(a) Supposons que A soit fini de cardinal n. Alors, les assertions suivantes sont équivalentes :

(i) f est injectif.
(ii) $\#\mathrm{Im}(f) = \#A = n$.

(b) Supposons que B soit fini de cardinal n. Alors, les assertions suivantes sont équivalentes :

(i) f est surjectif.
(ii) $\#\mathrm{Im}(f) = \#B = n$.

(c) Supposons que A, B soient finis de même cardinal n. Alors, les assertions suivantes sont équivalentes :

(i) f est injectif.
(ii) f est surjectif.
(iii) f est bijectif.

Démonstration. (a) $(i) \Rightarrow (ii)$: Comme les images $f(a)$ pour $a \in A$ sont distinctes, il en suit directement que l'image est de cardinal égal à $\#A$.
$(ii) \Rightarrow (i)$: Comme on suppose qu'il existe autant d'images qu'éléments dans la source, les images $f(a)$ pour $a \in A$ sont deux-à-deux dinstinctes, donc f est injectif.
(b) $(i) \Rightarrow (ii)$: Si f est surjectif, alors $\mathrm{Im}(f) = B$, donc en particulier $\#\mathrm{Im}(f) = \#B$.
$(ii) \Rightarrow (i)$: Comme $\mathrm{Im}(f)$ est un sous-ensemble de B, l'hypothèse $\#\mathrm{Im}(f) = \#B$ implique l'égalité $\mathrm{Im}(f) = B$, donc la surjectivité de f.
(c) C'est une conséquence directe de (a) et (b). □

Composition d'applications et application inverse

Définition 4.4. *Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. On appelle l'application*

$$g \circ f : A \to C, \quad a \mapsto g(f(a))$$

la composée de g et f.

Voici, des exemples :

- Considérons les applications $[1,2] \xrightarrow{f} [2,3] \xrightarrow{g} [4,9]$ données par les règles $f(x) = x+1$ et $g(x) = x^2$. Alors, l'application $g \circ f$ est donnée par la règle $(g \circ f)(x) = g(f(x)) = g(x+1) = (x+1)^2$.

- Soit $f : A \to B$ une application. Alors $\mathrm{id}_B \circ f = f$, puisque pour tout $a \in A$ on a $(\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a)$. De la même manière on voit $f \circ \mathrm{id}_A = f$.

Lemme 4.5 (Associativité de la composition d'applications)**.** *Soient A, B, C, D des ensembles et $f : A \to B$, $g : B \to C$ et $h : C \to D$ des applications. Alors, on a $h \circ (g \circ f) = (h \circ g) \circ f$.*

Démonstration. Deux applications $A \to D$ sont égales si elles prennent la même valeur pour chaque $a \in A$. Nous allons vérifier que ceci est le cas pour $h \circ (g \circ f)$ et $(h \circ g) \circ f$. Soit $a \in A$. Nous avons

$$(h \circ (g \circ f))(a) = h\big((g \circ f)(a)\big) = h\big(g(f(a))\big)$$

et

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h\big(g(f(a))\big).$$

Puisque les deux expressions sont les mêmes pour tout $a \in A$, nous avons achevé la démonstration. □

Lemme 4.6. *Si $f : A \to B$ est une application bijective, alors il existe une unique application $g : B \to A$ telle que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. Elle est donnée par la règle $g(b) = a$ où pour tout $b \in B$ on prend l'unique $a \in A$ tel que $f(a) = b$. L'application g est appelée* l'inverse de f *et souvent notée f^{-1} (attention : ne pas confondre la fonction inverse avec l'image réciproque !).*

Démonstration. Il y a deux choses à faire : (1) montrer l'existence d'une telle fonction g et (2) vérifier son unicité.
(1) Existence : Nous avons l'assertion

$$\forall\, b \in B, \exists!\, a \in A : f(a) = b.$$

En effet, l'existence provient de la surjectivité et l'unicité de l'injectivité. On pose $g(b) := a$. On a donc

$$\forall\, b \in B : f(g(b)) = f(a) = b \quad \Rightarrow \quad f \circ g = \mathrm{id}_B.$$

Soit $a \in A$. Pour $b := f(a)$ il existe un unique $a' \in A$ tel que $f(a') = b = f(a)$, donc $a = a'$ par l'injectivité de f. En conséquence, $g(f(a)) = a' = a$ et donc $g \circ f = \mathrm{id}_A$.
(2) Unicité : Supposons que $h : B \to A$ est une application qui satisfait aussi $h \circ f = \mathrm{id}_A$ et $f \circ h = \mathrm{id}_B$.
A cause de $f \circ h = \mathrm{id}_B$ et $f \circ g = \mathrm{id}_B$, nous concluons

$$f \circ h = f \circ g.$$

En conséquence, on a

$$g \circ (f \circ h) = g \circ (f \circ g).$$

L'associativité d'applications (lemme 4.5) implique :

$$(g \circ f) \circ h = (g \circ f) \circ g.$$

On utilisant $g \circ f = \mathrm{id}_A$ nous obtenons :

$$\mathrm{id}_A \circ h = \mathrm{id}_A \circ g.$$

Les égalités $\mathrm{id}_A \circ h = h$ et $\mathrm{id}_A \circ g = g$ impliquent

$$h = g,$$

et la démonstration est complète. □

Exercices sur les fonctions

Exercice 4.7. *Soient $A = \{1, 2, 3, 4, 5\}$ et $B = \{A, B, C, D\}$.*

(a) Décrire une application surjective de A dans B.

(b) Décrire une application de A dans B qui n'est ni surjective ni injective.

(c) Existe-t-il une application injective de A dans B ? Raison ?

(d) Décrire une application injective de B dans A.

(e) Décrire une application de B dans A qui n'est ni surjective ni injective.

(f) Existe-t-il une application surjective de B dans A ? Raison ?

Exercice 4.8. *(a) Trouver une application injective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.*

(b) Trouver une application surjective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.

(c) Trouver une bijection entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.

Exercice 4.9. *Soit $\sin : \mathbb{R} \to [-1, 1]$ la fonction sinus (connue de l'école) :*

(a) Est-ce que $\sin$ est bijectif ?

(b) Décrire l'image réciproque $\sin^{-1}(\{0\})$.

(c) Décrire l'image réciproque $\sin^{-1}(\{1\})$.

Exercice 4.10. *Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. Démontrer les assertions suivantes :*

(a) $g \circ f$ est injectif $\Rightarrow$ f est injectif.

(b) Si f et g sont tous les deux injectifs (respectivement surjectifs, respectivement bijectifs), alors $g \circ f$ est injectif (respectivement surjectif, respectivement bijectif).

Corrigé des exercices sur les fonctions

Exercice 4.7. Soient $A = \{1, 2, 3, 4, 5\}$ et $B = \{A, B, C, D\}$.

(a) Décrire une application surjective $f : A \to B$.

Par exemple : $f(1) = A$, $f(2) = B$, $f(3) = C$, $f(4) = D$, $f(5) = A$.

(b) Décrire une application de A dans B qui n'est ni surjective ni injective.

Par exemple : $f(1) = A$, $f(2) = A$, $f(3) = A$, $f(4) = A$, $f(5) = A$.

(c) Existe-t-il une application injective de A dans B ?

Non, car si une telle application injective f existait, nous aurions $\#\mathrm{Im}(f) = \#A = 5$ et $\mathrm{Im}(f) \subseteq B$, mais, B ne possède pas de sous-ensemble de cardinal 5 car $\#B = 4$, contradiction.

(d) Décrire une application injective $g : B \to A$.

Par exemple : $g(A) = 1$, $g(B) = 2$, $g(C) = 3$, $g(D) = 4$.

(e) Décrire une application de B dans A qui n'est ni surjective ni injective.

Par exemple : $g(A) = 1$, $g(B) = 1$, $g(C) = 1$, $g(D) = 1$.

(f) Existe-t-il une application surjective de B dans A ?

Non, car si $g : B \to A$ était surjective, alors on aurait $4 = \#B \geq \#A = 5$, contradiction.

Exercice 4.8.

(a) Trouver une application injective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.

Par exemple, $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$.

(b) Trouver une application surjective et non bijective de $\mathbb{N}$ dans $\mathbb{N}$.

Par exemple, $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto \begin{cases} \frac{n}{2} & \text{si } n \text{ est pair,} \\ 0 & \text{si } n \text{ est impair.} \end{cases}$

(c) Trouver une bijection entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.

Par exemple :

$$f(n) := \begin{cases} (n - m^2, m) & \text{si } m^2 \leq n \leq m^2 + m \text{ pour un } m \in \mathbb{N}, \\ (m, m^2 + 2m - n) & \text{si } m^2 + m + 1 \leq n \leq (m+1)^2 - 1 \text{ pour un } m \in \mathbb{N}. \end{cases}$$

On comprend cette application au mieux si on fait un petit dessin.

Exercice 4.9. Soit $\sin : \mathbb{R} \to [-1, 1]$ la fonction sinus (connue de l'école) :

(a) Est-ce que $\sin$ est bijectif ?

Non, car $\sin$ n'est pas injectif : par exemple $\sin(0) = \sin(\pi)$.

(b) Décrire l'image réciproque $\sin^{-1}(\{0\})$.

On a $\sin^{-1}(\{0\}) = \{n \cdot \pi \mid n \in \mathbb{Z}\}$.

(c) Décrire l'image réciproque $\sin^{-1}(\{1\})$.

On a $\sin^{-1}(\{1\}) = \{\frac{\pi}{2} + n \cdot 2\pi \mid n \in \mathbb{Z}\}$.

Exercice 4.10. Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. Démontrer les assertions suivantes :

(a) $g \circ f$ est injectif $\Rightarrow f$ est injectif.

Démonstration (de l'assertion contraposée). Supposons que f n'est pas injectif. Il existe donc $a_1, a_2 \in A$ tels que $a_1 \neq a_2$ et $f(a_1) = f(a_2)$. En conséquence, $g(f(a_1)) = g(f(a_2))$; cela montre que $g \circ f$ n'est pas injectif.

(b) Si f et g sont tous les deux injectifs (respectivement surjectifs, respectivement bijectifs), alors $g \circ f$ est injectif (respectivement surjectif, respectivement bijectif).

Démonstration. Supposons d'abord f, g injectifs et donnons-nous $a_1, a_2 \in A$ tels que $g(f(a_1)) = g(f(a_2))$. L'injectivité de g implique $f(a_1) = f(a_2)$. L'injectivité de f nous donne maintenant $a_1 = a_2$, montrant l'injectivité de $g \circ f$.

Supposons maintenant f, g surjectifs et donnons-nous $c \in C$. La surjectivité de g montre l'existence d'un $b \in B$ tel que $g(b) = c$. Maintenant la surjectivité de f implique l'existence de $a \in A$ tel que $f(a) = b$. Nous avons donc $g(f(a)) = g(b) = c$. Alors $g \circ f$ est surjectif.

Supposons finalement f, g bijectifs. Cela implique que f, g sont injectifs et surjectifs. Par ce que nous venons de voir, $g \circ f$ est injectif et surjectif, donc bijectif.

5 Relations binaires

Objectifs :

- Maîtriser la notion de relation binaire ;
- connaître et savoir démontrer des exemples de relations binaires.

On parle maintenant des relations à deux.
L'égalité dans $\mathbb{Q}$ définit un sous-ensemble de $\mathbb{Q} \times \mathbb{Q}$ comme suit :

$$\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x = y\} \subseteq \mathbb{Q} \times \mathbb{Q}.$$

Si on appelle cet ensemble S, alors, on a l'équivalence pour tout pair $x, y \in \mathbb{Q}$:

$$x = y \quad \Leftrightarrow \quad (x, y) \in S.$$

De la même manière, « $\leq$ » définit aussi un sous-ensemble de $\mathbb{Q}$:

$$\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x \leq y\} \subseteq \mathbb{Q} \times \mathbb{Q}.$$

L'égalité et le « plus petit ou égal à » sont des exemples de relations binaires (le mot « binaire » indique qu'il s'agit d'une relation entre deux objets). Nous allons maintenant formaliser cela.

Définition 5.1. *Soit E un ensemble ; on appelle* relation binaire sur E *toute partie R de l'ensemble $E \times E$.*

Vocabulaire 5.2. *Soient E un ensemble et R une relation binaire sur E. Pour un couple (x, y) de $E \times E$ tel que (x, y) appartient à R, on dit que x* et *y* sont en relation *et on note xRy ou $x \sim_R y$ (ou même $x \sim y$ si R est clair).*

Définitions 5.3. *Une relation binaire R sur un ensemble E est dite :*

- réflexive *si pour tout x dans E on a xRx ;*
- symétrique *si pour tout (x, y) dans $E \times E$ on a $(xRy \Rightarrow yRx)$;*
- antisymétrique *si pour tout (x, y) dans $E \times E$ on a $((xRy$ et $yRx) \Rightarrow x = y)$;*
- transitive *si pour tout (x, y, z) dans $E \times E \times E$ on a $((xRy$ et $yRz) \Rightarrow xRz)$;*
- totale *si pour tout (x, y) dans $E \times E$ on a $(xRy$ ou $yRx)$.*

Exemples 5.4.

(a) L'égalité sur un ensemble E est une relation réflexive, symétrique, antisymétrique, transitive ; elle est non totale dès que E a au moins 2 éléments.

(b) Soient E un ensemble et $\mathcal{P}(E)$ l'ensemble de ses sous-ensembles (appelés aussi parties*). La relation binaire R définie sur $\mathcal{P}(E)$ par $(ARB \Leftrightarrow A \subseteq B)$ est réflexive, transitive, antisymétrique ; elle est non symétrique dès que E est non vide et non totale dès que E a au moins 2 éléments.*

Nous allons rencontrer deux types de relations binaires : les relations d'ordre et les relations d'équivalence. Nous allons commencer par les premières.

Relations d'ordre

Définition 5.5. *Soit E un ensemble ; on appelle* relation d'ordre sur E *une relation binaire sur E qui est réflexive, transitive et antisymétrique.*

Exemples 5.6.

(a) L'égalité est une relation d'ordre.

(b) Sur l'ensemble des parties d'un ensemble, l'inclusion est une relation d'ordre (en générale non totale).

(c) Le « plus petit ou égal à $\leq$ » sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ est une relation d'ordre (totale).

Soient E un ensemble (non vide) et $\leq$ une relation d'ordre sur E.

Définition 5.7.

- *Un élément a de E est appelé* plus grand élément de E *s'il vérifie : $\forall x \in E, x \leq a$.*

- *Un élément a de E est appelé* plus petit élément de E *s'il vérifie :* $\forall x \in E, a \leq x$.

Remarque 5.8. *Le plus grand et plus petit élément d'un ensemble ordonné n'existent pas toujours, mais lorsqu'ils existent, ils sont uniques.*

Définition 5.9. *Soit A une partie de E.*

- *Un élément M de E qui vérifie :* $\forall x \in A, x \leq M$ *est appelé* un majorant de A.
- *Un élément m de E qui vérifie :* $\forall x \in A, m \leq x$ *est appelé* un minorant de A.

Vocabulaire 5.10. *Une partie qui possède un majorant (respectivement un minorant) est dite* majorée *(respectivement* minorée*).*

Relations d'équivalence

Définition et premiers exemples

Définition 5.11. *Soit E un ensemble ; on appelle* relation d'équivalence sur E *une relation binaire sur E qui est réflexive, symétrique et transitive.*

Exemples 5.12.

(a) L'égalité sur un ensemble est une relation d'équivalence.

(b) Soit E l'ensemble de tous les étudiants à l'UL. Pour $x, y \in E$ on définit $x \sim y$ si les étudiants x et y étudient dans le même programme. [On suppose ici qu'un étudiant n'étudie que dans un seul programme.]

(c) Soit E l'ensemble de tous les étudiants de ce cours. Pour $x, y \in E$ on définit $x \sim y$ si les étudiants x et y ont le même sexe.

(d) Sur l'ensemble des droites affines du plan, le parallélisme est une relation d'équivalence.

(e) Soient E et F des ensembles et f une application de E dans F. La relation binaire R_f définie sur E par

$$\forall (x, y) \in E^2, (xR_f y \Leftrightarrow f(x) = f(y))$$

est une relation d'équivalence. On l'appelle relation d'équivalence associée à f.

Classes d'équivalence et ensemble quotient

Soient E un ensemble (non-vide) et R une relation d'équivalence sur E fixés.

Définition 5.13. *(a) Soit x dans E ; on appelle* classe d'équivalence de x (pour la relation R) *le sous-ensemble $\{y \in E \mid xRy\}$ de E ; on le note $\bar{x}$.*

(b) Soit ω une classe d'équivalence de E ; tout élément x dans ω est appelé un représentant *de ω.*

(c) L'ensemble des classes d'équivalence de E pour la relation R est appelé ensemble quotient de E par R *; on le note E/R.*

Remarque 5.14. *Les éléments de l'ensemble E/R sont des classes d'équivalences ; ce sont donc eux-mêmes des ensembles (plus précisément, des sous-ensembles de E) !*

Exemples 5.15. *(a) Pour l'égalité sur un ensemble E, on a : $\bar{x} = \{x\}$.*

(b) Pour la relation d'avoir le même sexe pour les étudiants de ce cours, il n'existe que deux classes d'équivalences : celle des hommes et celles des femmes. Chaque homme dans ce cours est un représentant de la classe d'équivalence des hommes.

(c) Chaque étudiant de ce cours est un représentant de la classe d'équivalence « BASI filière mathématiques » pour la relation d'étudier dans le même programme.

(d) Soient E et F des ensembles et f une application de E dans F. Pour la relation d'équivalence R_f, la classe d'un élément x de E est :

$$\bar{x} = \{y \in E \mid f(y) = f(x)\} = f^{-1}(\{f(x)\}).$$

C'est « l'image réciproque de l'image de x ».

Proposition 5.16. *(a) Les classes d'équivalence de E sont toutes non vides et tout élément de E appartient à une et une seule classe d'équivalence (la sienne !).*

(b) Soient $x, y \in E$. Alors :

$$x \in \overline{y} \quad \Leftrightarrow \quad y \in \overline{x}.$$

(c) Soient $x, y \in E$. Si $y \in \overline{x}$, alors $\overline{y} = \overline{x}$.

(d) Soient x et y dans E. Alors on a : $xRy \Leftrightarrow \bar{x} = \bar{y}$.

(e) Soit $\overline{x}$ et $\overline{y}$ deux classes d'équivalence. Si $\overline{x} \cap \overline{y} \neq \emptyset$, alors $\overline{x} = \overline{y}$.

(f) L'ensemble des classes d'équivalences forme une partition *de E, c'est-à-dire :*

$$E = \bigsqcup_{\omega \in E/R} \omega.$$

(Rappelons que $\bigsqcup$ signifie la « réunion disjointe ».)

Démonstration. (a) Tout élément $x \in E$ appartient à la classe $\overline{x}$ par la réflexivité de la relation. Par définition, toute classe d'équivalence est de la forme $\overline{x}$, alors elle n'est pas vide.
(b) Nous avons les équivalences :

$$x \in \overline{y} \overset{\text{déf}}{\Leftrightarrow} yRx \overset{\text{symétrie}}{\Leftrightarrow} xRy \overset{\text{déf}}{\Leftrightarrow} y \in \overline{x}.$$

(c) Nous avons par définition $y \sim_R x$, et donc par la symétrie $x \sim_R y$. Prenons $y_1 \in \overline{y}$, donc $y \sim_R y_1$. La transitivité nous donne $x \sim_R y_1$; alors $y_1 \in \overline{x}$. Ceci montre $\overline{y} \subseteq \overline{x}$. Par (b) nous avons aussi $x \in \overline{y}$ et les mêmes arguments montrent $\overline{x} \subseteq \overline{y}$. Nous obtenons donc l'égalité $\overline{x} = \overline{y}$.
(d) « $\Leftarrow$ » est triviale. Pour « $\Rightarrow$ » on utilise (c).
(e) Soit $z \in \overline{x} \cap \overline{y}$, donc $z \in \overline{x}$ et $z \in \overline{y}$. Par (c) nous avons $\overline{z} = \overline{x}$ et $\overline{z} = \overline{y}$, donc $\overline{x} = \overline{y}$.
(f) et une conséquence directe de (a)–(e) : Il faut montrer

(1) que l'on a $E = \bigcup_{\omega \in E/R} \omega$ et

(2) que cette réunion est disjointe.

(1) est l'assertion (a) : tout élément de E appartient à une classe d'équivalence.
(2) est l'assertion (e) : deux classes d'équivalences sont soit les mêmes, soit disjointes. □

Proposition 5.17. *L'application de E dans E/R qui à tout élément x de E associe sa classe $\overline{x}$ est surjective ; on l'appelle* surjection canonique *de E dans E/R.*

En mathématiques, l'adjectif *canonique* est utilisé pour désigner un objet ou une construction naturelle, souvent définis de manière unique.

Démonstration. Appelons l'application s. Si $\overline{x}$ est une classe d'équivalence, alors $s(x) = \overline{x}$. Donc, on obtient la surjectivité. □

Factorisation canonique d'une application

Nous allons maintenant considérer un des exemples plus en détails. Soient E et F des ensembles et f une application de E dans F.

Vocabulaire 5.18. *Soient E un ensemble et A une partie de E ; on appelle* injection canonique de A dans E *l'application de A dans E qui envoie tout élément x de A sur x lui-même (vu comme élément de E).*

On note ici i l'injection canonique de $f(E)$ dans F et s la surjection canonique de E dans E/R_f.

Théorème 5.19. *Il existe une unique application bijective $\overline{f}$ de E/R_f dans $f(E)$ qui vérifie : $f = i \circ \overline{f} \circ s$.*

La relation vérifiée par les fonctions f, i, s et $\overline{f}$ peut s'écrire de manière compacte en disant que le *diagramme* suivant *commute*.

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle s}\downarrow & \circlearrowleft & \uparrow{\scriptstyle i} \\ E/R_f & \xrightarrow[\bar{f}]{\sim} & f(E) \end{array}$$

En règle générale, on note les applications surjectives par une flèche avec deux pointes $\twoheadrightarrow$, celles qui sont injectives par la flèche $\hookrightarrow$, et les bijections par une tilde au-dessus de la flèche $\xrightarrow{\sim}$.

Démonstration.

Unicité On considère deux applications, $\hat{f}$ et $\tilde{f}$ qui satisfont le théorème et on cherche à démontrer qu'elles sont égales.

Soient ω dans E/R_f une classe d'équivalence et x dans E un représentant de ω (c'est-à-dire qu'on a : $\omega = \overline{x} = s(x)$). Comme $\hat{f}$ et $\tilde{f}$ vérifient l'égalité $f = i \circ \hat{f} \circ s = i \circ \tilde{f} \circ s$, on a :

$$i\left(\hat{f}(\omega)\right) = i\left(\hat{f}(s(x))\right) = f(x) = i\left(\tilde{f}(s(x))\right) = i\left(\tilde{f}(\omega)\right).$$

Comme l'application i est injective, on en déduit : $\hat{f}(\omega) = \tilde{f}(\omega)$. Ceci étant valable pour toute classe ω dans E/R_f, on en conclut que $\hat{f}$ et $\tilde{f}$ sont égales.

Existence Soient ω dans E/R_f une classe d'équivalence et x dans E un représentant de ω. On pose $\overline{f}(\omega) = f(x)$.

Nous devons vérifier qu'on a bien construit ainsi une fonction $\overline{f}$, c'est-à-dire que la classe ω a une *unique* image par $\overline{f}$. Cette vérification est nécessaire car on a à priori défini $\overline{f}(\omega)$ à partir du choix d'un représentant x de ω, et pas seulement de ω lui-même.

Soit donc x' un autre représentant de la classe ω, c'est-à-dire qu'on a $x' \in \omega$ ou encore xR_fx'. Alors, par définition de la relation R_f, on a $f(x) = f(x')$. L'image de ω par $\overline{f}$ est donc bien définie (de manière unique). On dit que l'application f est « bien définie ».

On devra effectuer ce genre de vérification chaque fois qu'on veut définir une application sur un ensemble quotient.

L'application $\overline{f}$ est définie sur E/R_f et à valeurs dans $f(E)$. Nous allons démontrer qu'elle vérifie les propriétés du théorème.

Relation $f = i \circ \overline{f} \circ s$ Soit x dans E. Alors x est un représentant de sa classe d'équivalence $s(x)$ et on a par définition de $\overline{f}$: $(i \circ \overline{f} \circ s)(x) = i\left(\overline{f}(s(x))\right) = i\left(f(x)\right) = f(x)$.

Injectivité Soient ω et ω' des classes dans E/R_f vérifiant : $\overline{f}(\omega) = \overline{f}(\omega')$. Soient x un représentant de ω et x' un représentant de ω'. Alors on a : $f(x) = \overline{f}(\omega) = \overline{f}(\omega') = f(x')$. Ainsi, on a xR_fx', et donc $\omega = \overline{x} = \overline{x'} = \omega'$.

Surjectivité Soit y dans $f(E)$. Il existe x dans E vérifiant $y = f(x)$. Alors on a $y = f(x) = \overline{f}(s(x))$, donc y est dans l'image de $\overline{f}$.

□

Ainsi, toute application peut s'écrire comme composée d'une surjection, d'une bijection et d'une injection.

Chapitre II

Systèmes de nombres et structures algébriques

6 Les entiers naturels $\mathbb{N}$

Objectifs :

- Maîtriser les axiomes de Peano qui définissent les entiers naturels ;
- connaître la définition de l'addition, de la multiplication et de la relation d'ordre sur les entiers naturels ;
- savoir démontrer des propriétés simples ;
- maîtriser la notion de cardinal d'un ensemble.

Le but de cette section est d'esquisser la construction des nombres naturels. Jusqu'ici nous avons traité les entiers comme « connus (de l'école) ». Un des grands achèvements des mathématiques est de baser toutes les mathématiques sur une axiomatique fondamentale et de tout démontrer en partant des axiomes.
Pour vous en donner une idée, nous introduisons les axiomes de Peano qui définissent les nombres naturels. Par contre, nous n'avons pas le temps de donner toutes les démonstrations des propriétés « bien connues ».

Les axiomes de Peano

Essayons maintenant d'oublier tout ce que nous savons sur les entiers naturels. Nous allons les définir de façon axiomatique et ensuite dériver toutes les propriétés « habituelles » en n'utilisant que les axiomes. Dans cette section il faut donc toujours justifier les règles de calculs par les axiomes ou des assertions déjà dérivées à partir des axiomes.

Définition 6.1. *On appelle* système des nombres naturels *tout triplet* $(N, S, 0)$ *consistant d'un ensemble* N*, d'une application* $S : N \to N$ *et d'un élément* $0 \in N$ *qui satisfait les trois axiomes (appelés* axiomes de Peano*) :*

(PA1) $0 \notin S(N)$,

(PA2) S *est injective,*

(PA3) $\forall\, M \subseteq N : \big(0 \in M \wedge (n \in M \Rightarrow S(n) \in M) \Rightarrow M = N\big)$.

L'application S est appelée *application de successeur*. L'idée est « $S(n) = n+1$ » (mais nous n'avons pas encore l'addition !). Juste pour montrer qu'il existe beaucoup de systèmes de nombres naturels, on mentionne qu'après avoir fait tout ce qui suit, on peut voir qu'un système des nombres naturels est par exemple donné par $(\{0, -1, -2, -3, \ldots\}, S, 0)$ avec $S(n) = n - 1$.

Théorème 6.2. *Dans l'axiomatique de la théorie des ensembles de Zermelo-Fraenkel, il existe un système des nombres naturels.*

Démonstration. Comme nous n'avons pas introduit les axiomes de Zermelo-Fraenkel, nous ne pouvons pas démontrer ce théorème et nous référons par exemple au livre de Schichl/Steinbauer, Section 6.1.1.
L'idée derrière la construction est la suivante :

- On pose $0 := \emptyset$.
- Pour $0 \neq n \in N$, on pose $S(n) = n \cup \{n\}$, la réunion de n (qui est un ensemble !) et l'ensemble dont le seul élément est l'ensemble n.

Plus explicitement :

$$0 = \emptyset,\ \ 1 = \{\emptyset\},\ \ 2 = \{\emptyset, \{\emptyset\}\},\ \ 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \text{etc.}$$

□

A partir des axiomes de Peano nous démontrons maintenant le principe de récurrence que nous avons déjà utilisé (avec la phrase pas très convainquante « On s'en convainc que... »). Nous mettons donc les mathématiques que nous utilisons sur des fondations plus solides.

Proposition 6.3 (Principe de récurrence)**.** *Soit* $(N, S, 0)$ *un système des nombres naturels. Soit* $A(n)$ *une assertion dépendant de* n *dans* N*. Alors :*

$$(A(0) \wedge (\forall n \in N, A(n) \Rightarrow A(S(n)))) \Rightarrow (\forall\, n \in N, A(n)).$$

Démonstration. Nous définissons l'ensemble des nombres naturels pour lesquels l'assertion $A(n)$ est vraie :

$$V := \{n \mid n \in N, A(n)\}.$$

C'est un sous-ensemble de N. On a $0 \in V$ parce que $A(0)$ est vraie. Si $n \in V$, alors par définition $A(n)$ est vraie, donc $A(S(n))$ est vraie et en conséquence $S(n) \in V$. L'axiome (PA3) implique donc $V = N$, c'est-à-dire $A(n)$ est vraie pour tout $n \in N$. □

Lemme 6.4. *Soit* $(N, S, 0)$ *un système des nombres naturels. Alors,* $S(N) = N \backslash \{0\}$ *(tout* $n \in N \backslash \{0\}$ *est le successeur d'un élément dans* N*).*

Démonstration. Nous posons $M := S(N) \cup \{0\}$. C'est un sous-ensemble de N qui contient 0. Pour tout $m \in M$, on a $S(m) \in S(N) \subset M$. L'axiome (PA3) implique donc $M = N$. Comme (PA1) nous assure $0 \notin S(N)$, nous trouvons $S(N) = N \setminus \{0\}$. □

Lemme 6.5. *Soit $(N, S, 0)$ un système des nombres naturels. Alors, pour tout $n \in N$ nous avons $n \neq S(n)$.*

Démonstration. Exercice. □

La suite sert à justifier les définitions récursives. On commence par les parties initiales (il faut se les imaginer comme $\{0, 1, 2, \ldots, n\}$).

Définition 6.6. *Soit $(N, S, 0)$ un système des nombres naturels. Un sous-ensemble $I \subseteq N$ est appelé* partie initiale *si pour tout $i \in N$*

$$i \notin I \Rightarrow S(i) \notin I$$

ou équivalant : $S(i) \in I \Rightarrow i \in I$.

Lemme 6.7. *Soit $(N, S, 0)$ un système des nombres naturels.*

(a) Soit $\emptyset \neq I \subseteq N$ une partie initiale. Alors $0 \in I$.

(b) Pour tout $n \in N$ il existe une partie initiale I_n telle que $n \in I_n$ et $S(n) \notin I_n$ et satisfaisant $I_0 = \{0\}$ et $I_{S(n)} = I_n \sqcup \{S(n)\}$ pour tout $n \in N$. (Il faut s'imaginer I_n comme $\{0, 1, 2, \ldots, n-1, n\}$.)

(c) $\bigcup_{n \in N} I_n = N$.

Démonstration. (a) Supposons le contraire : $0 \notin I$. Soit $C := N \setminus I$ le complément. On a $0 \in C$ et $n \in C \Rightarrow S(n) \in C$, donc $C = N$ par l'axiome (PA3), donc $I = \emptyset$, contradiction.
(b) Par récurrence. Soit $A(n)$ l'assertion de l'existence d'une partie initiale I_n avec $n \in I_n$ et $S(n) \notin I_n$.

Initialisation : Pour $n = 0$ on pose $I_0 = \{0\}$. Evidemment $0 \in I_0$ et $S(0) \notin I_0$. En plus, I_0 est une partie initiale car (PA1) nous assure que 0 n'est pas dans $S(N)$.

Hérédité : « $A(n) \Rightarrow A(S(n))$ » : On pose $I_{S(n)} := I_n \cup \{S(n)\}$. La réunion est en fait disjointe car $S(n) \in I_n$ contredirait $A(n)$. Il est clair que $S(n) \in I_{S(n)}$. En plus, $I_{S(n)}$ est une partie initiale : si $S(m) \in I_n$, alors $m \in I_n \subset I_{S(n)}$ car I_n est une partie initiale ; si $S(m) = S(n)$, alors $m = n \in I_n \subset I_{S(n)}$.

Il reste à voir que $S(S(n)) \notin I_{S(n)}$. Supposons le contraire : $S(S(n)) \in I_{S(n)}$. Comme l'injectivité de S (PA2) exclut $S(S(n)) = S(n)$ à cause du lemme 6.5, on suppose $S(S(n)) \in I_n$; alors, comme I_n est une partie initiale, on aurait $S(n) \in I_n$, contradiction avec l'hypothèse $A(n)$.

Conclusion : Pour tout $n \in N$ l'assertion $A(n)$ est vraie, donc la partie (b) est vraie.

La deuxième assertion résulte de la construction.
(c) L'inclusion « $\subseteq$ » est triviale. L'inclusion « $\supseteq$ » résulte de $n \in I_n$. □

Pour la suite, vous pouvez penser à l'exemple suivant : $E = \mathbb{R}$, $e = 2$ et $g(x) = x^2$; cela donne lieu à la définition récursive suivante :

$$f(0) = 2 \text{ et pour } n \in \mathbb{N} : f(n+1) = (f(n))^2$$

ou en notation de suites

$$a_0 = 2 \text{ et pour } n \in \mathbb{N} : a_{n+1} = (a_n)^2.$$

Proposition 6.8. *[Définitions récursives] Soit $(N, S, 0)$ un système des nombres naturels. Soient E un ensemble, $e \in E$ et $g : E \to E$ une application. Alors, il existe une unique application $f : N \to E$ telle que $f(0) = e$ et pour tout $n \in N$, $f(S(n)) = g(f(n))$.*

Démonstration. Par récurrence, nous allons démontrer l'assertion suivante :

$$A(n) : \ \exists f_n : I_n \to E : \ f_n(0) = e \wedge \big(\forall\, m \in N : (S(m) \in I_n \Rightarrow f_n(S(m)) = g(f_n(m))\big).$$

Initialisation : Pour $n = 0$ on pose $f_0(0) = e$. L'existence est donc claire car $I_0 = \{0\}$.

Hérédité : « $A(n) \Rightarrow A(S(n))$ » : On se rappelle que $I_{S(n)} = I_n \sqcup \{S(n)\}$. On pose

$$f_{S(n)}(m) := \begin{cases} f_n(m) & \text{si } m \in I_n, \\ g(f_n(n)) & \text{si } m = S(n). \end{cases}$$

Il faut vérifier les propriétés :

- $f_{S(n)}(0) = f_n(0) = e$ par l'hypothèse de récurrence.
- Soit $m \in N$ tel que $S(m) \in I_{S(n)}$. Pour $m = n$, on a $f_{S(n)}(S(n)) = g(f_n(n)) = g(f_{S(n)}(n))$ par définition. Pour $m \neq n$, on a $f_{S(n)}(S(m)) = f_n(S(m)) = g(f_n(m)) = g(f_{S(n)}(m))$ par l'hypothèse de récurrence.

Nous allons maintenant définir l'application f pour $n \in N$ comme

$$f(n) := f_n(n).$$

Elle satisfait

- $f(0) = f_0(0) = e$,
- pour $n \in N$ on a $f(S(n)) = f_{S(n)}(S(n)) = g(f_n(n)) = g(f(n))$.

Nous avons montré l'existence à cause de $N = S(N) \cup \{0\}$ (lemme 6.4). Pour l'unicité on suppose que $\widetilde{f}$ est une deuxième application avec les mêmes propritétés que f. On considère l'ensemble

$$V := \{n \mid n \in N, f(n) = \widetilde{f}(n)\}.$$

Nous avons $0 \in V$ et si $n \in V$, alors $S(n) \in V$, parce que

$$f(S(n)) = g(f(n)) = g(\widetilde{f}(n)) = \widetilde{f}(S(n)),$$

donc par (PA3) $V = N$, montrant l'unicité. □

Proposition 6.9. *Si $(N, S, 0)$ et $(N', S', 0')$ sont des systèmes des nombres naturels, alors il existe une bijection $\varphi : N \to N'$ telle que $\varphi(0) = 0'$ et $\varphi \circ S = S' \circ \varphi$.*

Démonstration. Exercice. □

A cause de l'unicité dans la proposition 6.9, nous allons parler *des nombres naturels* et nous les notons $(\mathbb{N}, S, 0)$. Plus tard, nous n'allons qu'écrire $\mathbb{N}$.

Addition et multiplication

Nous définissons maintenant l'addition sur $(\mathbb{N}, S, 0)$.

Proposition 6.10. *Il existe une unique application*

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (m, n) \mapsto f(m, n) =: m + n$$

(noter que $m + n$ n'est qu'une façon d'écrire $f(m, n)$) telle que

(A1) $\forall\, m \in \mathbb{N} : m = f(m, 0) = m + 0$,

(A2) $\forall\, m \in \mathbb{N}, \forall\, n \in \mathbb{N} : m + S(n) = f(m, S(n)) = S(f(m, n)) = S(m + n)$.

Démonstration. Soit $m \in \mathbb{N}$. La proposition 6.8 nous permet de définir l'application $f_m : \mathbb{N} \to \mathbb{N}$ récursivement par

$$f_m(0) := m \text{ et pour } n \in \mathbb{N} : \ f_m(S(n)) := S(f_m(n)).$$

Pour finir la preuve, nous posons $f(m, n) := f_m(n)$. Les deux propriétés sont satisfaites par construction.
On montre l'unicité. Supposons que nous avons deux fonctions f, f' ayant les propriétés de f. Nous définissons $f_m(n) := f(m, n)$ et $f'_m(n) := f'(m, n)$. Les propriétés (A1) et (A2) donnent $f_m(0) = m = f'_m(0)$ et $f_m(S(n)) = S(f_m(n))$ et $f'_m(S(n)) = S(f'_m(n))$. L'unicité dans la proposition 6.8 montre $f_m = f'_m$, donc $f = f'$. □

A cause de la proposition, nous pouvons maintenant écrire

$$S(n) = S(f(n, 0)) = f(n, S(0)) = n + 1$$

avec $1 = S(0)$ (évidemment, on écrit $2 = S(1)$, $3 = S(2)$, etc.).

Proposition 6.11. *L'addition sur $(\mathbb{N}, S, 0)$ satisfait les propriétés suivantes. Pour tout $m, n, \ell \in \mathbb{N}$ on a*

(a) élément neutre : $m + 0 = m = 0 + m$;

(b) commutativité : $m + n = n + m$;

(c) associativité : $(m + n) + \ell = m + (n + \ell)$;

(d) $\ell + n = m + n \Rightarrow \ell = m$;

(e) $m+n=0 \Leftrightarrow m=0 \wedge n=0$.

Démonstration. (a) $m+0=m$ est vrai par définition. L'égalité $m=0+m$ se démontre par récurrence. [Attention : nous ne connaissons pas encore la commutativité. C'est pour cela que l'assertion n'est pas triviale, mais nécessite une démonstration.]

Initialisation : $0+0=f(0,0)=0$.

Hérédité : « $m \Rightarrow m+1$ » : $0+(m+1) \overset{(A2)}{=} (0+m)+1 = m+1$ où la dernière égalité utlise l'hypothèse de récurrence.

(b) On démontre d'abord :

$$(*) \quad \forall\, m,n \in \mathbb{N}: \ (m+1)+n=(m+n)+1.$$

Soit $m \in \mathbb{N}$. Récurrence pour $n \in \mathbb{N}$:

Initialisation : $(m+1)+0 \overset{(A1)}{=} m+1 \overset{(A1)}{=} (m+0)+1$.

Hérédité : « $n \Rightarrow n+1$ » : $(m+1)+(n+1) \overset{(A2)}{=} ((m+1)+n)+1 \overset{\text{hyp.réc.}}{=} ((m+n)+1)+1 \overset{(A2)}{=} (m+(n+1))+1$.

On démontre maintenant la commutativité aussi par récurrence pour $n \in \mathbb{N}$ avec $m \in \mathbb{N}$ fixé.

Initialisation : $m+0=0+m$ par (a).

Hérédité : « $n \Rightarrow n+1$ » : $m+(n+1) \overset{(A2)}{=} (m+n)+1 \overset{\text{hyp.réc.}}{=} (n+m)+1 \overset{(*)}{=} (n+1)+m$.

(c) Exercice.
(d) Récurrence pour n.

Initialisation : $m+0=\ell+0$ donne $m=\ell$ à cause de (a).

Hérédité : « $n \Rightarrow n+1$ » : Supposons $m+(n+1)=\ell+(n+1)$. Par (A2) on a $(m+n)+1=(\ell+n)+1$. Comme S est injective (PA2), on déduit $m+n=\ell+n$ et par l'hypothèse de récurrence $m=\ell$.

(e) L'implication $\Leftarrow$ est claire. Supposons donc $m+n=0$ et faisons une démonstration par l'absurde. Pour cela on suppose (sans perte de généralité à cause de la commutativité de (b)) $n \neq 0$. Donc $n=\ell+1$ pour un $\ell \in \mathbb{N}$. En conséqence $0=m+n=m+(\ell+1) \overset{(A2)}{=} (m+\ell)+1=S(m+\ell)$ ce qui contredit $0 \notin S(N)$ (PA1). □

De façon similaire on définit une multiplication sur $\mathbb{N}$.

Proposition 6.12. *Il existe une unique application (appelée* multiplication*)*

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (m,n) \mapsto g(m,n) =: m \cdot n$$

(noter que $m \cdot n$ n'est qu'une façon d'écrire $g(m,n)$) telle que

(M1) $\forall\, m \in \mathbb{N}: 0=g(m,0)=m \cdot 0$,

(M2) $\forall\, m \in \mathbb{N}, \forall\, n \in \mathbb{N} : m \cdot (n+1) = m \cdot S(n) = g(m,n) + m = m \cdot n + m$.

Esquisse de la démonstration. Soit $m \in \mathbb{N}$. La proposition 6.8 nous permet de définir l'application $g_m : \mathbb{N} \to \mathbb{N}$ récursivement par

$$g_m(0) := 0 \text{ et pour } n \in \mathbb{N} : \; g_m(S(n)) := g_m(n)) + m.$$

Pour finir la preuve, nous posons $g(m,n) := g_m(n)$. Les deux propriétés sont satisfaites par construction. L'unicité se montre comme dans le cas de l'addition. □

Proposition 6.13. *La multiplication sur* $(\mathbb{N}, S, 0)$ *satisfait les propriétés suivantes.*
Pour tout $m, n, \ell \in \mathbb{N}$ *on a*

(a) élément neutre : $m \cdot 1 = m = 1 \cdot m$ *;*

(b) commutativité : $m \cdot n = n \cdot m$ *;*

(c) associativité : $(m \cdot n) \cdot \ell = m \cdot (n \cdot \ell)$ *;*

(d) $\ell \cdot n = m \cdot n \Rightarrow \ell = m \vee n = 0$ *;*

(e) intégrité : $m \cdot n = 0 \Rightarrow m = 0 \vee n = 0$ *;*

(f) distributivité : $(m+n) \cdot \ell = m \cdot \ell + n \cdot \ell$.

Démonstration. Similaire à la démonstration de la proposition 6.11. □

La relation d'ordre

Définition 6.14. *Soient* $m, n \in \mathbb{N}$. *On appelle* m plus petit ou égal à n *(*$m \leq n$*) s'il existe* $d \in \mathbb{N}$ *tel que* $m + d = n$.
L'entier naturel d *est appelé* la différence de n et m.

Lemme 6.15. *(a)* $\forall\, n \in \mathbb{N} : 0 \leq n$ *;*

(b) $\forall\, n \in \mathbb{N} : (n = 0 \vee 1 \leq n)$.

(c) $\forall\, n, m \in \mathbb{N} : (n \leq m \leq n+1 \Rightarrow n = m \vee m = n+1)$.

Démonstration. (a) Cela est vrai car $0 + n = n$.
(b) Supposons $n \leq 1$, alors il existe $d \in \mathbb{N}$ tel que $n + d = 1$. Si $d = 0$, alors $n = 1$. Si $d \neq 0$, alors $d = d' + 1$, donc $n + d' + 1 = 1$ et en conséquence $n + d' = 0$, alors $n = 0$ par la proposition 6.11 (d).
(c) $n \leq m$ implique l'existence de $d \in \mathbb{N}$ tel que $m = n + d$, donc $n \leq n + d \leq n + 1$, dont on déduit l'existence de $e \in \mathbb{N}$ tel que $n + d + e = n + 1$. La proposition 6.11 (d) nous donne $d + e = 1$, alors $d \leq 1$. La partie (b) implique $d = 0 \vee 1 \leq d$, donc $d = 0$ ou $d = 1$. □

Proposition 6.16. *La relation* $\leq$ *sur* $\mathbb{N}$ *est une relation d'ordre qui est totale. Elle satisfait en plus*

$$\ell \leq m \Rightarrow \forall\, n \in \mathbb{N} : (\ell + n \leq m + n \wedge \ell \cdot n \leq m \cdot n).$$

Démonstration. Nous démontrons uniquement la totalité. Soit $n \in \mathbb{N}$. Considérons l'ensemble

$$M = \{m \mid m \in \mathbb{N}, (n \leq m) \vee (m \leq n)\}.$$

A cause du lemme 6.15(a), nous avons $0 \in M$. Supposons maintenant $m \in M$. Si $n \leq m$, alors $n+d = m$ pour un $d \in \mathbb{N}$ et donc $n+(d+1) = m+1$ d'où $n \leq m+1$, alors $m+1 \in M$. Si $m \leq n$ et $m \neq n$, alors $m+d = n$ avec $d \in \mathbb{N}$ et $d \neq 0$, donc $d = d'+1$, d'où $m+(d'+1) = (m+1)+d' = n$, alors $m+1 \leq n$ et $m+1 \in M$. Par (PA3) nous trouvons $M = \mathbb{N}$.
Les autres assertions se vérifient facilement ; nous ne donnons pas les détails ici. C'est un exercice instructif. □

La relation d'ordre nous permet de démontrer que $\mathbb{N}$ est *bien ordonné*.

Proposition 6.17 ($\mathbb{N}$ est bien ordonné)**.** *Toute partie M non vide de $\mathbb{N}$ possède un plus petit élément.*

Démonstration. Par récurrence. Soit $A(n)$ l'assertion : « toute partie $M \subseteq \mathbb{N}$ telle que $n \in M$ possède un plus petit élément ».

Initialisation : $A(0)$ est vraie car 0 est le plus petit élément de $\mathbb{N}$ par le lemme 6.15.

Hérédité : « $(\forall\, m \leq n : A(m)) \Rightarrow A(n+1)$ » : On distingue deux cas.
1er cas : Il existe $m \in M$ tel que $m \leq n$. Dans ce cas, $A(m)$ donne le résultat.
2ème cas : Il n'existe pas $m \in M$ tel que $m \leq n$. Alors par le lemme 6.15, $n+1 \in M$ est le plus petit élément de M.

□

En fait, on peut aussi déduire le principe de récurrence de la proposition 6.17 comme suit :

> On suppose que les assertions $A(0)$ et $(\forall n \in \mathbb{N}, A(n) \Rightarrow A(n+1))$ sont vraies ; on veut démontrer que, pour tout n dans $\mathbb{N}$, l'assertion $A(n)$ est vraie. On suppose par l'absurde que ce n'est pas le cas.
>
> La négation de $(\forall n \in \mathbb{N}, A(n))$ est : il existe n dans $\mathbb{N}$ pour lequel l'assertion $A(n)$ est fausse. On considère alors l'ensemble $\mathcal{A}$ des entiers naturels m tels que l'assertion $A(m)$ est fausse. Par hypothèse, l'ensemble $\mathcal{A}$ est non vide. Comme $\mathbb{N}$ est bien ordonné, $\mathcal{A}$ possède un plus petit élément ; notons le m_0. On remarque que, comme m_0 appartient à $\mathcal{A}$, l'assertion $A(m_0)$ est fausse.
>
> Comme $A(0)$ est vraie, $\mathcal{A}$ ne contient pas 0, donc m_0 est non nul. On peut donc considérer l'entier naturel $m_0 - 1$, qui est strictement inférieur à m_0 ; comme tous les éléments de $\mathcal{A}$ sont plus grands que m_0, l'entier $m_0 - 1$ n'appartient pas a $\mathcal{A}$. Ainsi, la propriété $A(m_0 - 1)$ est vraie. Alors, la propriété $A(m_0 - 1 + 1) = A(m_0)$ est vraie. On obtient une contradiction.

La propriété de bon ordre de $\mathbb{N}$ a également les deux conséquences suivantes.

Proposition 6.18. *Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.*

Démonstration. Soit $\mathcal{A}$ une partie non vide et majorée de $\mathbb{N}$.
On considère l'ensemble $\mathcal{M}$ des majorants de $\mathcal{A}$, c'est-à-dire l'ensemble :

$$\mathcal{M} = \{m \in \mathbb{N} \mid \forall a \in \mathcal{A}, a \leq m\}.$$

Par hypothèse ($\mathcal{A}$ est majorée), la partie $\mathcal{M}$ est non vide.
Soit m_0 le plus petit élément de $\mathcal{M}$. Si m_0 est dans $\mathcal{A}$, alors c'est le plus grand élément de $\mathcal{A}$.
On suppose par l'absurde que m_0 n'est pas dans $\mathcal{A}$. Alors pour tout a dans $\mathcal{A}$ ($\mathcal{A}$ est non vide), on a $a \leq m_0$ et $a \neq m_0$, donc $a < m_0$ et par suite $a \leq m_0 - 1$. Ainsi, l'entier $m_0 - 1$ est aussi un majorant de $\mathcal{A}$; il appartient donc à $\mathcal{M}$, ce qui contredit le choix de m_0 comme plus petit élément de $\mathcal{M}$. □

Lemme 6.19. *Pour tout $n \in \mathbb{N}$, nous avons $I_n = \{m \mid m \in \mathbb{N}, m \leq n\}$.*

Démonstration. « $\subseteq$ » : Considérons l'ensemble $M = I_n \cap \{m \mid m \in \mathbb{N}, m > n\}$. Si $M \neq \emptyset$, alors M possède un plus petit élément x. Comme $n+1 \notin I_n$, on a $x > n+1$ et $x = y+1$ avec $y \in \mathbb{N}$ et $y > n$. Le fait $y + 1 \in I_n$ implique $y \in I_n$ car I_n est une partie initiale. On trouve $y \in M$, contradiction car $y < x$ et x est le plus petit élément de M. Donc, M est l'ensemble vide et $I_n \subseteq \{m \mid m \in \mathbb{N}, m \leq n\}$.
« $\supseteq$ » : Considérons l'ensemble $M = \{m \mid m \in \mathbb{N}, m \leq n\} \setminus I_n$. C'est un ensemble majoré. Supposons M non-vide. Donc M possède un plus grand élément x ; on a $x \leq n$ et $x \notin I_n$. En fait, $x < n$ car $n \in I_n$. En conséquence, $x + 1 \notin I_n$ car I_n est une partie initiale et $x + 1 \leq n$. On trouve $x + 1 \in M$. Cela contradit la maximalité de x. Donc M est l'ensemble vide et $\{m \mid m \in \mathbb{N}, m \leq n\} \subseteq I_n$. □

Nous avons donc pour tout $n, m \in \mathbb{N}$:

$$n \leq m \Leftrightarrow I_n \subseteq I_m.$$

À partir des entiers naturels $\mathbb{N}$ et de relations d'équivalence sur des ensembles bien choisis, on construira dans la suite du cours les entiers relatifs $\mathbb{Z}$ et les nombres rationnels $\mathbb{Q}$ avec leurs propriétés usuelles.
Nous sommes à présent plus sûrs des fondations, et à partir de maintenant, nous allons travailler avec les nombres naturels comme nous l'avons toujours fait.

Le cardinal d'un ensemble

Soit E un ensemble. Nous avons déjà introduit le symbole $\#E$ pour noter le nombre d'éléments de E. Nous allons formaliser cette notion.

Définition 6.20. *Pour tout $n \in \mathbb{N}$ on note $E_n := I_n \setminus \{0\} = \{1, 2, \ldots, n\}$, en particulier, $E_0 = \emptyset$.*
Soit E un ensemble. Il est appelé fini *s'il existe $n \in \mathbb{N}$ et une bijection $\varphi : E_n \to E$. Dans ce cas, on dit que le nombre d'éléments $\#E$ (ou : $|E|$) de E (ou : le* cardinal*) est égal à n.*
Soient E, F des ensembles (pas nécessairement finis). On dit que E et F ont le même cardinal *s'il existe une application bijective $f : E \to F$.*
Les ensembles qui ont le même cardinal que $\mathbb{N}$ sont appelés dénombrables.

Noter que pour $n, m \in \mathbb{N}$ on a

$$n \leq m \Leftrightarrow E_n \subseteq E_m.$$

Exemple 6.21.

- $|\emptyset| = 0$ *(est $\emptyset$ est le seul ensemble de cardinal 0),* $|\{1\}| = 1$, $|\{A, B\}| = 2$.
- *Les nombres pairs sont dénombrables :*

$$\mathbb{N} \xrightarrow{n \mapsto 2n} \{2n \mid n \in \mathbb{N}\}$$

est une bijection.

- $\mathbb{N} \times \mathbb{N}$ *est dénombrable (voir l'exercice 4.8(c)).*
- $\mathbb{Z}$ *est dénombrable car*

$$\mathbb{N} \longrightarrow \mathbb{Z}, n \mapsto \begin{cases} 0 \mapsto 0, \\ n \mapsto \frac{n+1}{2} \text{ si } n \text{ est impair,} \\ n \mapsto -\frac{n}{2} \text{ si } n \text{ est pair} \end{cases}$$

est une bijection.

- $\mathbb{R}$ *n'est pas dénombrable par l'argument de la diagonale de Cantor (voir à propos sur feuille d'exercices).*

Lemme 6.22. *Soient $n, m \in \mathbb{N}$ deux nombres naturels distincts. Alors pour tout $m > n$, il n'existe pas d'injection $E_m \hookrightarrow E_n$.*

Démonstration. For $n \in \mathbb{N}$, on considère l'assertion

$$A(n) : \forall\, m > n : \text{ Il n'existe pas d'injection } E_m \to E_n.$$

Nous la démontrons par récurrence.

Initialisation Pour $n = 0$, on a $E_n = \emptyset$ et $m \in E_m \neq \emptyset$ pour tout $m > 0$. Il n'existe donc pas d'injection $E_m \to E_0$ (il n'existe même pas d'application).

Hérédité Supposons $A(n)$ vrai. Soit $m' = m + 1 > n + 1$. Supposons que nous avons une injection $\varphi : E_{m+1} \to E_{n+1}$.

1er cas. $n+1 \notin \mathrm{im}(\varphi)$. Alors φ se restreint pour donner une injection $E_{m'} \to E_n$, contradiction.

2ème cas. $n + 1 \in \mathrm{im}(\varphi)$. Alors il existe $a \in E_{m+1}$ tel que $\varphi(a) = n + 1$. Nous modifions l'injection φ comme suit

$$\varphi' : E_{m+1} \to E_{n+1}, \quad x \mapsto \begin{cases} \varphi(x) & \text{si } x \neq m+1 \wedge x \neq a, \\ n+1 & \text{si } x = m+1, \\ \varphi(m+1) & \text{si } x = a. \end{cases}.$$

L'application φ' est une injection et satisfait $\varphi'(m + 1) = n + 1$. Donc elle se restreint pour donner une injection $E_m \to E_n$, contradiction. L'assertion $A(n + 1)$ suit.

□

Proposition 6.23. *Soient E, F deux ensembles finis. Alors :*

(a) $\#E = \#F \Leftrightarrow$ *il existe une bijection* $f : E \to F$.

(b) $\#E \leq \#F \Leftrightarrow$ *il existe une injection de* E *dans* F.

(c) $\#F \leq \#E \Leftrightarrow$ *il existe une surjection de* E *dans* F.

Ce résultat sera utilisé très souvent pour calculer le cardinal d'un ensemble F : on trouvera une bijection entre cet ensemble et un ensemble E dont on connaît déjà le cardinal.

Démonstration. Soient $m := \#E$ et $n := \#F$. Par définition il existe des bijections $g : E_m \to E$ et $h : E_n \to F$. Notons g^{-1} l'inverse de g et h^{-1} l'inverse de h.
(a) « $\Rightarrow$ » : Comme $n = m$ on peut former la composée

$$E \xrightarrow{g^{-1}} E_n = E_m \xrightarrow{h} F$$

qui est une bijection car c'est la composée de deux bijections.
« $\Leftarrow$ » : Supposons que $f : E \to F$ est une bijection. Donc, la composée

$$E_n \xrightarrow{g} E \xrightarrow{f} F \xrightarrow{h^{-1}} E_m$$

est une bijection. Par le lemme 6.22 on obtient $n \leq m$. La même argumentation avec f^{-1} donne $m \leq n$, donc $n = m$.
(b) « $\Rightarrow$ » : Comme $n = m$ on peut former la composée

$$E \xrightarrow{g^{-1}} E_n \hookrightarrow E_m \xrightarrow{h} F$$

où $E_n \hookrightarrow E_m$ est l'inclusion. La composée est une injection car c'est la composée d'injections.
« $\Leftarrow$ » : Comme (a).
(c) Exercice. □

Voici encore un résumé de quelques propriétés utiles d'ensembles finis.

Proposition 6.24. *Soient E, F des ensembles finis. Alors :*

(a) Toute partie A de E est finie et vérifie $|A| \leq |E|$. Si on a de plus $|A| = |E|$, alors $A = E$.

(b) $E \cup F$ est fini. Si $E \cap F = \emptyset$, alors $|E \sqcup F| = |E| + |F|$. En général, $|E \cup F| = |E| + |F| - |E \cap F|$.

(c) $E \times F$ est fini et $|E \times F| = |E| \cdot |F|$.

(d) Soit $\mathcal{F}(E, F)$ l'ensemble de toutes les applications de E dans F. C'est un ensemble fini et $|\mathcal{F}(E, F)| = |F|^{|E|}$.

(e) $\mathcal{P}(E)$ est fini et $|\mathcal{P}(E)| = 2^{|E|}$.

(f) L'ensemble $\mathcal{S}(E)$ des bijections de E dans lui-même est fini et on a $|\mathcal{S}(E)| = |E|!$ ($|E|$ factorielle).

(g) Soit f une fonction de E dans F. Alors $|f(E)| \leq \min(|E|, |F|)$. On a $|f(E)| = |E|$ si et seulement si f est injective et $|f(F)| = |F|$ si et seulement si f est surjective.

Démonstration. C'est un bon exercice de démontrer les parties qui n'ont pas été traitées. □

7 Groupes

Objectifs :

- Apprendre et maîtriser la définition de groupes ;
- connaître et savoir calculer dans le groupe symétrique ;
- savoir démontrer des propriétés simples.

Le monoïde $(\mathbb{N}, +, 0)$

Les propriétés suivantes des nombres naturels ont été démontrées dans la proposition 6.11.

Associativité : $\forall\, n_1, n_2, n_3 \in \mathbb{N} :\ (n_1 + n_2) + n_3 = n_1 + (n_2 + n_3)$.

Élément neutre : $\forall\, n \in \mathbb{N} : 0 + n = n + 0 = n$.

Commutativité : $\forall\, n_1, n_2 \in \mathbb{N} : n_1 + n_2 = n_2 + n_1$.

Définition 7.1. *Soient G un ensemble, $e \in G$ un élément et*

$$* : G \times G \to G$$

une application. On appelle le triplet $(G, *, e)$ un monoïde *si*

Associativité : $\forall\, g_1, g_2, g_3 \in G :\ (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ *;*

Élément neutre : $\forall\, g \in G : e * g = g * e = g$.

Un monoïde $(G, *, e)$ est appelé commutatif *ou* abélien *si*

Commutativité : $\forall\, g_1, g_2 \in G : g_1 * g_2 = g_2 * g_1$.

Donc $(\mathbb{N}, +, 0)$ est un monoïde commutatif.

Lemme 7.2. *Soit $(G, *, e)$ un monoïde. Le seul élément f de G tel que pour tout $g \in G$ on a $f * g = g * f = g$ est e.*

Démonstration. $e = f * e = f$. □

Le groupe symétrique

Soit M un ensemble fini.

Notation 7.3.

$$S_M := \{f \mid f : M \to M \text{ application bijective }\}$$

Si $M = \{1, 2, \ldots, n\}$, alors on note $S_M =: S_n$.

Nous rappelons que le cardinal de S_n est $n!$.
Rappelons que nous avons déjà démontré *l'associativité de la composition d'applications* dans le lemme 4.5. Dans notre cas c'est : soient $f, g, h \in S_M$; alors

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Nous avons aussi défini *l'identité,* $\mathrm{id} : M \to M$*,* $m \mapsto m$. Elle satisfait :

$$\forall\, f \in S_M : \ \mathrm{id} \circ f = f \circ \mathrm{id} = f.$$

Donc, $(S_M, \circ, \mathrm{id})$ est un monoïde.
Dès que M a au moins trois éléments S_M **n'est pas commutatif** : Soient, par exemple, $M = \{1, 2, 3\}$ et $f(1) = 2$, $f(2) = 3$, $f(3) = 1$ et $g(1) = 2$, $g(2) = 1$, $g(3) = 3$; donc :

$$f \circ g(1) = 3, \ \ f \circ g(2) = 2, \ \ f \circ g(3) = 1 \text{ mais } g \circ f(1) = 1, \ \ g \circ f(2) = 3, \ \ g \circ f(3) = 2.$$

Mais S_M satisfait une autre propriété très importante : *l'existence d'inverse* que nous connaissons aussi déjà du lemme 4.6. Pour tout $f \in S_M$ il existe $g \in S_M$ tel que $f \circ g = g \circ f = \mathrm{id}$.

Définition de groupe et propriétés

Nous sommes menés par ces considérations à la définition d'un groupe :

Définition 7.4. *Soit $(G, *, e)$ un monoïde. Il est appelé un* groupe *si*

Existence d'inverse : $\forall\, g \in G\ \exists\, h \in G : h * g = g * h = e$.

Si un groupe $(G, *, e)$ est commutatif (en tant que monoïde), on parle d'un groupe abélien.

Donc, S_M est un groupe. On appelle S_n le *groupe symétrique (en n lettres).*
Attention : $(\mathbb{N}, +, 0)$ n'est pas un groupe car les inverses n'existent pas.
Par contre $(\mathbb{Z}, +, 0)$ est un groupe : l'élément inverse de $m \in \mathbb{Z}$ est $-m$ car

$$0 = (-m) + m = m + (-m).$$

Alors, $(\mathbb{Z}, +, 0)$ est un groupe abélien.

Lemme 7.5. *Soit $(G, *, e)$ un groupe et $g \in G$. L'inverse de g est unique : Si $h_1, h_2 \in G$ vérifient $h_i * g = g * h_i = e$ pour $i = 1, 2$, alors $h_1 = h_2$.*

Démonstration. $h_1 \overset{\text{élém. neutre}}{=} e * h_1 = (h_2 * g) * h_1 \overset{\text{associativité}}{=} h_2 * (g * h_1) = h_2 * e \overset{\text{élém. neutre}}{=} h_2$. □

Lemme 7.6. *Soit $(G, *, e)$ un groupe et $g, h \in G$. Soient g^{-1} l'inverse de g et h^{-1} l'inverse de h. Alors, l'inverse de $g * h$ est $h^{-1} * g^{-1}$.*

Démonstration. $(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = g * g^{-1} = e$ et $(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e * h = h^{-1} * h = e$. □

Les éléments du groupe symétrique

On présente deux manières pour noter les éléments f de S_n. Voici la première :

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ f(1) & f(2) & f(3) & \dots & f(n-1) & f(n) \end{pmatrix}.$$

Par exemple, si $n = 4$ et $f(1) = 2$, $f(2) = 4$, $f(3) = 3$, $f(4) = 1$, alors

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Beaucoup plus pratique, mais un peu plus difficile au début, est la deuxième manière, l'écriture en *cycles à supports disjoints*. Avant de l'expliquer il nous faut démontrer un lemme :

Lemme 7.7. *Soit $m \in M$ (fini). Il existe un $n \in \mathbb{N}_{>0}$ tel que $f^n(m) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ fois}}(m) = m$.*

Démonstration. Pour tout $n \in \mathbb{N}_{>0}$, l'élément $f^n(m)$ appartient à l'ensemble fini M. Donc, il existe $n_1 \neq n_2$ tels que $f^{n_1}(m) = f^{n_2}(m)$. Supposons sans perte de généralité que $n_1 > n_2$ et écrivons $n := n_1 - n_2$. Donc

$$f^{n_2}(m) = f^{n_1}(m) = f^{n_2} \circ f^n(m).$$

Soit $g \in S_M$ l'inverse de f^{n_2}, alors

$$m = g \circ f^{n_2}(m) = g \circ (f^{n_2} \circ f^n(m)) = (g \circ f^{n_2}) \circ f^n(m) = \mathrm{id} \circ f^n(m) = f^n(m).$$

La démontration est achevée. □

Nous notons f^{-1} l'inverse de f dans S_M.
Soit $m \in M$, $f \in S_M$ et $n \in \mathbb{N}_{>0}$ le plus petit entier naturel non nul tel que $f^n(m) = m$. Donc, $f^{-1}(m) = f^{n-1}(m)$. Le cycle de f qui contient m est défini comme :

$$\big(m \;\; f(m) \;\; f^2(m) \;\; f^3(m) \;\; \dots \;\; f^{n-1}(m)\big).$$

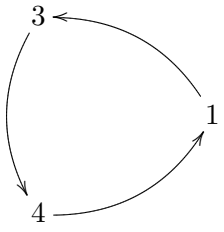
Exemple 7.8. *(a)* $M = \{1, 2, 3, 4, 5, 6\}$.

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

Le cycle qui contient 1 *est* $\big(1 \;\; 3 \;\; 4\big)$. *C'est évidemment aussi le cycle qui contient* 3 *et* 4. *Encore une fois, la signification de ce cycle est :*

$$1 \mapsto 3, \quad 3 \mapsto 4, \quad 4 \mapsto 1.$$

Alors, on voit le cycle vraiment comme un cycle (il n'y a ni début ni fin) : on peut se le représenter en écrivant les élément sur un cercle :



Donc on peut l'écrire aussi comme : $(3\ \ 4\ \ 1)$ *et* $(4\ \ 1\ \ 3)$. *(Attention ! Le cycle* $(1\ \ 4\ \ 3)$ *est différent : il représente l'application* $1 \mapsto 4, \quad 4 \mapsto 3, \quad 3 \mapsto 1$.*)*

Le cycle qui contient 2 *est* $(2\ \ 6)$*, et le cycle qui contient* 5 *est* (5).

L'écriture en cycles de f *est*

$$f = (1\ \ 3\ \ 4)\ (2\ \ 6)\ (5).$$

Souvent on n'écrit pas les cycles qui n'ont qu'un seul élément (sauf l'identité qui s'écrit $\mathrm{id} = (1)$*), alors*

$$f = (1\ \ 3\ \ 4)\ (2\ \ 6).$$

(b) Voici la liste complète des éléments de S_3 *:*

$$(1),\ \ (1\ \ 2),\ \ (1\ \ 3),\ \ (2\ \ 3),\ \ (1\ \ 2\ \ 3),\ \ (1\ \ 3\ \ 2).$$

(c) La composition de deux éléments en écriture en cycles (et, pour la dernière fois, autrement) :

$$\begin{aligned} (1\ \ 6\ \ 3\ \ 5)\ (2\ \ 4) \circ (1\ \ 3\ \ 4)\ (2\ \ 6) &= (1\ \ 5)\ (2\ \ 3)\ (4\ \ 6) \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 1 & 4 \end{pmatrix}. \end{aligned}$$

(d) L'inverse de $(1\ \ 6\ \ 3\ \ 5)\ (2\ \ 4) \in S_6$ *est* $(1\ \ 5\ \ 3\ \ 6)\ (2\ \ 4)$. *Donc pour obtenir l'inverse, on écrit les cycles en sense inverse.*

Définition 7.9.

(a) On appelle cycle *toute permutation* σ *dans* S_n *telle qu'il existe* k *compris entre* 1 *et* n*, et des entiers* $a_1, ..., a_k$ *dans* $\{1, ..., n\}$*, deux à deux distincts, tels que* $\sigma = (a_1 \dots a_k)$.

(b) L'entier k *et l'ensemble* $\{a_1, ..., a_k\}$ *sont alors uniques ;* k *est appelé la* longueur *du cycle et* $\{a_1, ..., a_k\}$ *est appelé le* support *du cycle.*

(c) Deux cycles sont dits à supports disjoints *si l'intersection de leurs supports est vide.*

Remarque 7.10. *(a) On rappelle que, lorsque l'on écrit un cycle, on peut commencer par n'importe quel élément du support (en respectant ensuite l'ordre des* a_i*). On a par exemple :*

$$(1635) = (6351) = (3516) = (5163).$$

(b) Deux cycles à supports disjoints commutent. Cela est un exercice facile.

(c) Attention, deux cycles dont les supports sont non disjoints ne commutent pas toujours. On a par exemple dans S_3 *:*

$$(12)(23) = (123) \neq (132) = (23)(12).$$

(d) Toute permutation de S_n s'écrit comme produit de cycles à supports disjoints. Cette écriture est unique, à l'ordre des cycles près.

On a par exemples les égalités :

$$\big(1\ \ 6\ \ 3\ \ 5\big)\ \big(2\ \ 4\big) = \big(2\ \ 4\big)\ \big(1\ \ 6\ \ 3\ \ 5\big) = \big(4\ \ 2\big)\ \big(3\ \ 5\ \ 1\ \ 6\big).$$

Définition 7.11. *Un élément $\tau \in S_n$ est appelé* transposition *s'il existe $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$ tels que $\tau = \big(i\ \ j\big)$.*

Proposition 7.12. *Le groupe symétrique S_n est engendré par ses transpositions, c'est-à-dire, tout élément peut s'écrire comme produit de transpositions.*

Démonstration. Il suffit de montrer que tout cycle $\big(a_1\ \ a_2\ \ a_3 \ldots a_r\big)$ s'écrit comme un produit de transpositions. C'est le cas car :

$$\big(a_1\ \ a_2\ \ a_3 \ldots a_r\big) = \big(a_r\ \ a_1\big) \circ \big(a_{r-1}\ \ a_1\big) \circ \cdots \circ \big(a_3\ \ a_1\big) \circ \big(a_2\ \ a_1\big).$$

□

8 Les entiers relatifs

Objectifs :

- Connaître la construction formelle de $\mathbb{Z}$ avec addition et multiplication à partir de $\mathbb{N}$;
- savoir démontrer des propriétés simples.

Construction de $\mathbb{Z}$

D'abord on écrira $\mathcal{Z}$ pour notre construction des entiers relatifs (pour souligner que c'est une construction d'un nouvel objet) ; après la construction, on utilisera la notation habituelle $\mathbb{Z}$ et on calculera avec $\mathbb{Z}$ comme chacun le connaît.
La construction est basée sur la relation d'équivalence suivante.

Lemme 8.1. *La relation binaire sur $\mathbb{N} \times \mathbb{N}$ définie par*

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a + d = b + c$$

est une relation d'équivalence.

Démonstration. La preuve est claire. La transitivité utilise des propriétés des entiers naturels établies dans la section 6. □

Les classes d'équivalences sont précisément les couples (a, b) ayant la même différence (qui peut être négative !) : donc,

$$\overline{a - b} := \overline{(a, b)} = \{(c, d) \in \mathbb{N} \times \mathbb{N} \mid c - d = a - b\}.$$

On peut donc prendre les classes d'équivalence pour cette relation d'équivalence comme une définition de $\mathbb{Z}$ si on arrive à définir l'addition et la multiplication « habituelles ». On s'occupe d'abord de l'addition.

Proposition 8.2. *Soit $\mathcal{Z}$ l'ensemble quotient de $\mathbb{N}$ par la relation d'équivalence définie dans le lemme 8.1.*

(a) L'application

$$+_{\mathcal{Z}} : \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}, \quad \overline{(a,b)} +_{\mathcal{Z}} \overline{(c,d)} := \overline{(a+c, b+d)}$$

est bien définie. La définition peut être écrite comme $\overline{a-b} +_{\mathcal{Z}} \overline{c-d} = \overline{(a+c)-(b+d)}$.

(b) Posons $0_{\mathcal{Z}} := \overline{(0,0)} = \overline{0-0}$. Alors, $(\mathcal{Z}, +_{\mathcal{Z}}, 0_{\mathcal{Z}})$ est un groupe abélien et l'inverse de $\overline{a-b} = \overline{(a,b)}$ est $\overline{b-a} = \overline{(b,a)}$; il est aussi noté $-\overline{a-b} = -\overline{(a,b)}$.

(c) L'application

$$i : \mathbb{N} \to \mathcal{Z}, \quad n \mapsto \overline{(n,0)} = \overline{n-0}$$

est injective et satisfait $i(a+b) = i(a) +_{\mathcal{Z}} i(b)$ pour tous $a, b \in \mathbb{N}$.

(d) $\overline{a-b} = \overline{(a,b)} \in i(\mathbb{N})$ si et seulement si $a \geq b$.

Démonstration. (a) Le point le plus important de cette preuve est de vérifier que $+_{\mathcal{Z}}$ est une **application bien définie**. Il faut donc montrer que la définition de $+_{\mathcal{Z}}$ ne dépend pas du choix des représentants des classes. Soient $(a',b') \in \overline{(a,b)}$ et $(c',d') \in \overline{(c,d)}$. Donc, par définition, on a

$$a + b' = a' + b \quad \text{et} \quad c + d' = c' + d.$$

En conséquence, ça donne

$$(a+c) + (b'+d') = (b+d) + (a'+c') \quad \text{donc} \quad \overline{(a+c, b+d)} = \overline{(a'+c', b'+d')},$$

démontrant que $+_{\mathcal{Z}}$ est bien définie.
(b) On va vérifier les axiomes : Soient $a, b, c, d, e, f \in \mathbb{N}$.

Associativité Elle est une conséquence directe de l'associativité du monoïde $(\mathbb{N}, +, 0)$:

$$(\overline{(a,b)} +_{\mathcal{Z}} \overline{(c,d)}) +_{\mathcal{Z}} \overline{(e,f)} = \overline{(a+c, b+d)} + \overline{(e,f)} = \overline{((a+c)+e, (b+d)+f)}$$
$$\overset{\text{assoc. de}\mathbb{N}}{=} \overline{(a+(c+e), b+(d+f))} = \overline{(a,b)} +_{\mathcal{Z}} \overline{(c+e, d+f)} = \overline{(a,b)} +_{\mathcal{Z}} (\overline{(c,d)} +_{\mathcal{Z}} \overline{(e,f)}).$$

Elément neutre C'est aussi une conséquence directe provenant de $\mathbb{N}$:

$$\overline{(a,b)} +_{\mathcal{Z}} 0_{\mathcal{Z}} = \overline{(a,b)} +_{\mathcal{Z}} \overline{(0,0)} = \overline{(a+0, b+0)} \overset{\text{élém. neutre de}\mathbb{N}}{=} \overline{(a,b)}$$

et de la même façon on a aussi $0_{\mathcal{Z}} + \overline{(a,b)} = \overline{(a,b)}$.

Existence d'inverse On a

$$\overline{(a,b)} +_{\mathcal{Z}} \overline{(b,a)} = \overline{(a+b, b+a)} = \overline{(a+b, a+b)} = \overline{(0,0)} = 0_{\mathcal{Z}}.$$

Commutativité C'est aussi une conséquence directe provenant de $\mathbb{N}$:

$$\overline{(a,b)} +_{\mathcal{Z}} \overline{(c,d)} = \overline{(a+c, b+d)} \overset{\text{commut. de}\mathbb{N}}{=} \overline{(c+a, d+b)} = \overline{(c,d)} +_{\mathcal{Z}} \overline{(a,b)}.$$

Donc, nous avons vérifié que $(\mathcal{Z}, +_{\mathcal{Z}}, 0_{\mathcal{Z}})$ est un groupe abélien.
(c) Montrons d'abord l'injectivité de i : Si $i(n) = i(m)$, alors $(n, 0) \sim (m, 0)$, donc $n + 0 = 0 + m$, donc $n = m$.
On vérifie la propriété énoncée :

$$i(a + b) = \overline{(a + b, 0)} = \overline{(a, 0)} +_{\mathcal{Z}} \overline{(b, 0)} = i(a) +_{\mathcal{Z}} i(b).$$

(d) Si $a \geq b$, il existe $d \in \mathbb{N}$ avec $a = b + d \in \mathbb{N}$, donc $\overline{(a, b)} = \overline{(d, 0)} = i(d)$. S'il existe $d \in \mathbb{N}$ tel que $\overline{(a, b)} = \overline{(d, 0)} = i(d)$, alors $a = b + d$, donc $a \geq b$. □

Lemme 8.3. *Pour tout* $\overline{a - b} = \overline{(a, b)} \in \mathcal{Z} \setminus i(\mathbb{N})$ *on a* $-\overline{a - b} = \overline{(b, a)} \in i(\mathbb{N})$ *et* $\overline{(a, b)} = \overline{(0, b - a)}$.

Démonstration. On a $a < b$, donc $\overline{(b, a)} \in \mathcal{Z}$. Le reste est clair. □

La multiplication des entiers relatifs

Nous allons maintenant définir une multiplication sur notre « modèle » des entiers relatifs.

Proposition 8.4. *(a) L'application*

$$\cdot_{\mathcal{Z}} : \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}, \quad \overline{(a, b)} \cdot_{\mathcal{Z}} \overline{(c, d)} := \overline{(ac + bd, ad + bc)}$$

est bien définie. On peut l'écrire comme

$$\overline{a - b} \ \cdot_{\mathcal{Z}} \ \overline{c - d} = \overline{(ac + bd) - (ad + bc)}.$$

(b) Posons $1_{\mathcal{Z}} := \overline{(1, 0)} = \overline{1 - 0}$. *Alors,* $(\mathcal{Z}, \cdot_{\mathcal{Z}}, 1_{\mathcal{Z}})$ *est un monoïde abélien.*

(c) La multiplication est distributive, *c'est-à-dire*

$$(\overline{(a, b)} +_{\mathcal{Z}} \overline{(c, d)}) \cdot_{\mathcal{Z}} \overline{(e, f)} = (\overline{(a, b)} \cdot_{\mathcal{Z}} \overline{(e, f)}) +_{\mathcal{Z}} (\overline{(c, d)} \cdot_{\mathcal{Z}} \overline{(e, f)})$$

pour tous $a, b, c, d, e, f \in \mathbb{N}$.

Démonstration. (a) Il faut donc montrer que la définition de $\cdot_{\mathcal{Z}}$ ne dépend pas du choix des représentants des classes. Soient $(a', b') \in \overline{(a, b)}$ et $(c', d') \in \overline{(c, d)}$. Donc par définition on a

$$a + b' = a' + b \quad \text{et} \quad c + d' = c' + d.$$

En conséquence on obtient

$$ac + b'c = a'c + bc, \quad a'd + bd = ad + b'd, \quad a'c + a'd' = a'c' + a'd, \quad b'c' + b'd = b'c + b'd'.$$

On les aditionne pour obtenir :

$$ac + b'c + a'd + bd + a'c + a'd' + b'c' + b'd = a'c + bc + ad + b'd + a'c' + a'd + b'c + b'd',$$

donc

$$(ac + bd) + (a'd' + b'c)' = (a'c' + b'd') + (ad + bc)$$

et en conséquence

$$\overline{(ac + bd, ad + bc)} = \overline{(a'c' + b'd', a'd' + b'c')}.$$

(b) et (c) Exercice. □

L'ordre naturel sur $\mathbb{Z}$

Nous allons étendre l'ordre naturel à $\mathbb{Z}$ (pour obtenir l'ordre « habituel »).
Rappelons que nous avons défini $\mathbb{Z} = \mathcal{Z}$ comme l'ensemble des classes d'équivalence $\overline{a-b} = \overline{(a,b)} = \{(c,d) \in \mathbb{N}\times\mathbb{N} \mid a+d = b+c\}$.

Définition-Lemme 8.5. *(a) Sur $\mathcal{Z} = \mathbb{Z}$ on définit une relation d'ordre totale par*

$$\overline{a-b} \preccurlyeq \overline{c-d} \Leftrightarrow a+d \leq b+c.$$

(b) Sur l'image de $\mathbb{N}$ par l'application naturelle $i : \mathbb{N} \to \mathcal{Z}, \quad n \mapsto \overline{n-0}$ cet ordre est le même que l'ordre de $\mathbb{N}$.

Démonstration. (b) est claire :

$$\overline{n-0} \preccurlyeq \overline{m-0} \Leftrightarrow n+0 \leq m+0 \Leftrightarrow n \leq m.$$

(a)

Bien défini Supposons $\overline{a-b} = \overline{a'-b'}$ (donc, $a+b' = a'+b$) et $\overline{c-d} = \overline{c'-d'}$ (donc, $c+d' = c'+d$). Nous trouvons les équivalences :

$$\begin{aligned}
\overline{a-b} \preccurlyeq \overline{c-d} &\Leftrightarrow a+d \leq b+c \\
&\Leftrightarrow a+d+b'+d' \leq b+c+b'+d' \\
&\Leftrightarrow (a+b')+d+d' \leq (c+d')+b+b' \\
&\Leftrightarrow (a'+b)+d+d' \leq (c'+d)+b+b' \\
&\Leftrightarrow (a'+d')+(b+d) \leq (b'+c')+(b+d) \\
&\Leftrightarrow a'+d' \leq b'+c' \\
&\Leftrightarrow \overline{a'-b'} \preccurlyeq \overline{c'-d'}
\end{aligned}$$

Donc, la définition ne dépend pas du choix.

Réflexivité $\overline{a-b} \preccurlyeq \overline{a-b} \Leftrightarrow a+b \leq b+a$.

Antisymétrie Si $\overline{a-b} \preccurlyeq \overline{c-d}$ et $\overline{c-d} \preccurlyeq \overline{a-b}$, alors, $a+d \leq b+c$ et $b+c \leq a+d$, alors $a+d = b+c$, donc $\overline{a-b} = \overline{c-d}$.

Transitivité

$$\begin{aligned}
&\overline{a-b} \preccurlyeq \overline{c-d} \text{ et } \overline{c-d} \preccurlyeq \overline{e-f} \\
\Rightarrow &a+d \leq b+c \text{ et } c+f \leq d+e \\
\Rightarrow &a+d+f \leq b+c+f \text{ et } c+f \leq d+e \\
\Rightarrow &a+d+f \leq b+d+e \\
\Rightarrow &a+f \leq b+e \\
\Rightarrow &\overline{a-b} \preccurlyeq \overline{e-f}.
\end{aligned}$$

Totalité Soient $\overline{a-b}, \overline{c-d} \in \mathcal{Z}$. Si $a+d \leq b+c$, alors $\overline{a-b} \preccurlyeq \overline{c-d}$. Si $b+c \leq a+d$, alors $\overline{c-d} \preccurlyeq \overline{a-b}$.

□

Après cette preuve nous allons écrire $\leq$ au lieu de $\preccurlyeq$.

Lemme 8.6. *Soient $x, y, z \in \mathbb{Z}$ tel que $x \leq y$. Alors :*

(a) $x+z \leq y+z$.

(b) Si $0 \leq z$, *alors* $x \cdot z \leq y \cdot z$.

(c) Si $z \leq 0$, *alors* $y \cdot z \leq x \cdot z$.

Démonstration. Soient $x = \overline{a-b}, y = \overline{c-d}, z = \overline{e-f}$. Nous avons $a+d \leq b+c$.
(a) Il en suit que $(a+e)+(d+f) \leq (c+e)+(b+f)$, donc $\overline{a-b}+\overline{e-f} \leq \overline{c-d}+\overline{e-f}$.
(b) Nous pouvons écrire $z = \overline{n-0}$ avec $n \in \mathbb{N}$. D'abord notons que la formule pour la multiplication dans $\mathcal{Z}$ nous donne $xz = xn = \overline{an-bn}$ et $yz = yn = \overline{cn-dn}$. Il suit de $a+d \leq b+c$ que $an+dn \leq bn+cn$, donc $xz = \overline{an-bn} \leq \overline{cn-dn} = yz$.
(c) Nous pouvons écrire $z = \overline{0-n}$ avec $n \in \mathbb{N}$. La formule pour la multiplication dans $\mathcal{Z}$ donne $xz = x\overline{0-n} = \overline{bn-an}$ et $yz = y\overline{0-n} = \overline{dn-cn}$. Il suit de $a+d \leq b+c$ que $an+dn \leq bn+cn$, donc $yz = \overline{dn-cn} \leq \overline{bn-an} = xz$. □

À partir de maintenant, nous allons utiliser la notation $\mathbb{Z}$ pour $\mathcal{Z}$ et on va écrire $+, \cdot$ au lieu de $+_{\mathcal{Z}}, \cdot_{\mathcal{Z}}$. On utilisera aussi les notations habituelles n pour $\overline{n-0} = \overline{(n,0)}$ et $-n$ pour $\overline{0-n} = \overline{(0,n)}$ (pour $n \in \mathbb{N}$).

9 Anneaux

Objectifs :

- Maîtriser la notion d'anneau ;
- connaître des exemples d'anneaux ;
- maîtriser les notions de diviseur de zéro et d'unité ;
- savoir démontrer des propriétés simples.

Les entiers relatifs $\mathbb{Z}$ sont un ensemble avec deux lois, l'addition et la multiplication,

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a,b) \mapsto a+b,$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a,b) \mapsto a \cdot b,$$

et deux éléments spéciaux 0, 1 tels que

- ($(\mathbb{Z}, +, 0)$ est un groupe abélien) : pour tout $\ell, m, n \in \mathbb{Z}$:

  - *élément neutre :* $m + 0 = m = 0 + m$;
  - *associativité :* $(m + n) + \ell = m + (n + \ell)$;
  - *existence d'inverse :* $m + (-m) = 0 = (-m) + m$;
  - *commutativité :* $m + n = n + m$.

- ($(\mathbb{Z}, \cdot, 1)$ est un monoïde commutatif) : pour tout $\ell, m, n \in \mathbb{Z}$:
  - *élément neutre :* $m \cdot 1 = m = 1 \cdot m$;
  - *associativité :* $(m \cdot n) \cdot \ell = m \cdot (n \cdot \ell)$;
  - *commutativité :* $m \cdot n = n \cdot m$.

- (relation entre $+$ et $\cdot$) :
  - *distributivité :* $(m + n) \cdot \ell = m \cdot \ell + n \cdot \ell$.

Comme vous le savez sans doute, les mêmes opérations existent par exemple pour les nombres rationnels, les nombres réels et les nombres complexes. Cela nous amène à donner un nom spécial aux ensembles ayant de telles structures : *anneau*.

Définition 9.1. *Soient A un ensemble, $0_A, 1_A \in A$ deux éléments (pas nécessairement distincts) et*

$$+_A : A \times A \to A, \quad \text{et} \quad \cdot_A : A \times A \to A$$

deux applications. On appelle le tuplet $(A, +_A, \cdot_A, 0_A, 1_A)$ un anneau (commutatif) *si*

- $(A, +_A, 0_A)$ *est un groupe abélien,*
- $(A, \cdot_A, 1_A)$ *est un monoïde (commutatif) et*
- *pour tous $a, b, c \in A$:*
$$a \cdot_A (b +_A c) = (a \cdot_A b) +_A (a \cdot_A c)$$
et
$$(a +_A b) \cdot_A c = (a \cdot_A c) +_A (b \cdot_A c)$$
*(*distributivité).

Donc, $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau commutatif. On le notera souvent juste $\mathbb{Z}$.
Notez que si l'anneau est commutatif (par définition la multiplication est commutative), il suffit de vérifier une seule des deux égalités pour la distributivité.
Souvent, nous allons supprimer l'indice A, donc on va écrire $0, 1, +, \cdot$ sans mentionner A explicitement. On va même écrire parfois A sans mentionner $0, 1, +, \cdot$, mais sachant que $0, 1, +, \cdot$ font partie des données d'un anneau et qu'ils sont fixés. Nous allons aussi supprimer $\cdot$ parfois et écrire ab pour $a \cdot b$. On convient également que la multiplication doit toujours être éxécutée avant l'addition : $a + b \cdot c = a + (b \cdot c)$.

Lemme 9.2. *Soit $(A, +, \cdot, 0, 1)$ un anneau. Alors, pour tous $a \in A$ on a $0 \cdot a = a \cdot 0 = 0$.*

Démonstration. $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$, donc, $(A, +, 0)$ étant un groupe, on a $0 = 0 \cdot a$. De la même façon : $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, donc $0 = a \cdot 0$. □

Exemple 9.3. *D'autres exemples d'anneaux sont :*

- $(\mathbb{Q}, +, \cdot, 0, 1)$ *est un anneau commutatif. Plus bas, on verra une construction formelle.*
- $(\mathbb{R}, +, \cdot, 0, 1)$ *est un anneau commutatif. Il est connu des cours d'analyse et d'algèbre linéaire. Plus bas, on verra une construction formelle.*
- $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), +, \circ, \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right))$ *est un anneau non commutatif ($\circ$ désigne le produit matriciel).*

Définition-Lemme 9.4. *Soit $(A, +, \cdot, 0, 1)$ un anneau. Un élément $u \in A$ est appelé* unité *s'il existe $v \in A$ tel que $uv = vu = 1$. Une unité est donc un élément inversible dans le monoïde $(A, \cdot, 1)$.*
L'ensemble des unités de A est noté $A^\times$. $(A^\times, \cdot, 1)$ est un groupe (abélien si l'anneau est commutatif). Il s'appelle groupe des unités de A.

Démonstration. L'associativité et l'existence d'élément neutre proviennent du fait que $(A, \cdot, 1)$ est un monoïde. L'existence d'inverse est la propriété définissant l'ensemble $A^\times$. □

Proposition 9.5. $\mathbb{Z}^\times = \{-1, 1\}$.

Démonstration. L'équation $a \cdot b = 1$ n'admet que les solutions $(a = 1, b = 1)$ et $(a = -1, b = -1)$ dans $\mathbb{Z}$. Donc 1 et -1 sont les seules unités de $\mathbb{Z}$. □

La construction de $\mathbb{Q}$ sera fait plus tard. Notre connaissance de $\mathbb{Q}$ nous permet déjà d'affirmer $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, car toute fraction non nulle $\frac{a}{b}$ a $\frac{b}{a}$ comme inverse.

Anneaux intègres

Proposition 9.6. *Pour tous $a, b \in \mathbb{Z}$ tels que $ab = 0$, on a $a = 0$ ou $b = 0$.*

Démonstration. Si $a \in \mathbb{N}$ et $b \in \mathbb{N}$, c'est la proposition 6.13. Si $a \in \mathbb{N}$ et $b \notin \mathbb{N}$, on a $0 = -1 \cdot 0 = -1 \cdot a \cdot b = a \cdot (-b)$, donc $a = 0$ ou $-b = 0$, donc $a = 0$ ou $b = 0$. Les deux autres cas sont similaires. □

Définition 9.7. *Soit $(A, +, \cdot, 0, 1)$ un anneau. On dit que A est un* anneau intègre *si pour tous $a, b \in A$ tels que $ab = 0$, on a $a = 0$ ou $b = 0$.*
Un élément $a \in A$ tel qu'il existe $b \in A \setminus \{0\}$ avec $ab = 0$ ou $ba = 0$ est appelé diviseur de zéro. *(Donc un anneau est intègre s'il n'existe pas de diviseur de zéro sauf 0.)*

Donc, $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau intègre.

Proposition 9.8. *Soit $(A, +, \cdot, 0, 1)$ un anneau intègre. Alors, on peut simplifier des produits comme suit : Pour tous $a, b, c \in A$ avec $a \neq 0$ tels que $ab = ac$ ou $ba = ca$ on a $b = c$.*
En particulier, cette règle est valable dans $\mathbb{Z}$.

Démonstration. Si $ab = ac$, alors $a(b - c) = 0$. Comme A est intègre nous obtenons $a = 0$ ou $b - c = 0$. Le premier cas est exclu, donc $b - c = 0$, donc $b = c$. Un argument similaire marche aussi pour $ba = ca$. □

Corps

Définition 9.9. *Soit $(A, +, \cdot, 0, 1)$ un anneau (commutatif). On l'appelle* corps (commutatif) *si*

- *tout $0 \neq a \in A$ est une unité pour la multiplication (c'est-à-dire, $A^\times = A \setminus \{0\}$) et*
- $0 \neq 1$.

Exemple 9.10.

- $(\mathbb{Q}, +, \cdot, 0, 1)$ *est un corps commutatif.*
- $(\mathbb{R}, +, \cdot, 0, 1)$ *est un corps commutatif.*
- $(\mathbb{Z}, +, \cdot, 0, 1)$ *n'est pas un corps car il existe $n \in \mathbb{Z} \setminus \{0\}$ qui n'est pas une unité, par exemple $n = 2$.*

On définira plus loin une famille de corps très importante : les corps finis.

Lemme 9.11. *Soit $(A, +, \cdot, 0, 1)$ un corps. Alors, A est un anneau intègre.*

Démonstration. Exercice. □

10 L'anneau des entiers relatifs revisité

Objectifs :

- Maîtriser la division euclidienne ;
- maîtriser les congruences et les règles de calculs ;
- connaître la relation entre congruences modulo n et l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$;
- connaître les corps fini premiers.

Magie de nombres (ou pas de magie ?)

Si vous me donnez un nombre naturel n (en écriture décimale), je peux tout de suite vous dire s'il est divisible par 9 ou pas. Connaissez-vous la règle ?
Si vous me donnez un nombre naturel n (en écriture décimale), je peux tout de suite vous dire s'il est divisible par 11 ou pas. Connaissez-vous la règle ?
Si vous me donnez un nombre naturel n, je peux tout de suite vous dire lequel est le dernier chiffre de 3^n (en écriture décimale). Par exemple, le dernier chiffre de

- 3^{122} est 9 ;
- 3^{2015} est 7. Effectivement, $3^{2015} =$

$$\begin{array}{c}
25080042038941917740411277432754132213088458429396188569550624575886438840272416 85 \\
92230352478466118474805828019065738322615576099491131371608801105453208238680156 05 \\
56105973417906788615677997270817002308165663760091704933847507773524892191836973 37 \\
36550344783649014160417866960257394320958565745970092212392005213434725479822823 33 \\
14676746046030011680610745470896116838317231815494252785564520279276825468757921 23 \\
55360174861501830887692020856123639631076274767980889199365167727307947318761293 95 \\
29677662981266857850195462245255756158937013662458483991432324212088303514655945 43 \\
43371094196080300249938040053454287804641161618723791975471945544468695711379237 92 \\
88861142481317314104416649319153376644343238204511379205427223526972584849904229 57 \\
21995324006626887514786000282859279760690335971464362806410760530870111130260825 89 \\
59955906990581027858613454717161138232679465898673005166680385608820976603213962 98 \\
0825725043386490463502031967485084726784039422586713034289 07
\end{array}$$

- (voyez le cours)

La divisibilité dans $\mathbb{Z}$

Soit $a, b \in \mathbb{Z}$. On rappelle que b *divise* a (notation : $b \mid a$) s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Lemme 10.1. *La divisibilité dans $\mathbb{Z}$ définit une relation réflexive et transitive qui satisfait aussi :*

(a) pour tous $a, b \in \mathbb{Z} \setminus \{0\}$: $\big((a \mid b \text{ et } b \mid a) \Rightarrow a = b \text{ ou } a = -b\big)$ *;*

(b) pour tous $a, b, c \in \mathbb{Z}$: $\big((a \mid b \text{ et } a \mid c) \Rightarrow a \mid (b + c) \text{ et } a \mid (b - c)\big)$.

Démonstration.

Réflexivité $a \mid a$ parce que $a \cdot 1 = a$.

Transitivité $a \mid b$ et $b \mid c$ impliquent l'existence de $q, r \in \mathbb{Z}$ tels que $b = qa$ et $c = rb$. Donc $c = qra$, donc $a \mid c$.

(a) $a \mid b$ et $b \mid a$ impliquent l'existence de $q, r \in \mathbb{Z}$ tels que $b = qa$ et $a = rb$. Donc $a = rqa$, donc (a étant non nul et $\mathbb{Z}$ intègre) $rq = 1$, et donc $r = \pm 1$ et $q = r$ par la proposition 9.5, d'où le résultat.

(b) $a \mid b$ et $a \mid c$ impliquent l'existence de $q, r \in \mathbb{Z}$ tels que $b = qa$ et $c = ra$. Donc, $b + c = (q + r)a$ et $b - c = (q - r)a$, donc $a \mid (b + c)$ et $a \mid (b - c)$.

□

Division euclidienne

Proposition 10.2 (Division euclidienne)**.** *Soient $x, y \in \mathbb{Z}$ avec $y \geq 1$. Il existe des uniques $q, r \in \mathbb{Z}$ tels que*

$$x = qy + r \text{ et } 0 \leq r \leq y - 1.$$

Démonstration.

Existence Soit $M := \{x - zy \mid z \in \mathbb{Z}\} \cap \mathbb{N}$. C'est un sous-ensemble non-vide de $\mathbb{N}$. Comme $\mathbb{N}$ est bien ordonné, il existe un plus petit élément $r \in M$; il est automatiquement de la forme $r = x - qy$. Si $r \geq y$, alors $r - y = x - (q + 1)y \in M$ est un élément encore plus petit que le plus petit élément. Donc $r < y$.

Unicité Supposons que $x = qy + r = q'y + r'$. Donc,

$$(q - q')y = r' - r.$$

Il en suit $y \mid (r' - r)$. Mais, on a aussi

$$-y < r' - r < y,$$

donc $0 = r' - r$ (car 0 est le seul multiple de y strictement plus grand que $-y$ et strictement plus petit que y), donc $r = r'$ et $q = q'$.

□

Congruences

Définition 10.3. *Soit $n \in \mathbb{N}_{>0}$. Deux entiers relatifs $x, y \in \mathbb{Z}$ sont appelés* congrus modulo n *si* $n \mid (x-y)$.
Notation : $x \equiv y \pmod{n}$ *(ou* $x \equiv y \mod (n)$*).*

Lemme 10.4. *Soient $n \in \mathbb{N}_{>0}$ et $x, y \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :*

(i) $x \equiv y \pmod{n}$.

(ii) Le reste de la division euclidienne de x par n est le même que le reste de la division de y par n.

Démonstration. Soient $x = q_1 n + r_1$ et $y = q_2 n + r_2$ avec $0 \leq r_1 \leq n-1$ et $0 \leq r_2 \leq n-1$.
« (i) $\Rightarrow$ (ii) » : Alors, $n \mid (x-y)$. Comme $n \mid (q_1 - q_2)n$, il suit que n divise $(x-y) - (q_1-q_2)n = r_1 - r_2$, donc $r_1 = r_2$ (même argument qu'en haut : $-n < r_1 - r_2 < n$).
« (ii) $\Rightarrow$ (i) » : Alors, $r_1 = r_2$, donc $x - y = (q_1 - q_2)n$, donc $n \mid (x-y)$, donc $x \equiv y \pmod{n}$. □

Définition-Lemme 10.5. *Soit $n \in \mathbb{N}$. La congruence modulo n définit une relation d'équivalence R_n :*

$$\forall (x,y) \in \mathbb{Z}^2, x R_n y \Leftrightarrow x \equiv y \pmod{n}.$$

L'ensemble quotient $\mathbb{Z}/R_n$ est noté $\mathbb{Z}/n\mathbb{Z}$. On a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et

$$\overline{0} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}, \overline{k} = \{\ldots, -2n+k, -n+k, k, n+k, 2n+k, \ldots\}.$$

La classe d'un entier k compris entre 0 et $n-1$ est le sous-ensemble de $\mathbb{Z}$ formé des entiers relatifs dont le reste dans la division euclidienne par n est égal à k.

Démonstration. Exercice. □

Anneaux quotients

Lemme 10.6. *Soient $n \in \mathbb{N}$ et $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ tels que*

$$x_1 \equiv y_1 \pmod{n} \quad \textit{et} \quad x_2 \equiv y_2 \pmod{n}.$$

Alors,

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{n} \quad \textit{et} \quad x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}.$$

Démonstration. Nous avons $n \mid (x_1 - y_1)$ et $n \mid (x_2 - y_2)$.
Pour la première assertion nous en concluons $n \mid ((x_1 - y_1) + (x_2 - y_2))$, donc $n \mid ((x_1 + x_2) - (y_1 + y_2))$, donc $x_1 + x_2 \equiv y_1 + y_2 \pmod{n}$.
Pour la deuxième assertion, il suit que $n \mid (x_1 - y_1)x_2$ et $n \mid (x_2 - y_2)y_1$, donc $n \mid ((x_1 - y_1)x_2 + (x_2 - y_2)y_1)$, donc $n \mid (x_1 x_2 - y_1 y_2)$, donc $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}$. □

On peut maintenant donner l'explication du calcul du dernier chiffre de 3^n pour $n \in \mathbb{N}$. Faire la division euclidienne de n par 4 : $n = 4q + r$ avec $0 \leq r \leq 3$. Alors :

$$3^n = 3^{4q+r} = (3^4)^q \cdot 3^r = 81^q \cdot 3^r \equiv 1^q \cdot 3^r = 3^r \pmod{10}.$$

Donc, le magicien n'a besoin que de faire la division euclidienne par 4 (pour ça il suffit de la faire pour les 2 derniers chiffres de n (trouvez la raison vous-mêmes !)) et de connaître (le dernier chiffre de) 3^r pour $r = 0, 1, 2, 3$.

Définition-Lemme 10.7. *Soit $n \in \mathbb{N}$. Nous définissons*

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$$

et

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}.$$

Alors, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un anneau commutatif.

Démonstration. Exercice. Utiliser le lemme 10.6 pour démontrer que $+$ et $\cdot$ sont bien définis (indépendants des choix de représentants) et le fait que $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau. □

Nous allons souvent noter les classes de $\mathbb{Z}/n\mathbb{Z}$ sans écrire les « barres ». Également, on notera l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ plus court comme $\mathbb{Z}/n\mathbb{Z}$.

Exemple 10.8. *(a) Voici les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$.*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(b) Voici les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$.

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(c) Voici les tables d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

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

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Plus grand diviseur commun (pgcd)

Définition 10.9. *Soient $d \in \mathbb{N}$ et $x, y \in \mathbb{Z}$. On appelle d* plus grand commun diviseur de x, y *(notation : $d = \mathrm{pgcd}(x, y)$) si*

- *$d \mid x$ et $d \mid y$ et*

- *pour tout* $e \in \mathbb{N}$ *on a* $((e \mid x$ *et* $e \mid y) \Rightarrow e \mid d)$.

Proposition 10.10. *Soient* $x, y \in \mathbb{Z}$ *pas tous les deux* 0.

(a) Un plus grand commun diviseur de x *et* y *existe et il est unique.*

(b) Identité de Bézout : *Il existe* $a, b \in \mathbb{Z}$ *tels que* $\mathrm{pgcd}(x, y) = ax + by$.

Démonstration. Soit $M := \{ax + by \mid a, b \in \mathbb{Z}\}$ et $M^+ := M \cap \mathbb{N}_{>0}$. Comme M^+ est un sous-ensemble non vide de $\mathbb{N}$, il possède un plus petit élément d (par le fait que $\mathbb{N}$ est bien ordonné).
Par définition il existe $a, b \in \mathbb{Z}$ tel que $d = ax + by$. Nous allons démontrer que d est un plus grand commun diviseur de x, y.
D'abord on montre $d \mid m$ pour tout $m \in M$ (comme $x, y \in M$, on obtient alors automatiquement $d \mid x$ et $d \mid y$). Soit $m = ux + vy$. On fait la division euclidienne par d :

$$m = qd + r \text{ avec } 0 \leq r \leq d - 1.$$

Alors,

$$r = m - qd = ux + vy - q(ax + by) = (u - qa)x + (v - qb)y,$$

donc $r = 0$ car si $1 \leq r$, alors $r \in M^+$ entraînerait que r est strictement plus petit que le plus petit élément de M^+, une contradiction.
Soit $e \in \mathbb{N}$ tel que $e \mid x$ et $e \mid y$. Donc, $e \mid (ax + by)$, donc $e \mid d$. Nous avons terminé la preuve que d est un plus grand commun diviseur.
L'unicité est claire : Si $d, e \in \mathbb{N}$ sont des plus grands communs diviseurs tous les deux, alors $d \mid e$ et $e \mid d$, et e et d sont tous les deux dans $\mathbb{N}_{>0}$, donc $d = e$. □

Le pgcd et l'identité de Bézout peuvent être calculés (et leur existence peut être démontrée) par l'algorithme d'Euclide (voir Exercices) que nous décrivons maintenant (et que vous avez dû voir à l'école).
Soient $r_0 \geq r_1$ deux entiers positifs. Nous allons calculer leur pgcd ainsi que l'identité de Bézout, par le processus récursif suivant :

Si $r_1 \geq 1$, calculer le reste r_2 de la div. de r_0 par r_1	$r_0 = q_1 r_1 + r_2$;
Si $r_2 \geq 1$, calculer le reste r_3 de la div. de r_1 par r_2	$r_1 = q_2 r_2 + r_3$;
$\vdots$	$\vdots$
Si $r_n \geq 1$, calculer le reste r_{n+1} de la div. de r_{n-1} par r_n	$r_{n-1} = q_n r_n + r_{n+1}$;
Si $r_{n+1} = 0$, on a terminé.	$r_n = \mathrm{pgcd}(r_0, r_1)$

Nous démontrons ci-dessous que r_n est en effet égal à $\mathrm{pgcd}(r_0, r_1)$. D'abord on vérifie que r_n divise r_0 et r_1 :

r_n divise r_{n-1}.
$\Rightarrow$ r_n divise $r_{n-2} = q_{n-1} r_{n-1} + r_n$.
$\Rightarrow$ r_n divise $r_{n-3} = q_{n-2} r_{n-2} + r_{n-1}$.
$\vdots$
$\Rightarrow$ r_n divise $r_1 = q_2 r_2 + r_3$.
$\Rightarrow$ r_n divise $r_0 = q_1 r_1 + r_2$.

Exemple 10.11. $r_0 = 99$ *et* $r_1 = 21$.

Calculer le reste $r_2 = 15$ *de la div. de* 99 *par* 21	$99 = 4 \cdot 21 + 15$ *;*
Calculer le reste $r_3 = 6$ *de la div. de* 21 *par* 15	$21 = 1 \cdot 15 + 6$ *;*
Calculer le reste $r_4 = 3$ *de la div. de* 15 *par* 6	$15 = 2 \cdot 6 + 3$ *;*
Le reste de la div. de 6 *par* 3 *est* 0	$6 = 2 \cdot 3$ *;*
	$3 = \mathrm{pgcd}(99, 21)$

On obtient l'identité de Bézout en utilisant les égalités dans la colonne à droite, commençant par le bas :

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2 \cdot (21 - 1 \cdot 15) = -2 \cdot 21 + 3 \cdot 15 \\ &= -2 \cdot 21 + 3 \cdot (99 - 4 \cdot 21) = 3 \cdot 99 - 14 \cdot 21. \end{aligned}$$

Le calcul de l'identité de Bézout dans l'exemple est un peu *ad hoc*. On va le remplacer par une formulation générale et plus élégante. On utilisera les matrices de taille 2×2 qu'on suppose connues du cours d'algèbre linéaire.

Soient $r_0 \geq r_1$ deux entiers positifs. Nous allons calculer leur pgcd ainsi que l'identité de Bézout, par le processus récursif suivant :

Si $r_1 \geq 1$, reste r_2 de la div. de r_0 par r_1	$A_1 := \left(\begin{smallmatrix} -q_1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} r_2 \\ r_1 \end{smallmatrix}\right) = A_1 \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$
Si $r_2 \geq 1$, reste r_3 de la div. de r_1 par r_2	$A_2 := \left(\begin{smallmatrix} -q_2 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_1$	$\left(\begin{smallmatrix} r_3 \\ r_2 \end{smallmatrix}\right) = A_2 \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$
$\vdots$	$\vdots$	$\vdots$
Si $r_n \geq 1$, reste r_{n+1} de la div. de r_{n-1} par r_n	$A_n := \left(\begin{smallmatrix} -q_n & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_{n-1}$	$\left(\begin{smallmatrix} r_{n+1} \\ r_n \end{smallmatrix}\right) = A_n \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$
Si $r_{n+1} = 0$, on a terminé.	$r_n = \mathrm{pgcd}(r_0, r_1)$	

Soit $A_{n-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Alors, l'égalité $\left(\begin{smallmatrix} r_n \\ r_{n-1} \end{smallmatrix}\right) = A_{n-1} \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \left(\begin{smallmatrix} r_1 \\ r_0 \end{smallmatrix}\right)$ nous donne

$$r_n = ar_1 + br_0,$$

l'identité de Bézout récherchée. Comme on sait que r_n divise r_0 et r_1, on obtient aussi une preuve que r_n est en effet le pgcd de r_0 et r_1 : tout diviseur de r_0 et r_1 doit diviser r_n.

Exemple 10.12. *On reprend l'exemple* $r_0 = 99$ *et* $r_1 = 21$.

Reste $r_2 = 15$ *de la div. de* 99 *par* 21	$A_1 = \left(\begin{smallmatrix} -4 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *;*
Reste $r_3 = 6$ *de la div. de* 21 *par* 15	$A_2 = \left(\begin{smallmatrix} -1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_1 = \left(\begin{smallmatrix} 5 & -1 \\ -4 & 1 \end{smallmatrix}\right)$ *;*
Reste $r_4 = 3$ *de la div. de* 15 *par* 6	$A_3 = \left(\begin{smallmatrix} -2 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot A_2 = \left(\begin{smallmatrix} -14 & 3 \\ 5 & -1 \end{smallmatrix}\right)$ *;*
Le reste de la div. de 6 *par* 3 *est* 0	
	$3 = \mathrm{pgcd}(99, 21)$

Les coefficients de l'identité de Bézout sont les coefficients de la première rangée de la matrice A_3 *:*

$$3 = -14 \cdot 21 + 3 \cdot 99.$$

Définition 10.13. *Soient* $m \in \mathbb{N}$ *et* $x, y \in \mathbb{Z}$*. On appelle* m *le* plus petit commun multiple de x, y *(notation :* $m = \mathrm{ppcm}(x, y)$*) si*

- $x \mid m$ *et* $y \mid m$ *et*
- *pour tout* $n \in \mathbb{N}$ *on a* $((x \mid n \text{ et } y \mid n) \Rightarrow m \mid n)$.

Proposition 10.14. *Soient $x, y \in \mathbb{Z}$ pas tous les deux 0.*

(a) Un plus petit commun multiple de x et y existe et il est unique.

(b) On a l'identité $xy = \mathrm{signe}(xy) \cdot \mathrm{ppcm}(x, y) \cdot \mathrm{pgcd}(x, y)$.

Démonstration. Exercice. □

Corps finis

Lemme 10.15. *Soit $n \in \mathbb{N}_{>1}$. Soit $x \in \mathbb{Z}$ tel que $\mathrm{pgcd}(x, n) = 1 = ax + bn$ avec $a, b \in \mathbb{Z}$ (l'identité de Bézout).*
Alors, la classe $\overline{a}$ est un inverse multiplicatif de la classe $\overline{x}$ dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$.

Démonstration. Nous avons $1 = ax + bn \equiv ax \pmod{n}$, donc $\overline{1} = \overline{ax} = \overline{a} \cdot \overline{x}$. □

Corollaire 10.16. *Soit $n \in \mathbb{N}_{>1}$. Alors, le groupe des unités de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \mid x \in \mathbb{Z}, \mathrm{pgcd}(x, n) = 1\}.$$

Démonstration. Dans le lemme 10.15 nous avons vu que toutes les classes $\overline{x}$ pour $x \in \mathbb{Z}$ tel que $\mathrm{pgcd}(x, n) = 1$ sont des unités.
Si $x = py$ et $n = pm$ avec $1 < p \leq n$, alors nous avons $\overline{m} \neq \overline{0}$ et

$$\overline{x} \cdot \overline{m} = \overline{y} \cdot \overline{p} \cdot \overline{m} = \overline{y} \cdot \overline{pm} = \overline{y} \cdot \overline{0} = \overline{0},$$

donc $\overline{x}$ ne peut pas être une unité, car s'il l'était : $\overline{1} = \overline{zx}$, alors

$$\overline{m} = \overline{1}\overline{m} = \overline{zxm} = \overline{z}\overline{0} = \overline{0},$$

une contradiction. □

Corollaire 10.17. *Soit $n \in \mathbb{N}_{>1}$. Les assertions suivantes sont équivalentes :*

(i) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un corps commutatif de cardinal n.

(ii) n est un nombre premier.

Si p est un nombre premier, on note $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$, et on l'appelle le corps fini de cardinal p.

Démonstration. « (i) ⇒ (ii) » : Supposons que n n'est pas un nombre premier, donc $n = ab$ avec $1 < a, b < n$. Alors par le corollaire 10.16 $\overline{a} \neq \overline{0}$ n'est pas une unité de $\mathbb{Z}/n\mathbb{Z}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.
« (ii) ⇒ (i) » : Si n est un nombre premier, tous les $a \in \mathbb{Z}$ tels que $1 \leq a \leq n - 1$ satisfont $\mathrm{pgcd}(a, n) = 1$, donc toutes les classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ sont inversibles. Donc, la seule classe qui n'est pas inversible est $\overline{0}$ et $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Appendice : Unique factorisation en nombres premiers

Dans cet appendice, nous donnons une caractérisation alternative des nombres premiers. Au semestre prochain, cette caractérisation va nous servir de modèle pour une généralisation des nombres premiers dans des anneaux plus généraux que $\mathbb{Z}$. Ici, nous en avons besoin pour démontrer le fait que tout nombre naturel s'écrit de façon (essentiellement) unique comme produit de nombres premiers.
Nous rappelons que nous avons déjà démontré le théorème d'Euclide que le nombre de nombres premiers est infini (théorème 1.5).

Lemme 10.18. *Soit $p \in \mathbb{N}_{>1}$. Les assertion suivantes sont équivalentes :*

(i) p est un nombre premier.

(ii) Pour tout $a, b \in \mathbb{Z}$ on a : si p divise le produit ab, alors p divise a ou p divise b.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soit p un nombre premier tel que $p \nmid a$. On veut montrer $p \mid b$.
Comme $p \nmid a$ et les seuls diviseurs positifs de p sont 1 et p, on a $\mathrm{pgcd}(a, p) = 1$ et l'identité de Bézout $1 = rp + sa$ pour certains $r, s \in \mathbb{Z}$. Puisque p divise ab, il divise aussi sab et brp, donc $p \mid (sab + brp)$, mais

$$sab + brp = (1 - rp)b + brp = b - brp + brp = b,$$

donc $p \mid b$.
« (ii) $\Rightarrow$ (i) » : Supposons que l'assertion (i) est fausse, c'est-à-dire que p n'est pas un nombre premier. Alors $p = ab$ avec $1 < a, b < p$ et $a, b \in \mathbb{N}$. Donc $p \mid p = ab$, mais $p \nmid a$ et $p \nmid b$, donc l'assertion (ii) est fausse. □

Corollaire 10.19. *Soient $p \in \mathbb{N}_{>1}$ un nombre premier, $s \in \mathbb{N}_{\geq 2}$ et $q_1, \ldots, q_s \in \mathbb{Z}$ tels que $p \mid q_1 q_2 \ldots q_s$. Alors il existe $i \in \{1, \ldots, s\}$ tel que $p \mid q_i$.*

Démonstration. Par récurrence pour $s \geq 2$. L'initialisation $s = 2$ est le contenu du lemme 10.18. Supposons que l'assertion est vraie pour un s. Nous allons la démontrer pour $s + 1$. Donc, supposons que $p \mid q_1 q_2 \ldots q_s q_{s+1}$. On le réécrit comme $p \mid ab$ avec $a = q_1 q_2 \ldots q_s$ et $b = q_{s+1}$. Par le lemme 10.18 il suit que $p \mid a$ ou $p \mid b$. Dans le dernier cas $p \mid q_{s+1}$. Dans le premier cas par l'hérédité nous obtenons $p \mid q_i$ pour un $i \in \{1, \ldots, s\}$, donc, l'assertion est vraie pour $s + 1$. □

Lemme 10.20. *Soit $n \in \mathbb{N}_{\geq 2}$. Alors, il existe un nombre premier p qui divise n.*

Démonstration. Nous avons déjà fait cet argument dans la preuve de l'infinitude des nombres premiers. On le refait ici :

$$M := \{m \in \mathbb{N}_{\geq 2} \mid m \text{ divise } n\}.$$

C'est un sous-ensemble de $\mathbb{N}$ qui n'est pas vide (car $n \in M$ comme $n \mid n$). Donc, comme $\mathbb{N}$ est bien ordonné, il existe un plus petit élément $p \in M$. Soit $t \in \mathbb{N}_{>1}$ un diviseur de p. Alors, par le lemme 10.1 (a) on a $t \mid n$, donc $t \in M$. Comme $t \leq p$ et p est le plus petit élément de M, il en suit que $t = p$, donc p est un nombre premier. □

Théorème 10.21 (Théorème fondamental de la théorie élémentaire des nombres)**.** *Tout nombre naturel $n \geq 1$ s'écrit comme produit fini de nombres premiers de façon unique à l'ordre près. ($n = 1$ correspond au produit vide.)*
Plus précisement on a pour tout $n \geq 2$:

(a) Il existe $r \in \mathbb{N}$ et $p_1, \ldots, p_r \in \mathbb{P}$ (des nombres premiers) tel que $n = p_1 p_2 \ldots p_r$.

(b) Si $s \in \mathbb{N}$ et $q_1, \ldots, q_s \in \mathbb{P}$ tels que $n = q_1 q_2 \ldots q_s$, alors $r = s$ et il existe une bijection $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ telle que pour tout $i \in \{1, \ldots, r\}$ on a $q_i = p_{\sigma(i)}$.

Démonstration.
(a) Soit

$$M := \{n \in \mathbb{N}_{\geq 2} \mid n \text{ n'est pas un produit fini de nombres premiers } \}.$$

C'est un sous-ensemble de $\mathbb{N}$. Supposons qu'il n'est pas vide, alors il possède un plus petit élément m. Par le lemme 10.20 il existe un nombre premier p qui divise m. Comme p est un produit de nombres premiers (le produit avec le seul facteur p), on a $p \notin M$, donc $p < m$, donc $2 \leq \frac{m}{p} < m$, donc $\frac{m}{p} \notin M$. Donc $\frac{m}{p}$ est un produit d'éléments premiers, donc $m = p\frac{m}{p}$ l'est aussi. Donc $m \notin M$. Contradiction. Donc M est vide.
(b) Nous démontrons le résultat par récurrence pour $n \geq 1$. Pour $n = 1$ le résultat est clair. Supposons que nous avons déjà démontré le résultat pour tout nombre naturel positif strictement plus petit que n. Montrons-le pour n.
Nous avons donc

$$p_1 p_2 \ldots p_r = n = q_1 q_2 \ldots q_s.$$

Comme $p_1 \mid n$, il suit du corollaire 10.19 qu'il existe un $j \in \{1, \ldots, s\}$ tel que $p_1 \mid q_j$. Comme q_j et p_1 sont des nombres premiers, on a $p_1 = q_j$. En conséquence, nous obtenons

$$p_2 \ldots p_r = \frac{n}{p_1} = q_1 q_2 \ldots q_{j-1} q_{j+1} \ldots q_s.$$

Comme $1 \leq \frac{n}{p_1} < n$, par hérédité $r - 1 = s - 1$ (donc $r = s$) et il existe une bijection $\sigma : \{1, \ldots, j - 1, j + 1, \ldots, r\} \to \{2, 3, \ldots, r\}$ telle que $q_i = p_{\sigma(i)}$ pour tout $i \in \{1, \ldots, j - 1, j + 1, \ldots, r\}$. Nous prolongeons $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ en posant $\sigma(j) = 1$. Evidemment, σ est une bijection. □

11 Les nombres rationnels

Cette section ne sera pas traitée dans le cours, mais il y aura quelques exercices pour vous familiariser avec le contenu. Dans cette section, nous montrons comment les nombres rationnels sont **construits** à partir des entiers relatifs. Donc vous pouvez vous convaincre à l'aide de cette section que les nombres rationnels ont aussi une fondation solide.

Construction des nombres rationnels

Nous avons construit l'anneau $(\mathbb{Z}, +, \cdot, 0, 1)$. Maintenant, nous allons l'utiliser pour une construction des nombres rationnels.

Nous allons définir les fractions comme des classes d'équivalence pour tenir compte du fait que le numérateur et le dénominateur d'une fraction ne sont pas uniques (on peut les multiplier par n'importe quel entier non nul : $\frac{a}{b} = \frac{ac}{bc}$).

Définition-Lemme 11.1. *Sur $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ on définit une relation*

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

C'est une relation d'équivalence.
La classe de (a, x) est formée de tous les (b, y) tel que $ay = bx$, ce qui justifie la notation $\frac{a}{x}$ pour la classe $\overline{(a, x)}$.
L'ensemble quotient est noté $\mathbb{Q}$, l'ensemble des nombres rationnels.

Démonstration. Exercice. □

Proposition 11.2. *Soit $\mathbb{Q}$ l'ensemble quotient du lemme 11.1.*

(a) Les deux applications

$$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$

et

$$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$

sont bien définies, c'est-à-dire que leurs définitions ne dépendent pas des choix des représentants (a, x) et (b, y) des classes $\frac{a}{x}$ et $\frac{b}{y}$.

(b) $(\mathbb{Q}, +, \cdot, \frac{0}{1}, \frac{1}{1})$ est un corps.

(c) L'application

$$\iota : \mathbb{Z} \to \mathbb{Q}, \quad n \mapsto \frac{n}{1}$$

est injective et on a $\iota(n + m) = \iota(n) + \iota(m)$ et $\iota(n \cdot m) = \iota(n) \cdot \iota(m)$.

Démonstration. Exercice. □

L'ordre naturel sur $\mathbb{Q}$

Définition-Lemme 11.3. *(a) Sur $\mathbb{Q}$ on définit une relation d'ordre totale par*

$$\frac{a}{b} \preccurlyeq \frac{c}{d} :\Leftrightarrow ad \leq bc$$

pour $b, d \in \mathbb{N}_{>0}$.

(b) Sur l'image de $\mathbb{Z}$ par l'application naturelle $\iota : \mathbb{Z} \to \mathbb{Q}, \quad n \mapsto \frac{n}{1}$ cet ordre est le même que l'ordre de $\mathbb{Z}$.

Démonstration. La démonstration n'est pas difficile et peut être faite comme exercice. □

À partir de maintenant nous allons écrire $\leq$ au lieu de $\preccurlyeq$.

Lemme 11.4. *Soient $x, y, z \in \mathbb{Q}$ tel que $x \leq y$. Alors :*

(a) $x + z \leq y + z$.

(b) Si $0 \leq z$, *alors* $x \cdot z \leq y \cdot z$.

(c) Si $z \leq 0$, *alors* $y \cdot z \leq x \cdot z$.

Démonstration. La démonstration n'est pas difficile et peut être faite comme exercice. □

La valeur absolue de $\mathbb{Q}$

Définition 11.5. *Pour $r \in \mathbb{Q}$ nous définissons* la valeur absolue de r *par*

$$|x| := \begin{cases} r & \text{si } 0 \leq r, \\ -r & \text{si } r \leq 0. \end{cases}$$

Proposition 11.6. *Pour $r, s \in \mathbb{Q}$ les assertions suivantes sont vraies :*

(a) $|r| \geq 0$ *et* $r = 0 \Leftrightarrow |r| = 0$.

(b) $|r \cdot s| = |r| \cdot |s|$ *(multiplicativité).*

(c) $|r + s| \leq |r| + |s|$ *(inégalité triangulaire).*

(d) Il existe $n \in \mathbb{N}$ tel que $|n| > 1$ (cette propriété « triviale » dit que la valeur propre est « archimédienne » ; il existe aussi des valeurs absolues qui ne sont pas archimédiennes).

Démonstration. (a) La seule chose à montrer est la suivante : Soit $r \leq 0$. Alors, $-1 \cdot 0 = 0 \leq -1 \cdot r = -r$, donc $0 \leq -r$.
(b) Clair.
(c) Nous avons $r \leq |r|$ et $s \leq |s|$ (on le vérifie directement). Donc $r + s \leq |r| + |s|$. De la même manière on conclut de $-r \leq |r|$ et $-s \leq |s|$ que $-(r + s) \leq |r| + |s|$. Les deux ensemble nous donnent : $|r + s| \leq |r| + |s|$.
(d) $|2| = 2 > 1$. □

Corollaire 11.7 (Deuxième inégalité triangulaire)**.** *Pour tout $r, s \in \mathbb{Q}$ on a :*

$$\big||r| - |s|\big| \leq |r + s| \leq |r| + |s|.$$

Démonstration. Nous avons $|r| = |r + s - s| \leq |r + s| + |s|$, donc $|r| - |s| \leq |r + s|$. De la même manière nous avons $|s| - |r| \leq |r + s|$, donc $\big||r| - |s|\big| \leq |r + s|$. □

Les nombres réels

Les nombres réels sont un objet étudié dans vos cours d'Analyse. Pour être complet, nous rajoutons encore une esquisse de la construction des nombres réels à partir des nombres rationnels.
Dans vos cours d'analyse, vous avez défini des suites de Cauchy (dans $\mathbb{Q}$ avec convergence pour la valeur absolue définie ci-dessus). Soit $\mathcal{C}$ l'ensemble de toutes les suites de Cauchy. Soit $\mathcal{N}$ le sous-ensemble de $\mathcal{C}$ des suites de Cauchy qui tendent vers 0.
Sur $\mathcal{C}$ on définit la relation d'équivalence

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} :\Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}} \in \mathcal{N}.$$

L'ensemble quotient de $\mathcal{C}$ modulo cette relation d'équivalence est l'ensemble des nombres réels. Les nombres rationnels s'y plongent via l'application qui envoie $x \in \mathbb{Q}$ sur la suite constante $a_n := x$ pour tout $n \in \mathbb{N}$. On additionne et multiplie deux classes (nombres réels) en additionnant ou multipliant des suites de Cauchy qui représentent ces classes terme par terme.

Chapitre III

Débuts de la théorie des groupes

12 Sous-groupes

Objectifs :

- Apprendre et maîtriser la définition de sous-groupes ;
- apprendre et maîtriser les groupes cycliques ;
- apprendre et maîtriser la génération de sous-groupes ;
- savoir démontrer des propriétés simples.

Nous rappelons d'abord les groupes que nous connaissons déjà :

- $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}^\times, \cdot, 1) = (\{-1, +1\}, \cdot, 1)$.
- $(\mathbb{Q}, +, 0)$, $(\mathbb{Q}^\times, \cdot, 1) = (\mathbb{Q} \setminus \{0\}, \cdot, 1)$.
- $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$, $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot, \overline{1})$.
- $(S_n, \circ, (1))$, le groupe symétrique.

Comme la définition l'exige, il s'agit d'un ensemble avec une « loi de groupe » qui est associative, possède un élément neutre et telle que chaque élément a un inverse. Si la loi de groupe est écrite « multiplicativement », on note l'inverse de a par a^{-1} ; si la loi est notée « additivement », on écrit $-a$ pour l'inverse de a.
Dans cette section nous allons étudier des sous-groupes. L'idée est simple : un sous-groupe d'un groupe est un sous-ensemble qui est « respecté » par la loi de groupe. Nous allons préciser ceci dans la définition suivante.
Regardons un exemple : Considérons $\mathbb{Z}$ comme groupe pour l'addition et deux sous-ensembles :

- $P := \{n \in \mathbb{Z} \mid n \text{ est pair }\}$,
- $I := \{n \in \mathbb{Z} \mid n \text{ est impair }\}$.

Bien que les deux sous-ensembles aient l'air très similaires, ils ne le sont pas du tout du point de vue suivant :
Si $a, b \in P$, alors $a + b \in P$. Mais : si $a, b \in I$, alors $a + b \notin I$. Nous voyons que la loi de groupe respecte P mais pas I.
D'ailleurs, l'élément neutre appartient à $P : 0 \in P$, mais pas à $I : 0 \notin I$. Par contre pour P et I on a que l'inverse de tout élément de l'ensemble y appartient aussi : si $a \in P$, alors $-a \in P$; si $a \in I$, alors $-a \in I$.

Définition 12.1. *Soit $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble. H est appelé* sous-groupe de *G (notation $H \leq G$) si*

- $e \in H$,
- *pour tout $a, b \in H$ on a $a \star b \in H$ (donc, $\star$ se restreint en une application $H \times H \to H$), et*
- *pour tout $a \in H$, l'inverse $a^{-1} \in H$.*

Exemple 12.2.

- *P est un sous-groupe de $(\mathbb{Z}, +, 0)$, mais I ne l'est pas.*
- *Pour tout $n \in \mathbb{Z}$ l'ensemble de tous les multiples de n est aussi un sous-groupe de $(\mathbb{Z}, +, 0)$.*
  En fait, tout sous-groupe de $\mathbb{Z}$ est de cette forme (voir la remarque 16.12).
- *Soit $(G, \star, e)$ un groupe. L'ensemble $\{e\}$ est un sous-groupe de G.*
- *Soit $(G, \star, e)$ un groupe. G est un sous-groupe de G.*
- *$\{-1, +1\} \subseteq \mathbb{Q}$ est un sous-groupe de $(\mathbb{Q}^\times, \cdot, 1)$, mais pas un sous-groupe de $(\mathbb{Q}, +, 0)$.*
- *Soit $S_3 = (S_3, \circ, (1))$ le groupe symétrique en $\{1, 2, 3\}$. Nous considérons l'ensemble $H := \{(1\ \ 2\ \ 3), (1\ \ 3\ \ 2), (1)\}$; c'est un sous-groupe, mais l'ensemble $\{(1\ \ 2), (1\ \ 3), (2\ \ 3), (1)\}$ ne l'est pas.*

Dans ce cours et dans les cours à suivre nous définissons souvent des « sous-objets d'objets » (autre exemple : sous-espace vectoriel) ; à chaque fois on exige que le sous-objet soit un objet du même type : un sous-espace vectoriel est un espace vectoriel ; ici : un sous-groupe est un groupe :

Lemme 12.3. *Soit $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble. Alors, les assertions suivantes sont équivalentes.*

(i) *H est un sous-groupe de G.*

(ii) *On a $\star(H \times H) \subseteq H$, $e \in H$ et $(H, \star, e)$ est un groupe.*

Démonstration. « (i) $\Rightarrow$ (ii) » : C'est clair : l'associativité provient de celle de G ainsi que le fait que e est l'élément neutre. En plus, e appartient à H par définition et les inverses de H y appartiennent aussi par définition.
« (ii) $\Rightarrow$ (i) » : Il suffit de montrer que pour $a \in H$, son inverse a^{-1} (dans le groupe G) appartient à H. Comme $(H, \star, e)$ est un groupe, l'élément a possède un inverse $b \in H$. L'unicité de l'inverse (lemme 7.5) montre que $b = a^{-1}$. □

Le lemme prochain donne un critère qui permet souvent de raccourcir la preuve qu'un sous-ensemble donné est un sous-groupe.

Lemme 12.4 (Critère pour sous-groupes)**.** *Soit $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble non-vide. Alors les assertions suivantes sont équivalentes :*

(i) $H \leq G$ *(H est un sous-groupe de G).*

(ii) Pour tout $a, b \in H$ *on a* $a \star b^{-1} \in H$.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soient $a, b \in H$. Comme H est un sous-groupe, on a $b^{-1} \in H$ et donc $a \star b^{-1} \in H$.
« (ii) $\Rightarrow$ (i) » : Comme H est non-vide, il y existe un élément $a \in H$. L'hypothèse nous donne $a \star a^{-1} \in H$, donc $e \in H$. Pour tout $b \in H$ on obtient $e \star b^{-1} = b^{-1} \in H$. Soient $a, b \in H$, donc $a \star (b^{-1})^{-1} = a \star b \in H$. Nous avons vérifié la définition et concluons que H est un sous-groupe de G. □

Exemple 12.5. *Tout élément du groupe $(\mathbb{Z}, +, 0)$ s'écrit en utilisant seulement 1 (et son inverse -1) ; par exemple $0 = 1 + (-1)$, $5 = 1 + 1 + 1 + 1 + 1$ et $-5 = -1 - 1 - 1 - 1 - 1$.*
On en déduit qu'un sous-groupe de $H \leq \mathbb{Z}$ qui contient 1 est automatiquement égal à $\mathbb{Z}$.

Définition 12.6. *Soit $(G, \star, e)$ un groupe. G est appelé* cyclique *s'il existe $g \in G$ tel que tout élément de G est de la forme g^n pour $n \in \mathbb{Z}$ où*

$$g^n = \begin{cases} e & \text{si } n = 0, \\ \underbrace{g \star g \star \cdots \star g}_{n\text{-fois}} & \text{si } n > 0, \\ \underbrace{g^{-1} \star g^{-1} \star \cdots \star g^{-1}}_{|n|\text{-fois}} & \text{si } n < 0. \end{cases}$$

Exemple 12.7.
- *Le groupe $(\mathbb{Z}, +, 0)$ est cyclique.*
- *Pour tout $n \in \mathbb{N}$ le groupe $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ est cyclique.*

Lemme 12.8. *Tout groupe cyclique est abélien.*

Démonstration. C'est évident : $g^n \star g^m = g^{n+m} = g^{m+n} = g^m \star g^n$ pour tout $n, m \in \mathbb{Z}$. □

Définition 12.9. *Soient $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. On dit que G est* engendré *par M (et que M est un* ensemble de générateurs*) si le seul sous-groupe de G qui contient M est G lui-même.*

Lemme 12.10. *Soit $(G, \star, e)$ un groupe. Les assertions suivantes sont équivalentes :*

(i) G est cyclique.

(ii) Il existe un ensemble de générateurs M de G de cardinal 1.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soit G cyclique avec élément « spécial » g. Si $H \leq G$ est un sous-groupe qui contient g, il contient automatiquement tous les éléments de G, donc $H = G$. Ceci montre que $M = \{g\}$ est un ensemble de générateurs.
« (ii) $\Rightarrow$ (i) » : Soit $M = \{g\}$ un ensemble de générateurs d'un seul élément. On pose $H := \{g^n \mid n \in \mathbb{Z}\}$. C'est un sous-groupe de G à cause du critère du lemme 12.4 : $g^n \star (g^m)^{-1} = g^{n-m} \in H$. Comme $g \in H$, l'hypothèse implique $H = G$, donc, G est cyclique. □

Nous allons maintenant généraliser ceci à un ensemble de générateurs de cardinal quelconque.

Définition-Lemme 12.11. *Soient $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. On pose*

$$\langle M \rangle := \{x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n} \mid n \in \mathbb{N}, x_i \in M, \epsilon_i \in \{-1, 1\}\}.$$

En mots : $\langle M \rangle$ est le sous-ensemble de G de ceux éléments de G qui s'écrivent comme produit d'éléments dans M et leurs inverses. Noter que le cas $n = 0$ (produit vide) correspond à l'élément neutre e. Alors $\langle M \rangle$ est un sous-groupe de G et tout sous-groupe de G qui contient M, contient aussi $\langle M \rangle$. En particulier, $\langle M \rangle$ est engendré par M.
Pour cette raison on l'appelle aussi le sous-groupe de G engendré par M.

Démonstration. Montrons d'abord que $\langle M \rangle$ est un sous-groupe de G en utilisant le lemme 12.4. Soient $x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n}$ et $y_1^{\delta_1} \star y_2^{\delta_2} \star \cdots \star y_m^{\delta_m}$ deux éléments de $\langle M \rangle$. Alors

$$x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n} \star y_m^{-\delta_m} \star \cdots \star y_2^{-\delta_2} \star y_1^{-\delta_1}$$

appartient aussi à $\langle M \rangle$. Donc $\langle M \rangle$ est un sous-groupe de G.
Il est clair que tout sous-groupe H de G qui contient les éléments de M aussi contient leurs inverses et tous les produits finis. Donc $\langle M \rangle \subseteq H$. Cela implique que $\langle M \rangle$ est engendré par M. □

Si G est cyclique de générateur g, alors $G = \langle g \rangle = \langle \{g\} \rangle$. Noter que si G n'est pas abélien, $x_1 \star x_2 \star x_1 \neq x_1^2 \star x_2$ en général.
Nous allons maintenant donner une construction plus abstraite du sous-groupe engendré par un ensemble M. Pour cela nous devons d'abord démontrer que l'intersection de sous-groupe est un sous-groupe.

Lemme 12.12. *Soient $(G, \star, e)$ un groupe, I un ensemble « d'indices » (par ex. $I = \{1, 2, \ldots, n\}$) et pour tout $i \in I$ soit H_i un sous-groupe de G. On pose $H := \bigcap_{i \in I} H_i$, l'intersection de tous les H_i. Alors, H est un sous-groupe de G.*

Démonstration.

- Commes les H_i sont des sous-groupes, on a $e \in H_i$ pour tout $i \in I$. Donc, $e \in \bigcap_{i \in I} H_i = H$.
- Soient $a, b \in \bigcap_{i \in I} H_i = H$. Donc, pour tout $i \in I$ on a $a, b \in H_i$. Comme H_i est un sous-groupe de G, on a $a \star b^{-1} \in H_i$, pour tout $i \in I$. Donc, $a \star b^{-1} \in \bigcap_{i \in I} H_i = H$. Par le lemme 12.4 H est un sous-groupe de G.

□

Proposition 12.13. *Soit $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. Alors*

$$\langle M \rangle = \bigcap_{H \leq G, M \subseteq H} H,$$

l'intersection de tous les sous-groupes H de G qui contiennent M.

Démonstration. Comme $\langle M \rangle$ est un groupe et contient M, on a que $\langle M \rangle$ fait partie des sous-groupes dans l'intersection. Alors nous avons l'inclusion « $\supseteq$ ».
Si H est un sous-groupe de G qui contient M, alors $\langle M \rangle \subseteq H$, donc nous avons l'inclusion « $\subseteq$ ». □

Exemple 12.14. *(a) Le groupe symétrique S_n (avec $n \in \mathbb{N}_{\geq 2}$) est engendré par les transpositions (voir exercices).*

(b) Le group $(M_{2+2}(\mathbb{Z}), +, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right))$ est engendré par les matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

13 Homomorphismes

Objectifs :

- Apprendre et maîtriser la définition de homomorphisme de groupes, de l'image et du noyau ;
- apprendre et maîtriser les propriétés fondamentales des homomorphismes de groupes, de leurs images et de leurs noyaux ;
- savoir démontrer des propriétés simples.

L'idée générale (valable pour groupes, anneaux, espaces vectoriels, etc.) est la suivante : Un (homo)-morphisme est une application qui respecte toutes les structures.

Exemple 13.1.

- *Soient $c : \mathbb{Z} \to \mathbb{Z}$ l'application définie par $n \mapsto 2n$ et $d : \mathbb{Z} \to \mathbb{Z}$ l'application définie par $n \mapsto 2n + 1$. Nous analysons leurs propriétés :*
  - *c et d sont injectives.*
  - *$c(n + m) = 2(n + m) = 2n + 2m = c(n) + c(m)$ pour tout $n, m \in \mathbb{Z}$.*
  - *$c(0) = 0$.*
  - *$d(n + m) = 2(n + m) + 1 \neq (2n + 1) + (2m + 1) = d(n) + d(m)$ pour $n, m \in \mathbb{Z}$.*
  - *$d(0) = 1$.*
  - *L'image de c est l'ensemble P, donc un sous-groupe de $(\mathbb{Z}, +, 0)$.*
  - *L'image de d est l'ensemble I, donc elle n'est pas un sous-groupe de $(\mathbb{Z}, +, 0)$.*

  Première conclusion : L'application c « respecte » la loi de groupe de $(\mathbb{Z}, +, 0)$ et elle envoie l'élément neutre 0 sur l'élément neutre. L'application d n'a aucune de ces deux propriétés.

- *Soit $\iota : \mathbb{Z} \to \mathbb{Q}$ l'injection donnée par $n \mapsto \frac{n}{1}$.*
  - *$\iota(n + m) = \frac{n+m}{1} = \frac{n}{1} + \frac{m}{1} = \iota(n) + \iota(m)$ pour tout $n, m \in \mathbb{Z}$.*

- $\iota(0) = \frac{0}{1}$.
- $\iota(n \cdot m) = \frac{nm}{1} = \frac{n}{1} \cdot \frac{m}{1} = \iota(n) \cdot \iota(m)$ *pour tout* $n, m \in \mathbb{Z}$.
- $\iota(1) = \frac{1}{1}$.

Première conclusion : L'application ι *« transforme » la loi de groupe de* $(\mathbb{Z}, +, 0)$ *en la loi de groupe de* $(\mathbb{Q}, +, 0)$ *et elle envoie l'élément neutre* 0 *pour la première loi sur l'élément neutre* 0 *pour la deuxième loi.*

De plus, l'application ι *« transforme » la loi de groupe de* $(\mathbb{Z}^\times, \cdot, 1) = (\{-1; 1\}, \cdot, 1)$ *en la loi de groupe de* $(\mathbb{Q}^\times, \cdot, 1)$ *et elle envoie l'élément neutre* 1 *pour la première loi sur l'élément neutre* 1 *pour la deuxième loi.*

- *Soit* $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ *l'exponentielle de vos cours d'analyse.*
  - $\exp$ *est une bijection.*
  - $\exp(x + y) = \exp(x) \cdot \exp(y)$ *pour tout* $x, y \in \mathbb{R}$.
  - $\exp(0) = 1$.

  Première conclusion : L'application $\exp$ *« transforme » la loi de groupe de* $(\mathbb{R}, +, 0)$ *en la loi de groupe de* $(\mathbb{R}_{>0}, \cdot, 1)$ *et elle envoie l'élément neutre* 0 *de* $(\mathbb{R}, +, 0)$ *sur l'élément neutre* 1 *de* $(\mathbb{R}_{>0}, \cdot, 1)$.

Ces propriétés nous mènent naturellement à la définition suivante :

Définition 13.2. *Soient* $(G, \star, e)$ *et* $(H, \circ, \epsilon)$ *deux groupes. Une application*

$$\varphi : G \to H$$

est appelée homomorphisme de groupes *si pour tout* $g_1, g_2 \in G$ *on a*

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Notation : Pour être très précis, on écrit les homomorphismes de groupes comme

$$(G, \star, e) \to (H, \circ, \epsilon).$$

Normalement, on est moins précis, et si on écrit : « Soit $\varphi : G \to H$ *un homomorphisme de groupes » on sous-entend que les lois de groupes et les éléments neutres sont fixés et connus du lecteur.*

Exemple 13.3.

- $c : \mathbb{Z} \to \mathbb{Z}$*, donnée par* $n \mapsto 2n$*, est un homomorphisme de groupes de* $(\mathbb{Z}, +, 0)$ *dans* $(\mathbb{Z}, +, 0)$*. Par contre,* d *n'est pas un homomorphisme de groupes.*
- $\iota : \mathbb{Z} \to \mathbb{Q}$*, donnée par* $n \mapsto \frac{n}{1}$ *est un homomorphisme de groupes de* $(\mathbb{Z}, +, 0)$ *dans* $(\mathbb{Q}, +, 0)$.
- $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ *est un homomorphisme de groupes de* $(\mathbb{R}, +, 0)$ *dans* $(\mathbb{R}_{>0}, \cdot, 1)$.
- *Soit* $n \in \mathbb{N}$*. On définit :*

  $$\pi : (\mathbb{Z}, +, 0) \to (\mathbb{Z}/n\mathbb{Z}, +, \overline{0}), \quad a \mapsto \overline{a},$$

  l'application qui envoie a *sur sa classe modulo* n*. C'est un homomorphisme de groupes par le lemme 10.6.*

- *Soit $(G, \star, e)$ un groupe et $H \leq G$ un sous-groupe. L'inclusion $i : H \to G$ (donnée par $h \mapsto h$) est un homomorphisme de groupes.*

Définition 13.4. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, \circ, \epsilon)$ un homomorphisme de groupes.*

- $\mathrm{im}(\varphi) := \varphi(G) := \{\varphi(g) \mid g \in G\}$ *est appelé* l'image de G par φ.
- *Plus généralement, soit $G' \leq G$ un sous-groupe. $\varphi(G') := \{\varphi(g) \mid g \in G'\}$ est appelé* l'image de G' par φ.
- $\ker(\varphi) := \{g \in G \mid \varphi(g) = \epsilon\}$ *est appelé le* noyau de φ *(en allemand* Kern*, en anglais* kernel*).*

Exemple 13.5. *Le noyau de l'homomorphisme*

$$\pi : (\mathbb{Z}, +, 0) \to (\mathbb{Z}/n\mathbb{Z}, +, \overline{0}), \quad a \mapsto \overline{a}$$

est égal à $\{m \mid n$ divise $m\}$, l'ensemble des multiples de n.

Définition-Lemme 13.6. *Soit $n \in \mathbb{N}_{\geq 1}$ et $(S_n, \circ, (1))$ le groupe symétrique. On définit l'application* signe (ou signature) *par*

$$\mathrm{sgn} : S_n \to \{+1, -1\}, \quad \pi \mapsto \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$

C'est un homomorphisme de groupes. Son noyau est noté A_n et appelé le groupe alterné.
Le signe de toute transposition $(i \quad j)$ (avec $i \neq j$) est -1.

Démonstration. Exercice. □

Proposition 13.7 (Propriétés des homomorphismes de groupes)**.** *Soient $(G, \star, e)$ et $(H, *, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, *, \epsilon)$ un homomorphisme de groupes. Alors :*

(a) $\varphi(e) = \epsilon$.

(b) Pour tout $g \in G$ on a : $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(c) Si $G' \leq G$ est un sous-groupe, alors $\varphi(G') \leq H$ est aussi un sous-groupe. En particulier, $\mathrm{im}(\varphi)$ est un sous-groupe de H.

(d) Si $H' \leq H$ est un sous-groupe, alors $\varphi^{-1}(H') \leq G$ est aussi un sous-groupe. (Attention : Ici $\varphi^{-1}(H')$ est l'image réciproque et pas un inverse de l'application !)

(e) Si $\psi : (H, *, \epsilon) \to (I, \otimes, u)$ est un homomorphisme de groupes, alors $\psi \circ \varphi : (G, \star, e) \to (I, \otimes, u)$ est aussi un homomorphisme de groupes.

(f) $\ker(\varphi) \leq G$ *est un sous-groupe.*

Démonstration. (a) On a $\varphi(e) = \varphi(e \star e) = \varphi(e) * \varphi(e)$, donc $\epsilon = \varphi(e) * (\varphi(e))^{-1} = \varphi(e) * \varphi(e) * (\varphi(e))^{-1} = \varphi(e)$.
(b) Par (a) on a $\epsilon = \varphi(e) = \varphi(g \star g^{-1}) = \varphi(g) * \varphi(g^{-1})$. donc, $(\varphi(g))^{-1} = (\varphi(g))^{-1} * \epsilon = (\varphi(g))^{-1} * \varphi(g) * \varphi(g^{-1}) = \varphi(g^{-1})$.
(c) Les éléments dans l'image $\varphi(G')$ sont de la forme $\varphi(g)$ pour $g \in G'$. Soient $\varphi(g_1), \varphi(g_2)$ avec $g_1, g_2 \in G'$ deux éléments de $\varphi(G')$. Comme $g_1 \star g_2^{-1} \in G'$ (car G' est un sous-groupe de G), on conclut que $\varphi(g_1 \star g_2^{-1}) = \varphi(g_1) * \varphi(g_2^{-1}) = \varphi(g_1) * \varphi(g_2)^{-1}$ appartient aussi à $\varphi(G')$ où on utilise (b) pour la dernière égalité. Par le lemme 12.4 nous obtenons donc que $\varphi(G')$ est un sous-groupe de H.
(d) Soit $g_1, g_2 \in \varphi^{-1}(H')$, donc, par définition, cela veut dire $\varphi(g_i) \in H'$ pour $i = 1, 2$. Comme H' est un sous-groupe de H, $\varphi(g_1) * \varphi(g_2)^{-1} \in H'$, donc $\varphi(g_1 \star g_2^{-1}) \in H'$.
(e) Soient $g_1, g_2 \in G$. Alors, $\psi(\varphi(g_1 \star g_2)) = \psi(\varphi(g_1) * \varphi(g_2)) = \psi(\varphi(g_1)) \otimes \psi(\varphi(g_2))$.
(f) Soient $g_1, g_2 \in \ker(\varphi)$. Par définition cela veut dire que $\varphi(g_1) = \epsilon = \varphi(g_2)$. Par (a) et (b) nous avons $\varphi(g_1 \star g_2^{-1}) = \varphi(g_1) * \varphi(g_2)^{-1} = \epsilon * \epsilon^{-1} = \epsilon$, donc $g_1 \star g_2^{-1} \in \ker(\varphi)$. Par le lemme 12.4 nous obtenons donc que $\ker(\varphi)$ est un sous-groupe de G.
On peut aussi remarquer que $\ker(\varphi)$ est l'image réciproque par φ de l'ensemble $\{\epsilon\}$, qui est un sous-groupe de H, et utiliser (d). □

L'utilité du noyau est de caractériser si l'homomorphisme est injectif (comme en algèbre linéaire).

Proposition 13.8. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, \circ, \epsilon)$ un homomorphisme de groupes.*

(a) Les assertions suivantes sont équivalentes :

- *(i)* *φ est surjectif.*
- *(ii)* $H = \mathrm{im}(\varphi)$.

(b) Les assertions suivantes sont équivalentes :

- *(i)* *φ est injectif.*
- *(ii)* $\ker(\varphi) = \{e\}$.

Démonstration. (a) C'est par définition ! On le mentionne ici uniquement à cause de la similarité avec (b).
(b) « (i) $\Rightarrow$ (ii) » : Soit $g \in \ker(\varphi)$. Alors, $\varphi(g) = \epsilon = \varphi(e)$, donc $g = e$ par l'injectivité de φ.
« (ii) $\Rightarrow$ (i) » : Soient $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$. Donc $\epsilon = \varphi(g_2)^{-1} \circ \varphi(g_1) = \varphi(g_2^{-1}) \circ \varphi(g_1) = \varphi(g_2^{-1} \star g_1)$. Alors $g_2^{-1} \star g_1 \in \ker(\varphi) = \{e\}$. Il en suit que $g_2^{-1} \star g_1 = e$, donc $g_1 = g_2$. Cela montre que φ est injectif. □

Définition 13.9. *Un homomorphisme de groupes qui est bijectif est appelé un* isomorphisme.
Parfois on appelle un homomorphisme injectif un monomorphisme *et un homomorphisme surjectif un* épimorphisme. *(Nous n'allons pas utiliser ces deux derniers termes.)*

Lemme 13.10. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes et $\varphi : (G, \star, e) \to (H, \circ, \epsilon)$ un isomorphisme de groupes. Comme φ est bijectif, il existe un inverse $\psi : H \to G$.*
Alors ψ est aussi un homomorphisme de groupes.

Démonstration. Soient $h_1, h_2 \in H$. Nous calculons :

$$\varphi(\psi(h_1) \star \psi(h_2)) = \varphi(\psi(h_1)) \circ \varphi(\psi(h_2)) = h_1 \circ h_2.$$

On applique ψ et obtient :

$$\psi(\varphi(\psi(h_1) \star \psi(h_2))) = \psi(h_1 \circ h_2),$$

donc $\psi(h_1) \star \psi(h_2) = \psi(h_1 \circ h_2)$ et on voit que ψ est un homomorphisme de groupes. □

Définition-Lemme 13.11. *Soit $(G, \star, e)$ un groupe. On pose*

$$\mathrm{Aut}(G) := \{\varphi : G \to G \mid \varphi \text{ est un isomorphisme } \}.$$

Par id_G on note l'identité $G \to G$. Alors, $(\mathrm{Aut}(G), \circ, \mathrm{id}_G)$ est un groupe, appelé groupe des automorphismes de G.

Démonstration. C'est clair ! □

Proposition 13.12. *[Cayley] Soit $(G, \star, e)$ un groupe fini. Soit $S(G) := \{\sigma : G \to G \mid \text{ bijection } \}$. Rappelons que $(S(G), \circ, \mathrm{id}_G)$ est le groupe symétrique sur l'ensemble G.*

(a) Pour $g \in G$ on définit une bijection par

$$\sigma_g : G \to G, \quad h \mapsto g \star h.$$

(b) L'application

$$\varphi : G \to S(G), \quad g \mapsto \sigma_g$$

est un homomorphisme de groupes qui est injectif.

Démonstration. (a) On vérifie qu'il s'agit en effet d'une bijection :

Injectivité Si $\sigma_g(h_1) = \sigma_g(h_2)$, alors par définition $g \star h_1 = g \star h_2$ et en conséquence $h_1 = g^{-1} \star g \star h_1 = g^{-1} \star g \star h_2 = h_2$.

Surjectivité Soit $h \in G$. Alors, $\sigma_g(g^{-1} \star h) = g \star g^{-1} \star h = h$, donc nous avons montré que $h \in \mathrm{im}(\varphi)$.

(b) Soit $h \in G$. Alors :

$$\sigma_{g_1} \circ \sigma_{g_2}(h) = \sigma_{g_1}(g_2 \star h) = g_1 \star (g_2 \star h) = (g_1 \star g_2) \star h = \sigma_{g_1 \star g_2}(h).$$

Donc

$$\varphi(g_1) \circ \varphi(g_2) = \sigma_{g_1} \circ \sigma_{g_2} = \sigma_{g_1 \star g_2} = \varphi(g_1 \star g_2),$$

et φ est un homomorphisme de groupes.
Pour l'injectivité prenons g tel que $\sigma_g = \mathrm{id}_G$. Donc on a $\sigma_g(e) = g \star e = g = \mathrm{id}_G(e) = e$. Donc le seul élément dans le noyau de φ est e et on conclut que φ est injectif. □

14 Le théorème de Lagrange

Objectifs :

- Apprendre et maîtriser les classes d'un groupe suivant un sous-groupe ;
- connaître la définition de l'indice d'un sous-groupe ;
- connaître et savoir démontrer le théorème de Lagrange ;
- savoir démontrer des propriétés simples.

A partir de cette section on utilisera la convention suivante : si on dit « soit G un groupe », on l'écrit multiplicativement $g \cdot h = gh$ et on note 1 son élément neutre.

Définition-Lemme 14.1. *Soit G un groupe et $H \leq G$ un sous-groupe. La relation définie par*

$$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1^{-1} \cdot g_2 \in H$$

est une relation d'équivalence.
Les classes d'équivalence sont de la forme

$$gH = \{g \cdot h \mid h \in H\}$$

et elles s'appellent classes à gauche de G suivant H. *L'ensemble de ces classes est noté G/H.*
Donc, on a

- $G = \bigsqcup_{gH \in G/H} gH$,
- $g_1H \cap g_2H = \begin{cases} \emptyset & \text{si } g_1^{-1}g_2 \notin H, \\ g_1H & \text{si } g_1^{-1}g_2 \in H. \end{cases}$

Un élément $g_2 \in g_1H$ est appelé un représentant. *On a alors $g_1H = g_2H$.*

Démonstration. La vérification que c'est une relation d'équivalence est un exercice. Le reste est une conséquence valable pour toutes les relations d'équivalence (voir la proposition 5.16). □

Exemple 14.2. *$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes à gauche du groupe $\mathbb{Z}$ (pour l'addition) suivant le sous-groupe $n\mathbb{Z}$.*
En effet, dans la définition-lemme 10.5 nous avons défini la relation d'équivalence

$$x \sim_{R_n} y \Leftrightarrow x \equiv y \pmod{n}.$$

Nous avons

$$x \equiv y \pmod{n} \Leftrightarrow x - y \in n\mathbb{Z}.$$

Donc la relation d'équivalence définie dans 10.5 est la même que celle de 14.1.

Définition-Lemme 14.3. *Soit G un groupe et $H \leq G$ un sous-groupe.*

(a) De la même manière que dans la définition-lemme 14.1 on définit les classes à droite de G suivant H*, en utilisant la relation d'équivalence*

$$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1 \cdot g_2^{-1} \in H.$$

Les classes à droites sont de la forme

$$Hg = \{h \cdot g \mid h \in H\}$$

et l'ensemble de toutes ces classes est noté $H\backslash G$*. On a*

- $G = \bigsqcup_{Hg \in H\backslash G} Hg$,
- $Hg_1 \cap Hg_2 = \begin{cases} \emptyset & \text{si } g_1 g_2^{-1} \notin H, \\ Hg_1 & \text{si } g_1 g_2^{-1} \in H. \end{cases}$

(b) L'application

$$\phi : G/H \to H\backslash G, \quad gH \mapsto Hg^{-1}$$

est bijective.

Démonstration. C'est clair ! (Noter pour (b) que $Hg^{-1} = (gH)^{-1}$ parce que $H^{-1} = H$.) □

Lemme 14.4. *Soient G un groupe et $H \leq G$ un sous-groupe. Pour tout $g_1, g_2 \in G$ l'application*

$$g_1 H \longrightarrow g_2 H, \quad g_1 h \mapsto (g_2 g_1^{-1}) g_1 h = g_2 h$$

est bijective. Donc $\#H = \#gH$ pour tout $g \in G$ (les deux peuvent être infinis).

Démonstration. La surjectivité est évidente. Regardons donc l'injectivité : $g_2 h_1 = g_2 h_2$ implique $g_2^{-1} g_2 h_1 = g_2^{-1} g_2 g_2 h_2$, donc $h_1 = h_2$. □

Définition 14.5. *Soient G un groupe et $H \leq G$ un sous-groupe.* L'indice de H dans G *est défini par*

$$(G : H) := \#G/H = \#H\backslash G$$

(il peut être infini).

Théorème 14.6 (Lagrange)**.** *Soient G un groupe et $H \leq G$ un sous-groupe. Alors :*

$$\#G = (G : H) \cdot \#H.$$

Démonstration. C'est une conséquence immédiate de la réunion disjointe $G = \bigsqcup_{gH \in G/H} gH$ et le fait $\#H = \#gH$ pour tout $g \in G$ par le lemme 14.4.
Plus précisement, on va distinguer les cas $\#G = \infty$ et $\#G < \infty$. Si $\#G = \infty$, il suit de la réunion disjointe que $\#H = \#gH$ est infini ou $(G : H)$ est infini. Dans les deux cas, le produit $(G : H) \cdot \#H$ est infini. Si $\#G < \infty$, il est clair que $(G : H)$ et $\#H$ sont tous les deux finis. La formule est maintenant claire. □

Corollaire 14.7. *Soient G un groupe fini et $H \leq G$ un sous-groupe. Alors, $\#H$ divise $\#G$ et l'indice $(G : H)$ divise $\#G$.*

Démonstration. Cela suit directement du théorème de Lagrange 14.6 $\#G = (G : H) \cdot \#H$ car l'indice est entier. □

Exemple 14.8. *(a) Si H est un sous-groupe de S_3, sa cardinalité ne peut pas être 4 ou 5 car les seuls diviseurs de $\#S_3 = 6$ sont $1, 2, 3, 6$. Il existe des sous-groupes de cardinal $1, 2, 3, 6$ (trouvez les vous-mêmes !).*

(b) Si $H \lneq S_4$ est un sous-groupe, sa cardinalité est inférieure ou égale à 12 et elle ne peut pas être $5, 7, 9, 10, 11$ car les seuls diviseurs de $\#S_4 = 24$ sont $1, 2, 3, 4, 6, 8, 12$.

(c) Le groupe S_5 de cardinal 120 ne possède pas de sous-groupe de cardinal 15 (c'est un exercice).

Noter : $15 \mid 120$. Donc en général, pour un diviseur n de $\#G$ il n'existe pas de sous-groupe de G de cardinal n.

15 Ordres

Objectifs :

- Apprendre et maîtriser l'ordre d'un élément dans un groupe ;
- connaître et savoir démontrer le 'petit Fermat de la théorie des groupes' à partir du théorème de Lagrange ;
- connaître et savoir démontrer la classification des groupes cycliques ;
- asvoir appliquer les résultats à la classification des groupes de très petit cardinal ;
- savoir démontrer des propriétés simples.

Soient G un groupe et $g \in G$. Rappelons la définition de g^n pour tout $n \in \mathbb{Z}$ (voir la définition 12.6) :

$$g^n = \begin{cases} 1 & \text{si } n = 0, \\ \underbrace{g \cdot g \cdot \ldots \cdot g}_{n\text{-fois}} & \text{si } n > 0, \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{|n|\text{-fois}} & \text{si } n < 0. \end{cases}$$

On rappelle que l'ordre ou le cardinal de G est son nombre d'éléments (si G est infini, alors on dit que son ordre est infini). Maintenant, on définit l'ordre d'un élément d'un groupe.

Définition 15.1. *Soit G un groupe. Pour un élément $g \in G$ on définit* l'ordre *de g (notation : $\mathrm{ord}(g)$) comme le plus petit entier positif $n > 0$ tel que $g^n = 1$, l'élément neutre (si un tel n n'existe pas, alors on dit que $\mathrm{ord}(g) = \infty$).*

Exemple 15.2.

- *Dans tout groupe, l'ordre de l'élément neutre est* 1 *et c'est le seul élément d'ordre* 1.

  Raison : $g = g^1 = 1$.

- *Les ordres des éléments du groupe symétrique* S_3 *sont les suivants :*

$$\operatorname{ord}\big((1)\big) = 1, \ \operatorname{ord}\big((1\ 2)\big) = 2, \ \operatorname{ord}\big((1\ 3)\big) = 2,$$
$$\operatorname{ord}\big((2\ 3)\big) = 2, \ \operatorname{ord}\big((1\ 2\ 3)\big) = 3, \ \operatorname{ord}\big((1\ 3\ 2)\big) = 3.$$

- *Les ordres des éléments de* $(\mathbb{Z}/6\mathbb{Z}, +, \overline{0})$ *sont les suivants :*

$$\operatorname{ord}(\overline{0}) = 1, \ \operatorname{ord}(\overline{1}) = 6, \ \operatorname{ord}(\overline{2}) = 3, \ \operatorname{ord}(\overline{3}) = 2, \ \operatorname{ord}(\overline{4}) = 3, \ \operatorname{ord}(\overline{5}) = 6.$$

  Donc $\mathbb{Z}/6\mathbb{Z}$ *est un groupe cyclique qui peut être engendré par* $\overline{1}$ *ou* $\overline{5} = \overline{-1}$.

- *Dans* $(\mathbb{Z}, +, 0)$*, l'ordre de tout* $0 \neq m \in \mathbb{Z}$ *est infini (car* $nm \neq 0$ *pour tout* $n \in \mathbb{N}_{>0}$*).*

Lemme 15.3. *Soient* G *un groupe et* $g \in G$.

(a) On suppose $n = \operatorname{ord}(g) < \infty$*. Soit* $m \in \mathbb{Z}$*. Alors,* $g^m = 1$ *si et seulement si* $n \mid m$.

(b) Soit $m \in \mathbb{N}$ *tel que* $m < \operatorname{ord}(g)$*. Alors, les éléments* $1, g, g^2, \ldots, g^m$ *sont deux à deux distincts.*

Démonstration. (a) Supposons d'abord $m = nq$ avec $q \in \mathbb{Z}$. Alors, $g^m = g^{nq} = (g^n)^q = 1^q = 1$.
Soit maintenant $m \in \mathbb{Z}$ tel que $g^m = 1$. La division euclidienne nous donne $m = q \operatorname{ord}(g) + r$ avec $0 \leq r \leq \operatorname{ord}(g) - 1$. Donc $1 = g^m = (g^{\operatorname{ord}(g)})^q \cdot g^r = 1^q \cdot g^r = g^r$. La seule possibilité est $r = 0$ car sinon l'existence de r contradirait la définition de l'ordre.
(b) On suppose que l'assertion est fausse. Alors, on a $g^a = g^b$ avec $0 \leq a < b \leq m$, ce qui donne $g^{b-a} = 1$, une contradiction car $0 < b - a \leq m < \operatorname{ord}(g)$. □

Rappelons aussi la notation $\langle g_1, \ldots, g_r \rangle$ pour le sous-groupe de G engendré par $g_1, \ldots, g_r \in G$. Ce sous-groupe est l'ensemble de tous les éléments de G qui s'écrivent comme produit fini de

$$g_1, \ldots, g_r, g_1^{-1}, \ldots, g_r^{-1}$$

où on peut utiliser les éléments plusieurs (ou aucune) fois et dans un ordre quelconque. En particulier, $\langle g \rangle$ est l'ensemble $\{g^m \mid m \in \mathbb{Z}\}$.

Proposition 15.4. *Soient* G *un groupe et* $g \in G$*. Alors,*

$$\operatorname{ord}(g) = \#\langle g \rangle.$$

En mots : l'ordre du sous-groupe engendré par g *est égal à l'ordre de* g.

Démonstration. Supposons d'abord que $\operatorname{ord}(g)$ est infini. Alors pour tout $m \in \mathbb{N}$ les éléments $1, g, g^2, \ldots, g^m$ sont distincts par le lemme 15.3 (b), donc $\langle g \rangle$ est un groupe de cardinal infini.
Supposons maintenant $\operatorname{ord}(g) = n < \infty$. Alors les n éléments $1, g, g^2, \ldots, g^{n-1} \in \langle g \rangle$ sont distincts, encore par le lemme 15.3 (b). On montre que $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{n-1}\}$. Soit donc $g^m \in \langle g \rangle$. On utilise la division euclidienne pour écrire $m = qn + r$ avec $0 \leq r < n$. Nous avons $g^m = g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r$. Cela montre l'inclusion « $\subseteq$ ». L'autre inclusion est triviale. □

Corollaire 15.5. *Soient G un groupe fini et $g \in G$. Alors $\mathrm{ord}(g) \mid \#G$.*
En mots : l'ordre de tout élément divise l'ordre du groupe.

Démonstration. Par le corollaire 14.7 du théorème de Lagrange et la proposition 15.4 on a $\mathrm{ord}(g) = \#\langle g \rangle \mid \#G$. □

Corollaire 15.6 (« Petit théorème de Fermat de la théorie des groupes »)**.** *Soit G un groupe fini. Alors, pour tout $g \in G$ on a $g^{\#G} = 1$.*

Démonstration. Cela suit directement du corollaire 15.5 et du lemme 15.3 (a). □

Lemme 15.7. *Soit G un groupe fini de cardinal n. Alors, G est cyclique si et seulement s'il existe $g \in G$ tel que $\mathrm{ord}(g) = n$.*

Démonstration. C'est clair. □

Corollaire 15.8. *Soit G un groupe fini tel que son cardinal $\#G$ est un nombre premier. Alors G est cyclique.*

Démonstration. Soit $p = \#G$, un nombre premier par hypothèse. Soit $g \in G$ différent de 1. Comme $\mathrm{ord}(g)$ divise p (par le corollaire 15.5) et $\mathrm{ord}(g) \neq 1$, alors $\mathrm{ord}(g) = p$, donc G est cyclique par le lemme 15.7. □

Corollaire 15.9. *Soient G un groupe et $H_1, H_2 \leq G$ deux sous-groupes finis de G.*
Si $\mathrm{pgcd}(\#H_1, \#H_2) = 1$, alors $H_1 \cap H_2 = \{1\}$.

Démonstration. Soit $g \in H_1 \cap H_2$. Donc $\mathrm{ord}(g) \mid \#H_1$ et $\mathrm{ord}(g) \mid \#H_2$, donc $\mathrm{ord}(g) = 1 = \mathrm{pgcd}(\#H_1, \#H_2)$, donc $H_1 \cap H_2 = \{1\}$. □

Proposition 15.10 (Classification des groupes cycliques)**.** *Soit G un groupe cyclique.*

(a) Si $n = \#G$ est fini, alors G est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$.

(Si on dit que deux groupes sont isomorphes, cela veut dire qu'il existe un isomorphisme de groupes entre les deux.)

(b) Si G n'est pas fini, alors G est isomorphe au groupe $(\mathbb{Z}, +, 0)$.

Démonstration. Soit g un générateur de G.
(a) L'application

$$\varphi : \mathbb{Z}/n\mathbb{Z} \to G, \quad \overline{a} \mapsto g^a$$

est bien définie et un isomorphisme de groupes. Effectivement, elle ne dépend pas du représentant a de la classe $\overline{a}$ modulo n car $g^{a+bn} = g^a(g^n)^b = g^a$. Elle est clairement un homomorphisme de groupes surjectif, donc bijective car le cardinal de $\mathbb{Z}/n\mathbb{Z}$ et de G est n.
(b) Comme G n'est pas fini, $\mathrm{ord}(g)$ n'est pas fini non plus. L'application

$$\varphi : \mathbb{Z} \to G, \quad a \mapsto g^a$$

est un isomorphisme de groupes. Effectivement, elle est clairement un homomorphisme de groupes surjectif. Si $g^a = g^b$ avec $a \neq b$, alors $g^{b-a} = 1$ donc g est d'ordre fini, contradiction. □

Proposition 15.11. *Soient G un groupe et $g \in G$ un élément d'ordre fini. Alors pour tout $i \in \mathbb{N}_{>0}$ on a*

$$\mathrm{ord}(g^i) = \frac{\mathrm{ppcm}(i, \mathrm{ord}(g))}{i} = \frac{\mathrm{ord}(g)}{\mathrm{pgcd}(i, \mathrm{ord}(g))}.$$

En particulier, si $i \mid \mathrm{ord}(g)$, alors $\mathrm{ord}(g^i) = \frac{\mathrm{ord}(g)}{i}$.

Démonstration. Comme $(g^i)^{\mathrm{ord}(g)} = (g^{\mathrm{ord}(g)})^i = 1$, il est clair que $\mathrm{ord}(g^i) < \infty$. Soit $m = \mathrm{ord}(g)$. On cherche le $n \geq 1$ minimal tel que

- $m \mid n$ ($\Leftrightarrow g^n = 1$) et
- $i \mid n$ ($\Leftrightarrow g^n = (g^i)^{n/i}$).

Donc, $n = \mathrm{ppcm}(m, i)$ et $\mathrm{ord}(g^i) = \frac{n}{i} = \frac{\mathrm{ppcm}(i,m)}{i} = \frac{\mathrm{ppcm}(i,m)\cdot\mathrm{pgcd}(i,m)}{i\cdot\mathrm{pgcd}(i,m)} = \frac{i\cdot m}{i\cdot\mathrm{pgcd}(i,m)} = \frac{m}{\mathrm{pgcd}(i,m)}$. □

Définition-Lemme 15.12. *Soit I un ensemble et pour tout i soit G_i un groupe. Alors le produit cartésien $\prod_{i\in I} G_i$ est un groupe, appelé* produit direct de G_i, $i \in I$, *pour la loi de groupe*

$$\cdot : \prod_{i\in I} G_i \times \prod_{i\in I} G_i \to \prod_{i\in I} G_i, \quad (g_i)_{i\in I} \cdot (h_i)_{i\in I} := (g_i \cdot h_i)_{i\in I}$$

et l'élément neutre $(1)_{i\in I}$.

Démonstration. Le cas $I = \{1, 2\}$ est un exercice. Le cas général marche de la même manière. □

Lemme 15.13. *Soient G un groupe abélien fini et $H_1, H_2 \leq G$ deux sous-groupes de G. Si $H_1 \cap H_2 = \{1\}$ (ce qui est le cas, en particulier, si $\mathrm{pgcd}(\#H_1, \#H_2) = 1$ par le corollaire 15.9), alors l'application $\phi : H_1 \times H_2 \to G$ donnée par $(h_1, h_2) \mapsto h_1h_2$ est un homomorphisme de groupes injectif.*

Démonstration. **Homomorphisme** On calcule

$$\phi((h_1, h_2)(h_1', h_2')) = \phi((h_1h_1', h_2h_2')) = h_1h_1'h_2h_2' \overset{\text{abélien}}{=} h_1h_2h_1'h_2' = \phi((h_1, h_2))\phi((h_1', h_2')).$$

Injectivité $\phi((h_1, h_2)) = h_1h_2 = 1$, donc $h_1 = h_2^{-1} \in H_1 \cap H_2 = \{1\}$, donc $h_1 = h_2 = 1$.

□

Exemple 15.14. *Nous faisons la liste de tous les groupes d'ordre ≤ 7 à isomorphisme près.*

- *Le seul groupe d'ordre 1 est le groupe trivial ; son seul élément est l'élément neutre.*
- *$n = 2, 3, 5, 7$. Comme tout groupe d'ordre premier est cyclique par le corollaire 15.8, il en suit que le seul groupe d'ordre n à isomorphisme près est $\mathbb{Z}/n\mathbb{Z}$.*

- $n = 4$ *: Nous connaissons deux groupes d'ordre* 4 *:* $\mathbb{Z}/4\mathbb{Z}$ *et* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *qui ne sont pas isomorphes (le premier est cyclique et le deuxième non-cyclique). On va démontrer qu'il n'y en a pas plus ; on verra notamment que tout groupe d'ordre* 4 *est abélien (c'était déjà un exercice).*

  Soit G *un groupe d'ordre* 4 *qui n'est pas cyclique (s'il est cyclique, il est isomorphe à* $\mathbb{Z}/4\mathbb{Z}$*). On choisit* $a \neq b$ *deux éléments de* G *qui ne sont pas l'élément neutre. On a* $\mathrm{ord}(a) \mid \#G$*, donc* $\mathrm{ord}(a) = 2$*, car s'il était* 4*, le groupe serait cyclique engendré par* a*. Le même argument montre* $\mathrm{ord}(b) = 2$*. On a* $\langle a \rangle \cap \langle b \rangle = \{1\}$*. Soit* $c := ab$*. Il est clair que* $c \neq 1, a, b$*. Par le même argument* $ba \neq 1, a, b$*, donc* $c = ba$*. Donc* G *est abélien. Par le lemme 15.13 nous obtenons que* $\langle a \rangle \times \langle b \rangle$ *est isomorphe à* G*. Donc* $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*.*

- $n = 6$*. Nous connaissons deux groupes d'ordre* 6 *:* $\mathbb{Z}/6\mathbb{Z}$ *et* S_3 *qui ne sont pas isomorphes (par exemple : le premier est abélien et le deuxième non-abélien). On va démontrer qu'il n'y en a pas plus.*

  Soit G *un groupe d'ordre* 6 *qui n'est pas cyclique (s'il est cyclique, il est isomorphe à* $\mathbb{Z}/6\mathbb{Z}$*). Alors, tout élément* $1 \neq g \in G$ *doit être d'ordre* 2 *ou* 3 *car l'ordre doit être un diviseur de* $\#G = 6$ *et* $\mathrm{ord}(g) = 6$ *dirait que* G *est cyclique :* $\langle g \rangle = G$*.*

  On montre d'abord qu'il existe $a, b \in G$ *tels que* $\mathrm{ord}(a) = 3$ *et* $\mathrm{ord}(b) = 2$ *(cela est une conséquence directe du théorème de Sylow (que l'on verra plus tard)).*

  Supposons qu'il n'existe pas d'élément d'ordre 3*. Dans ce cas, tous les éléments non-neutres sont d'ordre* 2*. En conséquence* G *est abélien (par un exercice). Soient* $b_1 \neq b_2 \in G$ *deux éléments d'ordre* 2*. Alors, l'homomorphisme injectif* $\phi : \langle b_1 \rangle \times \langle b_2 \rangle \to G$ *du lemme 15.13 (noter :* $\langle b_1 \rangle \cap \langle b_2 \rangle = \{1\}$*) implique que l'image de* ϕ *est un sous-groupe d'ordre* 4*. Cela est une contradiction au corollaire 14.7. Donc, il existe* $a \in G$ *d'ordre* 3*.*

  On choisit $b \notin \langle a \rangle =: H$*. Comme* $G = H \sqcup bH$*, il en suit que* $b^2 \in H$ *ou* $b^2 \in bH$*. Le deuxième cas est impossible (sinon* b *serait dans* H*). Donc* $b^2 \in H$*. Donc* $\mathrm{ord}(b^2)$ *est* 1 *ou* 3 *(par la proposition 15.11). Le dernier cas mènerait à* $\mathrm{ord}(b) = 6$ *qui est exclu. Donc* $\mathrm{ord}(b) = 2$*.*

  Notons que $ab \neq 1, a, a^2, b$*. On a aussi* $a^2b \neq 1, a, a^2, b, ab$*. Donc* $G = \{1, a, a^2, b, ab, a^2b\}$*. Si* $ba = ab$*, alors* G *serait abélien et dans ce cas* $\mathrm{ord}(ab) = 6$ *(pour voir cela, il suffit de calculer* $ab \neq 1$*,* $(ab)^2 = a^2b^2 = a^2 \neq 1$ *et* $(ab)^3 = a^3b^3 = b^2b = b \neq 1$*) et le groupe serait cyclique ce que nous supposons ne pas être le cas. La seule autre possiblité est* $ba = a^2b$*.*

  Dans S_3 *nous posons* $A := (1\ \ 2\ \ 3)$ *et* $B := (1\ \ 2)$*. Nous définissons* $\phi : S_3 \to G$ *par* $\phi(\mathrm{id}) = 1$*,* $\phi(A) = a$*,* $\phi(A^2) = a^2$*,* $\phi(B) = b$*,* $\phi(AB) = ab$*, et* $\phi(A^2B) = a^2b$*. C'est clairement une bijection. Que c'est un homomorphisme est une conséquence de* $\mathrm{ord}(A) = 3$*,* $\mathrm{ord}(B) = 2$ *et* $BA = A^2B$ *qui est facilement vérifié.*

16 Sous-groupes distingués et quotients

Objectifs :

- Apprendre et maîtriser la notion de sous-groupe distingué ;
- connaître la définition de quotients d'un groupe par un sous-groupe distingué ;

- connaître pourquoi la normalitité est nécessaire ;
- savoir calculer dans les quotients ;
- connaître et savoir appliquer les théorèmes d'isomorphisme ;
- savoir démontrer des propriétés simples.

Soit G un groupe et $H \subseteq G$ un sous-groupe. Nous avons défini les *classes à gauche suivant* H comme les ensembles

$$gH = \{gh \mid h \in H\}$$

et les *classes à droite suivant* H comme les ensembles

$$Hg = \{hg \mid h \in H\}.$$

On rappelle également que l'ensemble des classes à gauche est noté G/H et celui des classes à droite est noté $H\backslash G$.
Revenons à notre premier exemple : Soit $n \in \mathbb{N}_{\geq 1}$. Par la division euclidienne tout $m \in \mathbb{Z}$ s'écrit de façon unique comme

$$m = qn + r$$

avec $q \in \mathbb{Z}$ et un « reste » $0 \leq r \leq n-1$. Pour $a, b \in \mathbb{Z}$, les assertions suivantes sont équivalentes :

(i) a et b ont le même reste dans la division euclidienne par n ;

(ii) $a \in \overline{b} := b + n\mathbb{Z} = \{b + nm \mid m \in \mathbb{Z}\}$;

(iii) $a - b \in n\mathbb{Z}$;

(iv) $n \mid (a - b)$;

(v) $a \equiv b \mod n$.

On considère le groupe $(\mathbb{Z}, +, 0)$ et son sous-groupe $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$. Comme $\mathbb{Z}$ est commutatif (abélien), les classes à gauche et les classes à droite sont les mêmes :

$$b + n\mathbb{Z} = \{b + nm \mid m \in \mathbb{Z}\} = \{nm + b \mid m \in \mathbb{Z}\} = n\mathbb{Z} + b.$$

Nous avons donc $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Nous rappelons aussi le fait important qu'on a une addition sur $\mathbb{Z}/n\mathbb{Z}$ qui en fait un groupe (d'élément neutre $\overline{0}$).
Notre but maintenant est d'essayer d'imiter la loi de groupe de $\mathbb{Z}/n\mathbb{Z}$ pour définir une loi de groupe sur G/H pour les cas où cela est possible.
L'addition de $\mathbb{Z}/n\mathbb{Z}$ est basée sur l'observation suivante :
Observation fondamentale : Soient $a, a', b, b' \in \mathbb{Z}$ tels que

$$a \equiv a' \mod n \quad \text{et} \quad b \equiv b' \mod n.$$

Alors,

$$a + b \equiv a' + b' \mod n.$$

Nous en rappelons la démonstration : Comme $n \mid (a' - a)$ et $n \mid (b' - b)$, il existe $c, d \in \mathbb{Z}$ tels que $a' = a + cn$ et $b' = b + dn$; donc $a' + b' = a + b + (c + d)n$ et n divise $(a' + b') - (a + b)$.
On rappelle la définition de l'addition sur $\mathbb{Z}/n\mathbb{Z}$; seulement pour l'instant nous la notons $\oplus$ pour bien la distinguer de l'addition sur $\mathbb{Z}$. On définit la somme de $\overline{a} = (a + n\mathbb{Z})$ et $\overline{b} = (b + n\mathbb{Z})$ comme

$$\overline{a} \oplus \overline{b}a + n\mathbb{Z} \oplus b + n\mathbb{Z} := \overline{a + b} = (a + b) + n\mathbb{Z}.$$

Il ne s'agit pas de la somme de deux entiers, mais d'une somme de deux *ensembles d'entiers* ! Comme $\oplus$ doit être une application, nous avons besoin d'une règle qui à deux classes données associe une troisième classe. C'est ici que l'observation fondamentale intervient ; elle donne :

> Soient a et a' deux représentants de la même classe, c'est-à-dire $a' + n\mathbb{Z} = a + n\mathbb{Z}$; soient b et b' aussi dans la même classe : $b' + n\mathbb{Z} = b + n\mathbb{Z}$.
>
> Alors $a' + b'$ et $a + b$ représentent aussi la même classe : $(a' + b') + n\mathbb{Z} = (a + b) + n\mathbb{Z}$.

Cela veut dire : *la classe $(a + b) + n\mathbb{Z}$ ne dépend que de la classe de a et de la classe de b.*
Essayons de faire la même chose pour un groupe quelconque. Traduisons d'abord l'observation fondamentale en langage des classes à gauche :

$$a + n\mathbb{Z} = a' + n\mathbb{Z} \ \wedge \ b + n\mathbb{Z} = b' + n\mathbb{Z} \Rightarrow (a + b) + n\mathbb{Z} = (a' + b') + n\mathbb{Z}.$$

Nous étudions maintenant à quel point on obtient le résultat analogue dans le contexte général. Soient $x, x', y, y' \in G$:

$$xH = x'H \ \wedge \ yH = y'H \overset{?}{\Rightarrow} (xy)H = (x'y')H.$$

Les assertions $xH = x'H$ et $yH = y'H$ sont équivalentes à $x^{-1}x' \in H$ et $y^{-1}y' \in H$. On veut obtenir $(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' \in H$.

Lemme 16.1. *Soit G un groupe et $H \subseteq G$ un sous-groupe. Alors les assertions suivantes sont équivalentes :*

(i) Pour tout $x, x', y, y' \in G$ on a : $xH = x'H \ \wedge \ yH = y'H \Rightarrow (xy)H = (x'y')H$.

(ii) Pour tout $g \in G$ et tout $h \in H$ on a $g^{-1}hg \in H$.

(iii) Pour tout $g \in G$ on a $gH = Hg$.

Définition 16.2. *Un sous-groupe $H \leq G$ est appelé* normal/distingué *(notation : $H \trianglelefteq G$; anglais : normal subgroup, allemand : Normalteiler) si les assertions équivalentes du lemme 16.1 sont satisfaites.*

Exemple 16.3. *Si G est abélien, tout sous-groupe $H \leq G$ est normal. En particulier, $n\mathbb{Z}$ est normal dans $\mathbb{Z}$.*

Démonstration. « (i) $\Rightarrow$ (ii) » : Soient $g \in G$ et $h \in H$. On pose $y = y' = g$, $x = 1$ et $x' = h$. Cela donne par (i) : $g^{-1}hg = y^{-1}x^{-1}x'y' \in H$.
« (ii) $\Rightarrow$ (iii) » : Soit $g \in G$. Par (ii) nous avons $Hg \subseteq gH$. En appliquant (ii) aussi avec g^{-1} (au lieu de g), nous avons $gH \subseteq Hg$, donc l'égalité $gH = Hg$.
« (iii) $\Rightarrow$ (i) » : Soient $x, x', y, y' \in G$. On pose $g = y$, $h = x^{-1}x' \in H$ et $h' = y^{-1}y' \in H$. Alors par (iii) nous avons $g^{-1}hg \in H$, donc $g^{-1}hgh' = y^{-1}x^{-1}x'yy^{-1}y' = y^{-1}x^{-1}x'y' \in H$, donc $(xy)H = (x'y')H$. □

Nous avons donc trouvé une généralisation de l'observation fondamentale sous l'hypothèse que le sous-groupe H soit distingué. Cela nous permet de définir une loi de groupe sur G/H (et donc aussi sur $H\backslash G$ car $gH = Hg$ pour tout $g \in G$).

Proposition 16.4. *Soit $(G, \cdot, 1)$ un groupe et $H \trianglelefteq G$ un sous-groupe normal.*

(a) L'application

$$\star : G/H \times G/H \to G/H, \quad (g_1H, g_2H) \mapsto g_1H \star g_2H := (g_1g_2)H$$

est bien définie.

(b) $(G/H, \star, H)$ est un groupe, appelé quotient de G par H (en allemand on dit soit Quotient soit Faktorgruppe).

(c) L'application

$$\pi : G \to G/N, \quad g \mapsto gN$$

est un homomorphisme de groupes surjectif, appelé projection naturelle. *On a* $\ker(\pi) = N$.

Démonstration. (a) En effet, le lemme 16.1 montre que la définition ne dépend pas du choix des représentants.
(b)

Associativité $(g_1H \star g_2H) \star g_3H = (g_1g_2)H \star g_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = g_1H \star (g_2g_3)H = g_1H \star (g_2H \star g_3H)$ pour tout $g_1H, g_2H, g_3H \in G/H$.

Existence du neutre $gH \star H = (g1)H = gH$ pour tout $gH \in G/H$.

Existence d'inverse $gH \star g^{-1}H = (gg^{-1})H = H$ pour tout $gH \in G/H$.

(c)

Surjectivité Clair.

Homomorphisme $\pi(gh) = (gh)H = gH \star hH = \pi(g) \star \pi(h)$ pour tout $g, h \in G$.

Noyau $\pi(g) = gH = H$ si et seulement si $g \in H$.

□

Exemple 16.5. *(a) $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ est le quotient de $(\mathbb{Z}, +, 0)$ par le sous-groupe distingué $(n\mathbb{Z}, +, 0)$.*

(b) Noter que (b) dit que tout sous-groupe normal $H \trianglelefteq G$ est le noyau d'un homomorphisme de groupes : de la projection naturelle.

Nous venons de voir dans l'exemple précédent que tout sous-groupe normal est le noyau d'un homomorphisme de groupes. En fait, tout noyau d'un homomorphisme de groupes est normal :

Proposition 16.6. *Soit $\varphi : G_1 \to G_2$ un homomorphisme de groupes. Alors, le* noyau de φ *est un sous-groupe normal de G_1.*

Démonstration. Nous savons déjà que $\ker(\varphi)$ est un sous-groupe de G_1. Montrons qu'il est normal. Soient $h \in \ker(\varphi)$ et $g \in G$. Utilisant la propriété que φ est un homomorphisme de groupes, nous avons

$$\varphi(g^{-1}\cdot h\cdot g) = \varphi(g^{-1})\cdot\varphi(h)\cdot\varphi(g) = \varphi(g^{-1})\cdot e_2\cdot\varphi(g) = \varphi(g^{-1})\cdot\varphi(g) = \varphi(g^{-1}\cdot g) = \varphi(e_1) = e_2.$$

Donc $g^{-1}\cdot h\cdot g \in \ker(\varphi)$, montrant que $\ker(\varphi)$ est normal. □

Exemple 16.7. *Soit $n \in \mathbb{N}_{\geq 2}$. Alors, le groupe alterné A_n est un sous-groupe normal du groupe symétrique S_n car c'est le noyau de* sgn.

Proposition 16.8. *Soit $\varphi : G \to L$ un homomorphisme de groupes.*

(a) Si $H \trianglelefteq L$ est un sous-groupe normal, alors l'image réciproque $\varphi^{-1}(H) \trianglelefteq G$ est un sous-groupe normal.

(b) $\ker(\varphi) \trianglelefteq G$ est un sous-groupe normal (nous avons déjà vu cette assertion ; ici on donne une preuve plus courte).

(c) Si φ est surjective et $H \trianglelefteq G$ est un sous-groupe normal, alors l'image $\varphi(H) \trianglelefteq L$ est un sous-groupe normal.

Démonstration. (a) Soit $x \in \varphi^{-1}(H)$, donc $\varphi(x) \in H$. Soit $g \in G$. Alors

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in H,$$

donc $gxg^{-1} \in \varphi^{-1}(H)$, montrant que $\varphi^{-1}(H)$ est un sous-groupe normal de G.
(b) suit de (a) pour $H = \{1\} \trianglelefteq L$.
(c) Soit $\varphi(h) \in \varphi(H)$. Soit $\ell \in L$. Par surjectivité de φ, nous avons $\ell = \varphi(g)$ pour un $g \in G$. Donc

$$\ell^{-1}\varphi(h)\ell = \varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g^{-1}hg) \in \varphi(H)$$

car $g^{-1}hg \in H$, montrant que $\varphi(H)$ est un sous-groupe normal de L. □

Théorème 16.9 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soit $\varphi : G \to H$ un homomorphisme de groupes. Soit $N := \ker(\varphi)$ son noyau.*

(a) Pour tout $g \in G$ et tout $n \in N$ on a $\varphi(gn) = \varphi(g)$. Donc pour tout $g_1, g_2 \in gN$ on a $\varphi(g_1) = \varphi(g_2)$. Donc l'image $\varphi(g)$ ne dépend que de la classe gN de g suivant N.

(b) (a) nous permet de définir l'application

$$\overline{\varphi} : G/N \to H, \quad gN \mapsto \overline{\varphi}(gN) := \varphi(g).$$

C'est un homomorphisme injectif de groupes. Donc $\overline{\varphi} : G/N \to \mathrm{im}(\varphi)$ est un isomorphisme de groupes.

(Cette application est la même que dans le théorème 5.19.)

Démonstration. (a) C'est clair.
(b)

Homomorphisme $\overline{\varphi}(g_1N \cdot g_2N) = \overline{\varphi}(g_1g_2N) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1N)\overline{\varphi}(g_2N)$.

Injectivité Si $\overline{\varphi}(gN) = \varphi(g) = 1$, alors $g \in N$, donc $gN = N$.

Calcul de l'image Soit $h \in \mathrm{im}(\varphi)$. Donc, il existe $g \in G$ tel que $\varphi(g) = h$, donc $\overline{\varphi}(gN) = \varphi(g) = h$.

□

Exemple 16.10. *(a) Soient $n \in \mathbb{N}$ et $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection naturelle de noyau $n\mathbb{Z}$. L'application $\overline{\pi} : \mathbb{Z}/\ker(\pi) = \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est l'identité.*

(b) Soit $n \in \mathbb{N}_{>1}$. Le noyau $\mathrm{sgn} : S_n \to \{+1, -1\}$ est le groupe alterné A_n et $\overline{\mathrm{sgn}} : S_n/\ker(\mathrm{sgn}) = S_n/A_n \to \{+1, -1\}$ est un isomorphisme.

La proposition suivante est importante car elle décrit les sous-groupes des groupes quotients.

Proposition 16.11. *Soit G un groupe et $N \trianglelefteq G$ un sous-groupe normal et $\pi : G \to G/N$ la projection naturelle.*

(a) L'application

$$\Phi : \{\text{sous-groupes de } G/N\} \longrightarrow \{\text{sous-groupes de } G \text{ qui contiennent } N\},$$

donnée par $H \mapsto \pi^{-1}(H)$ est bijective. L'inverse Ψ de Φ est $U \mapsto \pi(U)$.

(b) Soient $H_1, H_2 \leq G/N$ deux sous-groupes. Alors

$$H_1 \subseteq H_2 \quad \Leftrightarrow \quad \Phi(H_1) \subseteq \Phi(H_2).$$

(c) Soit $H \leq G/N$ un sous-groupe. Alors

$$H \trianglelefteq G/N \quad \Leftrightarrow \quad \Phi(H) \trianglelefteq G.$$

Démonstration. (a)

- Pour $H \leq G/N$ l'image réciproque $\Phi(H) = \pi^{-1}(H)$ est en effet un sous-groupe comme nous l'avons vu avant. En plus $\pi^{-1}(H) \supseteq \pi^{-1}(\{1\}) = \ker(\pi) = N$.
- Nous avons aussi vu que les images des homomorphismes de groupes sont des sous-groupes du groupe d'arrivée, donc $\Psi(U) = \pi(U)$ est un sous-groupe de G/N.
- Voici une assertion auxiliaire :

  Soient $\pi : G \to G'$ un homomorphisme de groupes et $U \leq G$ un sous-groupe qui contient $\ker(\pi)$. Alors $\pi^{-1}(\pi(U)) = U$.

  On vérifie cette égalité :
  « $\subseteq$ » : Soit $x \in \pi^{-1}(\pi(U))$, donc $\pi(x) \in \pi(U)$, donc $\pi(x) = \pi(u)$ pour un $u \in U$. Donc $1 = \pi(x)\pi(u)^{-1} = \pi(xu^{-1})$, donc $xu^{-1} \in \ker(\pi) \subseteq U$, donc $xu^{-1} = v \in U$, donc $x = uv \in U$.
  « $\supseteq$ » : Soit $u \in U$, donc $\pi(u) \in \pi(U)$, donc $u \in \pi^{-1}(\pi(U))$.

- Soit $U \leq G$ un sous-groupe tel que $N \subseteq U$. Par l'assertion auxiliaire on a : $\Phi(\Psi(U)) = \pi^{-1}(\pi(U)) = U$.
- Voici une autre assertion auxiliaire :

  Soient $\pi : G \to G'$ une application surjective et $H \subseteq G'$ un sous-ensemble. Alors $H = \pi(\pi^{-1}(H))$.

  On vérifie cette égalité.
  « $\subseteq$ » : Soit $h \in H$. Comme π est surjectif, il existe $g \in G$ tel que $\pi(g) = h$. Donc $g \in \pi^{-1}(H)$ et $h = \pi(g) \in \pi(\pi^{-1}(H))$.

  « $\supseteq$ » : Soit $x \in \pi(\pi^{-1}(H))$. Donc, il existe $g \in \pi^{-1}(H)$ tel que $x = \pi(g)$. Mais, $x = \pi(g)$ appartient à H car $g \in \pi^{-1}(H)$.
- Soit $H \leq G/N$ un sous-groupe. Par l'assertion auxiliaire on a : $\Psi(\Phi(H)) = \pi(\pi^{-1}(H)) = H$.

(b) est clair.
(c) Cela est une conséquence directe des deux faits (Proposition 16.8) : l'image réciproque d'un sous-groupe normal est normale ; l'image par un homomorphisme surjectif d'un sous-groupe normal est également normale. □

Remarque 16.12. *(a) On remarque d'abord que tout sous-groupe $U \subseteq \mathbb{Z}$ est égal à $m\mathbb{Z}$ pour un $m \in \mathbb{N}$. Plus précisement, $m = 0$ si $U = \{0\}$; si $U \neq \{0\}$, alors on prend m comme le pgcd des éléments de U.*

Effectivement, le premier cas est clair. Soit donc $U \neq \{0\}$ et m le pgcd. Il est clair que $m \in U$, donc $m\mathbb{Z} \subseteq U$. Inversement, si $a \in U$, alors a est un multiple de m, donc $a \in m\mathbb{Z}$, d'où $U = m\mathbb{Z}$.

(b) Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}_{\geq 1}$ est de la forme $m\mathbb{Z}/n\mathbb{Z}$ avec $m \mid n$.

Pour le voir, on considère la projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Soit $H \subseteq \mathbb{Z}/n\mathbb{Z}$ un sous-groupe. Soit $U = \pi^{-1}(H)$; ce groupe est égal à $m\mathbb{Z}$ pour un $m \in \mathbb{N}$ par (a). Le fait $n\mathbb{Z} \subseteq m\mathbb{Z}$ se traduit en $m \mid n$. Alors $H = m\mathbb{Z}/n\mathbb{Z}$.

Il existe encore deux théorèmes d'isomorphismes. Pour les énoncer et les démontrer, nous avons d'abord besoin du lemme suivant.

Lemme 16.13. *Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal. Soit $HN := \{hn \mid h \in H, n \in N\}$. Alors :*

(a) $H \cap N$ est un sous-groupe normal de H.

(b) $HN = NH := \{nh \mid h \in H, n \in N\}$

(c) HN est un sous-groupe de G.

(d) N est un sous-groupe normal de HN.

(e) Si H est aussi un sous-groupe normal de G, alors HN est un sous-groupe normal de G.

Démonstration. Exercice. □

Proposition 16.14 (Deuxième théorème d'isomorphisme)**.** *Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal. Alors, l'homomorphisme naturel de groupes*

$$\varphi : H \to HN \to HN/N, \quad h \mapsto hN$$

« induit » (par le théorème d'isomorphisme 16.9) l'isomorphisme de groupes

$$\overline{\varphi} : H/(H \cap N) \to HN/N, \quad h(H \cap N) \mapsto hN.$$

Démonstration. Noter d'abord que le lemme 16.13 nous assure que tout est bien défini. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $h \in H$ tels que $hN = N$, donc $h \in H \cap N$, montrant $\ker(\varphi) = H \cap N$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 16.9. □

Proposition 16.15 (Troisième théorème d'isomorphisme)**.** *Soient G un groupe, $H, N \lhd G$ des sous-groupes normaux tels que $N \subseteq H$. Alors, l'homomorphisme naturel de groupes*

$$\varphi : G/N \to G/H, \quad gN \mapsto gH$$

« induit » (par le théorème d'isomorphisme 16.9) l'isomorphisme de groupes

$$\overline{\varphi} : (G/N)/(H/N) \to G/H, \quad gN(H/N) \mapsto gH.$$

Démonstration. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $gN \in G/N$ tels que $gH = H$, donc $g \in H$, donc $gN \in H/N$, montrant $\ker(\varphi) = H/N$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 16.9. □

17 Actions de groupes

Groupes de symétries

Définition 17.1. *On appelle* isométrie du plan *toute application*

$$\varphi : \mathbb{R}^2 \to \mathbb{R}^2$$

telle que pour tout $x, y \in \mathbb{R}^2$

$$|\varphi(x) - \varphi(y)| = |x - y|.$$

En d'autres mots, les isométries sont les applications du plan qui préservent les distances.
L'ensemble des isométries du plan est noté I_2. Noter que $(I_2, \circ, \mathrm{id})$ est un groupe.

Exemple 17.2. *(a) Toute réflexion à un point ou à un axe est une isométrie.*

(b) Toute rotation autour d'un point est une isométrie.

Définition 17.3. *Soit $F \subset \mathbb{R}^2$ un sous-ensemble (une figure). On appelle* symétrie de F *toute isométrie $\varphi \in I_2$ telle que $\varphi(F) = F$.*
L'ensemble de toutes les symétries de F est un groupe : le groupe des symétries de F *:* $\mathrm{Sym}(F)$.

Exemple 17.4. *(au tableau)*

(a) 4 *symétries du losange (sommets nommés A,B,C,D ; angles aigus à* A *et* C*, angles obtus à* B *et* D*) :* id*,* s_x *(réflexion à l'axe* x*),* s_y *(réflexion à l'axe* y*),* $r = s_y \circ s_x = s_y \circ s_x$ *(rotation de* $180°$*).*

(b) $2n$ *symétries du* n*-gone régulier (on numérote les sommets* P_i *à l'inverse du sens des aiguilles d'une montre) :* r^i *pour* $i = 0, \ldots, n-1$ *avec* r *la rotation autour* $360°/n$*, et* $s \circ r^i$ *pour* $i = 0, \ldots, n-1$ *avec* s *la réflexion à l'axe à travers un sommet et le centre. On a* $s \circ r_i = r_i^{-1} \circ s = r_{n-i} \circ s$*.*

Si n *est pair, on n'a que* $n/2$ *réflexions à l'axe à travers un sommet et le centre. Par contre, il existe aussi* $n/2$ *réflexions à des axes à travers le centre qui sont perpendiculaires à un côté (automatiquement à deux côtés). On se convainc que quand-même toute réflexion est de la forme* sr^i*.*

Lemme 17.5. *L'ensemble* $V = \{\mathrm{id}, s_x, s_y, r\}$ *est l'ensemble de toutes les symétries du losange. Donc* V *est le groupe des symétries du losange.*

Démonstration. Soit σ une symétrie du losange. Soit, σ garde l'angle aigu (autour de A) invariant, soit σ le transforme à l'autre angle aigu (autour de C). Dans le premier cas, on pose $\tau = \sigma$, dans le deuxième cas on pose $\tau = r_y \circ \sigma$. Maintenant, $\tau(A) = A$, donc $\tau(C) = C$. Soit τ garde l'angle obtu (autour de B) invariant, soit τ le transforme en l'autre angle obtu (autour de D). Dans le premier cas, on pose $\rho = \tau$, dans le deuxième cas on pose $\rho = r_x \circ \tau$. On a maintenant que $\rho(A) = A$, $\rho(B) = B$, $\rho(C) = C$, $\rho(D) = D$. Donc $\rho = \mathrm{id}$. □

Lemme 17.6. *L'ensemble* $D_n = \{r^i \mid i = 0, \ldots, n-1\} \cup \{sr^i \mid i = 0, \ldots, n-1\}$ *est l'ensemble de toutes les symétries du* n*-gone régulier. Donc* D_n *est le groupe des symétries du* n*-gone régulier. Son cardinal est* $2n$*.*

Démonstration. On remarque d'abord que toute symétrie préserve la propriété que deux sommets sont voisins. On note aussi que la réflexion r inverse la numérotation : si avant la réflexion, la numérotation était dans le sense des aiguilles d'une montre, après la numérotation sera dans le sens inverse, et vice versa.
Soit σ une symétrie. Comme σ transforme sommets voisins en sommets voisins, soit σ préserve l'ordre de la numérotation, soit σ l'inverse. Dans le premier cas, on pose $\tau = \sigma$, dans le deuxième cas on pose $\tau = s \circ \sigma$. Maintenant τ préserve l'ordre de la numérotation. Donc après une rotation r_i convenable, $r_i \circ \tau$ est l'identité sur l'ensemble des sommets, donc $r_i \circ \tau = \mathrm{id}$. Cela montre que σ est soit une rotation, soit une rotation suivie par la réflexion. □

Actions de groupes

Toute symétrie du n-gone régulier envoie un sommet sur un sommet et elle est uniquement déterminée par ce qu'elle fait avec les sommets. Cela mène au concept de l'action d'un groupe sur un ensemble.
Pour être plus concret, considérons l'exemple du pentagone (5-gone) régulier. Numérotons les sommets A, B, C, D, E à l'inverse du sens des aiguilles d'une montre. Soit $E = \{A, B, C, D, E\}$ l'ensemble des sommets. Toute symétrie est donc une application bijective de E dans E. En d'autres

mots, toute symétrie du 5-gon est un élément du groupe symétrique S_E. Si on appelle les sommets $1, 2, 3, 4, 5$, alors le groupe des symétries du 5-gon est un sous-groupe de S_5. La rotation autour du centre par $72°$ correspond au cycle $(1\ 2\ 3\ 4\ 5)$ et la réflexion à l'axe à travers le centre et 1 est la permutation $(2\ 5)(3\ 4)$.

Définition 17.7. *Soient E un ensemble et G un groupe. On dit que G* agit (à gauche) *sur E (on parle d'une* action (ou opération) du groupe sur l'ensemble *E) s'il existe une application*

$$G \times E \to E, \quad (g, x) \mapsto g.x = gx$$

telle que

- $\forall\, g, h \in G \forall\, x \in E : g.(h.x) = (gh).x$ *et*
- $\forall x \in E : 1.x = x$.

Les opérations à droite peuvent êtres définies d'une manière similaire.

Exemple 17.8. *(a) Le groupe des symétries d'un n-gone régulier agit sur l'ensemble des sommets.*

(b) Soit G un groupe et $E = G$. Nous prenons la loi de groupe $G \times E \to E$, $(g, e) \mapsto g \cdot e$ pour définir une action à gauche de G sur lui-même.

(c) Soit G un groupe et encore $E = G$. La conjugaison *$G \times E \to E$,$(g, e) \mapsto geg^{-1}$ définit une action à gauche de G sur lui-même. (La seule chose non-triviale à vérifier, c'est $(gh)e(gh)^{-1} = g(heh^{-1})g^{-1}$.)*

Toute opération d'un groupe sur un ensemble peut être exprimée dans le groupe symétrique. Plus précisément, nous avons les assertions suivantes.

Lemme 17.9. *Soient G un groupe et E un ensemble.*

(a) Si $G \times E \to E$ est une opération de groupe, l'application $\varphi : G \to S_E$ donnée par la règle que $\varphi(g)$ est l'application $E \to E$ telle que $(\varphi(g))(e) = g.e$ est un homomorphisme de groupes.

(b) Si $\varphi : G \to S_E$ est un homorphisme de groupes, alors $g.e := (\varphi(g))(e)$ définit une opération à gauche de G sur E.

(c) Les constructions de (a) et (b) établissent une bijection entre l'ensemble des homomorphismes de groupes $G \to S_E$ et les opérations à gauche de G sur E.

Démonstration. (a) D'abord il faut vérifier que $\varphi(g)$ est une bijection $E \to E$. Si $(\varphi(g))(x) = (\varphi(g))(y)$ avec $x, y \in E$, alors on a $g.x = g.y$; en agissant par g^{-1}, on obtient $g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x = g^{-1}.(g.y) = y$. Cela montre que $\varphi(g)$ est injectif. Maintenant soit $x \in E$ donné ; alors $(\varphi(g))(g^{-1}(x)) = g(g^{-1}.x) = (g^{-1}g).x = 1.x = x$, donc $\varphi(g)$ est aussi surjectif et en conséquence bijectif.
Montrons que φ est un homomorphisme de groupes. Soient $g, h \in G$ et $x \in E$. Alors $(\varphi(gh))(x) = (gh).x = g.(h.x) = (\varphi(g))((\varphi(h))(x) = (\varphi(g) \circ \varphi(h))(x)$, donc $\varphi(gh) = \varphi(g) \circ \varphi(h)$.
(b) Il suffit de vérifier les deux axiomes : $1.x = (\varphi(1))(x) = \mathrm{id}(x) = x$ et $g.(h.x) = \varphi(g) \circ \varphi(h)(x) = \varphi(gh)(x) = (gh).x$ pour tout $g, h \in G$.
(c) Clair. □

Définition 17.10. *(a) Soit $x \in E$. L'ensemble $G.x = \{g.x \mid g \in G\}$ s'appelle* l'orbite de x *(en anglais : orbit, en allemand : Bahn). L'ensemble des orbites est noté $G\backslash E$.*

(b) Soit $x \in E$. L'ensemble $G_x = \{g \in G \mid g.x = x\}$ s'appelle le stabilisateur *(ou* groupe d'isotropie*) de x.*

(c) S'il existe $x \in E$ tel que $G.x = E$, on dit que l'opération de G sur E est transitive.

(d) Soit $\pi : G \to S_E$ l'homomorphisme associé à l'opération de G sur E dans le lemme 17.9. S'il est injectif, on dit que l'opération de G sur E est fidèle *(faithful, treu).*

Lemme 17.11. *Le stabilisateur G_x est un sous-groupe de G.*

Démonstration. Soient $g, h \in G_x$. Notons d'abord que l'application de g^{-1} à $g.x = x$ donne $g^{-1}.(g.x) = g^{-1}.x$, donc $g^{-1}.x = (g^{-1}g).x = 1.x = x$. Alors $(g^{-1}h).x = g^{-1}.(h.x) = g^{-1}.x = x$, donc $g^{-1}h \in G_x$, d'où G_x est un sous-groupe de G. □

Exemple 17.12. *(a) Considérons le 5-gone régulier. L'orbite de n'importe quel sommet est l'ensemble de tous les sommets, donc l'opération est transitive. Le stabilisateur de n'importe quel sommet est l'identité et la réflexion à l'axe à travers le centre et le sommet choisi. L'opération est fidèle.*

(b) Considérons l'opération de G sur lui-même par multiplication. Le stabilisateur de $1 \neq g \in G$ est $\{1\}$. Cette action est fidèle et transitive.

En fait, l'homomorphisme $\pi : G \to S_E$ associé à cette opération dans le lemme 17.9 est celui de la proposition 13.12 de Cayley.

(c) Considérons l'opération par conjugaison de G sur lui-même. L'orbite de $h \in G$ est l'ensemble $\{ghg^{-1} \mid g \in G\}$. Si G est abélien, tout $g \in G$ agit comme l'identité. On parle d'une action triviale. Elle n'est certainement pas fidèle (sauf si $G = \{1\}$).

Nous avons la proposition importante suivante.

Proposition 17.13. *Soient E un ensemble et G un groupe. On suppose que G agit sur E.*

(a) La relation binaire $\sim_G$ définie sur E par

$$\forall\,(x,y) \in E^2 : x \sim_G y \iff \exists g \in G : y = g.x$$

est une relation d'équivalence sur E.

Pour tout x dans E, la classe d'équivalence de x pour cette relation est l'orbite de x sous l'action de G.

Comme pour toute relation d'équivalence nous avons la réunion disjointe

$$E = \bigsqcup_{\omega \in G\backslash E} \omega.$$

(b) Pour $x \in E$, l'application $G/G_x \to E$ (de l'ensemble des classes à gauche de G suivant le stabilisateur G_x dans E) donnée par $gG_x \mapsto g.x$ est bien définie et bijective. En particulier, on a $\#G.x = (G : G_x)$ (le cardinal de l'orbite est l'indice du stabilisateur).

(c) Dans toute orbite $\omega \in G\backslash E$ on choisit un représentant x_ω. Alors, on a l'égalité :

$$\#E = \sum_{\omega \in G\backslash E} G.x_\omega = \sum_{\omega \in G\backslash E} (G : G_{x_\omega}) = \#G \cdot \sum_{\omega \in G\backslash E} \frac{1}{\#G_{x_\omega}}$$

où pour la dernière égalité nous supposons G fini. Cette égalité s'appelle formule des classes (Bahnenbilanzgleichung).

Démonstration. (a) Vérification simple et propriétés des relations d'équivalence.
(b)

Bien défini. Montrons que l'application ne dépend pas du choix de représentants : $gG_x = hG_x$, donc $g = h \cdot r$ avec $r \in G_x$. Donc $g.x = (hr).x = h.(r.x) = h.x$ car $r.x = x$.

Injectif. Soient $g.x = h.x$ avec $g, h \in G$. Alors nous avons $h^{-1}.(g.x) = h^{-1}(h.x)$, donc $(h^{-1}g).x = (h^{-1}h).x = 1.x = x$, d'où $h^{-1}g \in G_x$, donc $gG_x = hG_x$.

Surjectif. Soit $g \in G$. Alors gG_x est envoyé sur $g.x$.

(c) suit de (a) et (b). □

Proposition 17.14 (Burnside)**.** *Soient E un ensemble fini et G un groupe fini. Alors*

$$\#(G\backslash E) = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}_g,$$

où $\mathrm{Fix}_g = \{x \in E \mid g.x = x\}$.

Démonstration. Nous avons

$$\#(G\backslash E) = \sum_{\omega \in G\backslash E} 1 = \sum_{\omega \in G\backslash E} \sum_{x \in \omega} \frac{1}{\#\omega} = \sum_{\omega \in G\backslash E} \sum_{x \in \omega} \frac{1}{\#Gx}$$
$$= \sum_{x \in E} \frac{1}{\#Gx} = \sum_{x \in E} \frac{\#G_x}{\#G} = \frac{1}{\#G} \sum_{x \in E} \#G_x.$$

Pour $g \in G$ et $x \in E$ nous posons

$$\delta_{g,x} = \begin{cases} 1 & \text{si } g.x = x, \\ 0 & \text{sinon.} \end{cases}$$

Nous obtenons

$$\sum_{x \in E} \#G_x = \sum_{x \in E} \sum_{g \in G} \delta_{g,x} = \sum_{g \in G} \sum_{x \in E} \delta_{g,x} = \sum_{g \in G} \#\mathrm{Fix}_g.$$

La formule de Burnside est montrée. □

Exemple 17.15. *Nous déterminons le nombre de colliers différents à 5 perles mobiles sur un fil dont les couleurs sont rouge, blanc ou bleu. C'est une application de la formule de Burnside.*
On peut s'imaginer les 5 perles comme les sommets (coloriés en rouge, blanc ou bleu) d'un 5-gone régulier. Soit E l'ensemble de tous les 5-gones dont les sommets sont rouge, blanc ou bleu. Alors $\#E = 3^5 = 243$.
Comme nous l'avons vu, toute symétrie du 5-gone donne le même collier, et si deux 5-gones coloriés donnent le même collier, alors il s'agit d'une symétrie. En d'autres mots, le groupe $G = D_5$ agit sur E. Le nombre de colliers différents est le nombre d'orbites pour cette action. Nous pouvons donc utiliser la formule de Burnside.
Si $g = \mathrm{id}$, alors $\#\mathrm{Fix}_{\mathrm{id}} = 3^5$. Si g est une des 4 rotations non-triviales, alors seuls les colliers d'une seule couleur sont fixés ; il y en a trois (un par couleur). Si g est une des 5 réflexions, alors le sommet fixé peut avoir n'importe quelle couleur ; les quatres autres sommets forment deux couples qui sont échangés ; chaque couple peut avoir n'importe quelle couleur ; donc 3^3 éléments sont fixés.
En conséquence, il existe

$$\#(G\backslash E) = \frac{1}{\#D_5}(3^5 + 4 \cdot 3 + 5 \cdot 3^3) = \frac{243 + 12 + 135}{10} = 39$$

colliers différents.

Exemple 17.16. *Considérons une variante de l'opération de G sur lui-même par multiplication, donc de l'homomorphisme de Cayley de la proposition 13.12. Soit G un groupe et $H \subseteq G$ un sous-groupe. Posons $E = G/H$, l'ensemble des classes à gauche suivant H. G agit sur G/H par multiplication : $g_1.(g_2H) := (g_1g_2).H$ pour tout $g_1, g_2 \in G$. En d'autres mots, nous avons l'homomorphisme*

$$\varphi : G \to S_{G/H}, \quad g_1 \mapsto (g_2H \mapsto (g_1g_2)H)$$

avec $S_{G/H}$ le groupe symétrique.
Comme application de cette opération, nous montrons l'assertion suivante (qui généralise le fait (exercice) que tout sous-groupe d'indice 2 d'un groupe fini est normal).

> Soit $G \neq \{1\}$ un groupe fini et soit p le nombre premier le plus petit tel que $p \mid \#G$.
> Alors tout sous-groupe H de G d'indice p est normal.

Calculons le noyau de φ. On cherche donc les $g_1 \in G$ tels que $g_1g_2H = g_2H$ pour tout $g_2H \in G/H$ ou, de façon équivalente, les $g_1 \in G$ qui appartiennent à $g_2Hg_2^{-1}$ pour tout $g_2 \in G$. Le noyau de φ est donc $\bigcap_{g\in G} gHg^{-1}$.
Soit maintenant H d'indice p où p est le plus petit premier divisant $\#G$. Donc le cardinal de $S_{G/H}$ est $p!$. Par le théorème d'isomorphisme et le théorème de Lagrange, le cardinal de $G/\ker(\varphi)$ divise $p!$. Il est clair que $\ker(\varphi) \subseteq H$. Par la généralisation du théorème de Lagrange (exercice) nous avons

$$(G : \ker(\varphi)) = (G : H) \cdot (H : \ker(\varphi)) = p \cdot (H : \ker(\varphi)).$$

On conclut que $(H : \ker(\varphi))$ divise $(p-1)!$ et $(G : \ker(\varphi)) = \frac{\#G}{\#\ker(\varphi)}$, donc $\#G$. Comme $\#G$ n'est pas divisible par un premier strictement plus petit que p, on obtient $(H : \ker(\varphi)) = 1$, donc $H = \ker(\varphi)$. En tant que noyau d'un homomorphisme, H est un sous-groupe normal.

18 Les théorèmes de Sylow

Avant de démontrer les théorèmes de Sylow, nous étudions de plus près l'opération d'un groupe G sur lui-même par conjugaison (voir l'exemple 17.12)

$$G \times G \to G, \quad (g,h) \mapsto ghg^{-1}.$$

Définition 18.1. *Soit G un groupe. Le stabilisateur de $h \in G$ pour l'opération de G sur lui-même par conjugaison*

$$Z_h := Z_h(G) := \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\}$$

s'appelle le centralisateur de h dans G. *C'est un sous-groupe de G car les stabilisateurs le sont toujours.*
Soit $H \subseteq G$ un sous-ensemble. Le centralisateur de H dans G *est défini comme*

$$Z_H(G) := \{g \in G \mid \forall\, h \in H : gh = hg\} = \bigcap_{h \in H} Z_h(G).$$

C'est un sous-groupe car une intersection de sous-groupes est toujours un sous-groupe.

Exemple 18.2. *(a) $Z_G(G)$ est le centre $\mathcal{Z}(G)$ de G, c'est-à-dire, l'ensemble $\{g \in G \mid \forall\, h \in G : gh = hg\}$.*

(b) Pour $g \in G$, on a l'équivalence $g \in \mathcal{Z}(G) \Leftrightarrow Z_g(G) = G$.

En particulier, l'orbite de $g \in \mathcal{Z}(G)$ pour la conjugaison est $\{g\}$.

(c) $Z_{(1\ 2\ 3)}(S_3) = \langle (1\ 2\ 3) \rangle$.

Corollaire 18.3. *Soit G un groupe fini. Pour toute orbite de cardinal ≥ 2 (pour l'action de G sur lui-même par conjugaison), on choisit un représentant x_i. Soit n le nombre de telles orbites. On a*

$$G = \bigsqcup_{g \in \mathcal{Z}(G)} \{g\} \sqcup \bigsqcup_{i=1}^{n} \{gx_ig^{-1} \mid g \in G\}$$

et donc

$$\#G = \#\mathcal{Z}(G) + \sum_{i=1}^{n} (G : Z_{x_i}(G))$$

avec $Z_{x_i}(G) \neq G$ pour tout $i = 1, \ldots, n$.

Démonstration. C'est précisement la formule des orbites de la proposition 17.13 (c) appliquée à l'action de G sur lui-même par conjugaison. □

Nous sommes maintenant prêts pour le premier théorème de Sylow. D'abord il s'agit de mettre en place la terminologie nécessaire.

Définition 18.4. *Soit p un nombre premier. On appelle p-groupe tout groupe fini d'ordre p^n pour un $n \in \mathbb{N}$.*

Exemple 18.5. *(a) Le groupe $G = \{1\}$ d'ordre $p^0 = 1$ est un p-groupe pour tout nombre premier p.*

(b) $\mathbb{Z}/p\mathbb{Z}$ est un p-groupe de cardinal $p = p^1$.

(c) $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ est un p-groupe de cardinal p^2.

(d) L'ensemble des matrices

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

est un p-groupe de cardinal p^3 pour la multiplication de matrices. Ce groupe n'est pas abélien.

Définition 18.6. *Soit G un groupe fini de cardinal $n = p^r m$ où p est un nombre premier tel que $p \nmid m$. Un sous-groupe $H \leq G$ est appelé* p-groupe de Sylow *(ou* p-Sylow*) si $\#H = p^r$.*
En d'autres mots, un p-groupe de Sylow est un sous-groupe qui est un p-groupe de cardinal égal à la plus grande puissance de p qui divise le cardinal de G.

Exemple 18.7. *(a) Si $p \nmid \#G$, alors $\{1\}$ est un p-groupe de Sylow de G.*

(b) Prenons $G = S_3$ de cardinal 6. Il existe trois 2-groupes de Sylow : $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$. Il n'existe qu'un seul 3-groupe de Sylow : $\langle(1\ 2\ 3)\rangle$.

(c) Prenons $G = A_4$ de cardinal $12 = 2^2 \cdot 3$. Il existe un 2-groupe de Sylow :

$$\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Il existe plusieurs 3-groupes de Sylow : $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, etc.

Lemme 18.8. *Soit G un groupe fini de cardinal $\#G = m$ et p un nombre premier qui divise m. Alors il existe $g \in G$ d'ordre p.*

Démonstration. Supposons le contraire : il n'existe aucun élément de g d'ordre p. On numérote les éléments de G : $1 = g_0, g_1, g_2, \ldots, g_{m-1}$. Prenons le produit cartésien $C := \prod_{i=1}^{m-1} \langle g_i \rangle$. C'est un ensemble de cardinal égal à

$$\prod_{i=1}^{m-1} \#\langle g_i \rangle = \prod_{i=1}^{m-1} \operatorname{ord}(g_i)$$

où la dernière égalité découle de la proposition 15.4. Par notre hypothèse le cardinal de C n'est pas divisible par p. Notons que C est un groupe pour la loi interne « composante par composante » comme dans la définition-lemme 15.12. L'application

$$\varphi : C \to G, \quad (g_1^{e_1}, g_2^{e_2}, \ldots, g_{m-1}^{e_{m-1}}) \mapsto \prod_{i=1}^{m-1} g_i^{e_i}$$

est un homomorphisme de groupes qui est surjectif. Donc le cardinal de G est égal au cardinal $\#C/\#\ker(\varphi)$, donc c'est un diviseur de $\#C$. En conséquence, p ne peut pas diviser $\#G$ non-plus. Contradiction. □

Dans la démonstration à venir nous avons besoin d'un petit lemme que nous aurions pu déjà montrer plus tôt.

Lemme 18.9. *Soit $\pi : G \to H$ un homomorphisme surjectif de groupes. Soit $V \subseteq H$ un sous-groupe et $U = \pi^{-1}(V)$ le sous-groupe de G obtenu comme image réciproque.*
Alors nous avons l'égalité d'indices $(G : U) = (H : V)$.

Démonstration. Considérons l'application

$$\varphi : G/U \to H/V, \quad gU \mapsto \pi(g)V.$$

Elle est bien définie car si $g_1U = g_2U$, alors $g_2^{-1}g_1 \in U$, donc $\pi(g_2^{-1}g_1) \in V$ d'où $\pi(g_1)V = \pi(g_2)V$. Elle est surjective : soit $hV \in H/V$ une classe donnée ; la surjectivité de π nous permet de choisir $g \in G$ tel que $\pi(g) = h$; donc $\varphi(gU) = \pi(g)V = hV$. Finalement, φ est aussi injectif. Supposons que nous avons deux classes $g_1U, g_2U \in G/U$ telles que $\varphi(g_1U) = \varphi(g_2U)$, donc $\pi(g_1)V = \pi(g_2)V$ d'où $\pi(g_2^{-1}g_1) \in V$, alors $g_2^{-1}g_1 \in \pi^{-1}(V) = U$ ce qui implique $g_1U = g_2U$.
Comme φ est bijectif, on a $(G : U) = (H : V)$. □

Théorème 18.10 (1er théorème de Sylow)**.** *Soient G un groupe fini et p un nombre premier. Alors G possède un p-groupe de Sylow.*

Démonstration. Récurrence sur le cardinal m de G.
L'initialisation $\#G = m = 1$ est triviale.
Supposons le théorème démontré pour tout groupe de cardinal strictement inférieur à m. Soit G un groupe de cardinal m. Si $p \nmid m$, le groupe $\{1\}$ est un p-groupe de Sylow, comme nous l'avons vu. Soit donc $m = p^e r$ avec $p \nmid r$ et $e \geq 1$. Nous utilisons la formule des orbites du corollaire 18.3 :

$$\#G = \#\mathcal{Z}(G) + \sum_{i=1}^{n} (G : Z_{x_i}(G))$$

avec $Z_{x_i}(G) \neq G$ pour tout $i = 1, \ldots, n$.

1er cas : $p \nmid \#\mathcal{Z}(G)$**.** De la formule des orbites il suit qu'il existe $i \in \{1, 2, \ldots, n\}$ tel que

$$p \nmid (G : Z_{x_i}(G)) = \frac{\#G}{\#Z_{x_i}(G)} = \frac{p^e r}{\#Z_{x_i}(G)}.$$

Donc $p^e \mid \#Z_{x_i}(G)$. Comme $Z_{x_i}(G) \neq G$, on a $\#Z_{x_i}(G) < m$ ce qui nous permet d'utiliser l'hypothèse de récurrence : $Z_{x_i}(G)$ contient un p-groupe P de cardinal p^e. Ce groupe est un p-groupe de Sylow pour G.

2ème cas : $p \mid \#\mathcal{Z}(G)$**.** Comme $\mathcal{Z}(G)$ est abélien, le lemme 18.8 implique qu'il existe $g \in \mathcal{Z}(G)$ d'ordre p. Soit $N = \langle g \rangle$ le sous-groupe cyclique engendré par g. Comme g commute avec tous les éléments de G, le sous-groupe N est distingué. Nous pouvons donc prendre le quotient $\overline{G} := G/N$. C'est un groupe de cardinal $m/p = p^{e-1}r$, donc l'hypothèse de récurrence s'applique. Nous obtenons un sous-groupe $\overline{P} \subseteq \overline{G}$ de cardinal p^{e-1}. Pour produire un p-groupe de Sylow dans G, nous considérons la projection $\pi : G \twoheadrightarrow \overline{G} = G/N$ qui envoie g sur sa classe gN. Posons $P := \pi^{-1}(\overline{P})$. Nous savons (c'est un fait général qui n'utilise rien de notre situation particulière ici) que P est un sous-groupe de G et par le lemme 18.9 on obtient $\frac{\#G}{\#P} = (G : P) = (\overline{G} : \overline{P}) = r$ d'où $\#P = p^e$ est un p-groupe de Sylow.

La démonstration est achevée. □

Lemme 18.11. *Soit P un p-groupe de Sylow de G. Alors pour tout $g \in G$, le groupe gPg^{-1} est aussi un p-groupe de Sylow.*

Démonstration. C'est clair car l'application $P \to gPg^{-1}$ qui envoie $h \in P$ sur ghg^{-1} est une bijection d'inverse $gPg^{-1} \to P$ telle que $h' \in gPg^{-1}$ est envoyé sur $g^{-1}h'g$. Il est clair que ces deux applications sont surjectives ; donc $\#P \geq gPg^{-1}$ et $\#P \leq gPg^{-1}$ d'où l'égalité recherchée. □

Considérons maintenant une autre opération. Soit G toujours un groupe. Soit

$$E = \{H \mid H \subseteq G \text{ sous-groupe}\},$$

l'ensemble de tous les sous-groupes de G. Le groupe G agit sur E par conjugaison :

$$G \times E \to E, \quad (g, H) \mapsto gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Définition 18.12. *Le* normalisateur de H dans G *est défini comme le stabilisateur de H pour l'opération décrite ci-dessus :*

$$N_H(G) := \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}.$$

Le normalisateur est un sous-groupe car tout stabilisateur pour toute opération est un sous-groupe. En plus, on a toujours $H \trianglelefteq N_H(G)$.

Exemple 18.13. *(a)* $N_{\langle(1\,2\,3)\rangle}(S_3) = S_3$.

(b) Plus généralement, si $H \trianglelefteq G$ est normal, alors $N_H(G) = G$.

Soit $\mathcal{S}_p$ le sous-ensemble (non-vide à cause du théorème 18.10) de E de tous les p-groupes de Sylow. Le lemme 18.11 implique que l'opération de G sur E laisse $\mathcal{S}_p$ invariant.

Proposition 18.14. *Soit G un groupe fini et P un p-groupe de Sylow. Soit $H \subseteq G$ un sous-groupe qui est un p-groupe.*

(a) Si $hPh^{-1} = P$ pour tout $h \in H$, alors $H \subseteq P$.

(b) Il existe $g \in G$ tel que $S = gPg^{-1}$ est un p-groupe de Sylow avec $H \subseteq S$. En particulier, tout p-groupe est contenu dans un p-groupe de Sylow.

Démonstration. (a) L'hypothèse implique $H \subseteq N_P(G)$ et on a, comme toujours, $P \trianglelefteq N_P(G)$. En conséquence (voir le lemme 16.13 (c)), HP est un sous-groupe de $N_P(G)$. Le 2ème théorème d'isomorphisme 16.14 donne

$$HP/P \cong H/H \cap P.$$

Donc HP est un p-groupe (car $\frac{\#HP}{\#P}$ est une puissance de p car c'est un diviseur de $\#H$) qui contient P. Donc $HP = P$ car S est un p-groupe de Sylow. On en conclut que $H \subseteq P$.
(b) Comme nous l'avons vu, le stabilisateur de l'opération de G par conjugaison sur P est le normalisateur $N_P(G)$ de P dans G. Soit $G.P = \{gPg^{-1} \mid g \in G\}$ l'orbite. Par la proposition 17.13 (b) nous avons $\#G.P = \#G/\#N_P(G)$. Comme $P \subseteq N_P(G)$, on a $p^e \mid N_P(G)$, donc $p \nmid \#G.P$.

Soit H maintenant un sous-groupe de G qui est un p-groupe. Nous avons que H agit sur l'orbite $G.P$ par conjugaison. Considérons la réunion disjointe des orbites pour cette action :

$$G.P = \bigsqcup_{i=1}^{s} \{hg_iPg_i^{-1}h^{-1} \mid h \in H\}.$$

Encore la proposition 17.13 (b) nous dit que le cardinal de toute orbite de H est un diviseur de $\#H$, donc c'est une puissance de p. Comme le cardinal de $G.P$ n'est pas divisible par p, il doit y avoir au moins une classe $\{hg_kPg_k^{-1}h^{-1} \mid h \in H\}$ de cardinal $p^0 = 1$.
On pose $S = g_kPg_k^{-1}$. C'est un p-groupe de Sylow et par ce qui précède (cardinal de l'orbite pour H est 1), pour tout $h \in H$ on a $hSh^{-1} = S$. Donc (a) donne le résultat. □

Théorème 18.15 (2ème théorème de Sylow)**.** *Soit G un groupe fini. Si $P_1, P_2 \subseteq G$ sont des p-groupes de Sylow, alors il existe $g \in G$ tel que $gP_1g^{-1} = P_2$.*
En d'autres mots, l'action par conjugaison de G sur l'ensemble $\mathcal{S}_p$ des p-groupes de Sylow est transitive.

Démonstration. Il suffit de prendre $H = P_2$ et $P = P_1$ dans la proposition 18.14. □

Théorème 18.16 (3ème théorème de Sylow)**.** *Soient G un groupe fini et p un nombre premier. Soit s_p le nombre des p-groupes de Sylow de G. Alors, $s_p \mid \#G$ et $s_p \equiv 1 \mod p$.*

Démonstration. Comme l'opération de G sur $\mathcal{S}_p$ est transitive par le deuxième théorème de Sylow 18.15, $\mathcal{S}_p$ est une orbite et donc son cardinal s_p est un diviseur de $\#G$ par la proposition 17.13 (b). Soit P un p-groupe de Sylow. Au lieu de l'action de G sur $\mathcal{S}_p$, on considère maintenant l'action de P et ses orbites. Une des orbites, c'est $\{P\}$. Pour $g \in G$, soit $\{hgPg^{-1}h^{-1} \mid h \in P\}$ une autre orbite. Par la proposition 17.13 (b) et le fait que P est un p-groupe, soit le cardinal de cette orbite est 1, soit divisible par p. Si on est dans le premier cas, on a $hgPg^{-1}h^{-1} = gPg^{-1}$ pour tout $h \in P$. Donc la proposition 18.14 (a) implique $P \subseteq gPg^{-1}$, alors $P = gPg^{-1}$ à cause du fait que les deux ensembles sont du même cardinal. Cela veut dire que $\{P\}$ est la seule orbite pour l'action de P de cardinal 1. Toutes les autres orbites sont de cardinal divisible par p.
Comme $\mathcal{S}_p$ est la réunion disjointe des orbites pour l'action de P, on obtient $s_p \equiv 1 \mod p$. □

Corollaire 18.17. *Soit G un groupe fini et p un nombre premier.*

(a) Si $p \mid \#G$, alors il existe $g \in G$ d'ordre p.

(b) G est un p-groupe si et seulement si l'ordre de tout élément de G est une puissance de p.

Démonstration. (a) Soit P un p-groupe de Sylow de G et soit $g \in P$ un élément différent de 1. Alors l'ordre de g est une puissance de p, disons p^r. En conséquence, $h := g^{p^{r-1}}$ est d'ordre p.
(b) La seule chose non-triviale est que G est un p-groupe. Si cela n'était pas le cas, alors par (a) on aurait un élément d'ordre p' avec p' un premier différent de p. □

Corollaire 18.18. *Soit G un groupe fini et p un nombre premier. Si G possède exactement un p-groupe de Sylow P, alors P est normal.*

Démonstration. On sait que pour tout $g \in G$, le groupe gPg^{-1} est aussi un p-groupe de Sylow. Comme il n'y en a qu'un seul, on a $gPg^{-1} = P$ pour tout $g \in G$ d'où P est normal. □

Corollaire 18.19. *Soient $p < q$ deux nombres premiers tels que $p \nmid (q-1)$. Alors tout groupe G de cardinal pq est cyclique.*

Démonstration. Par le troisième théorème de Sylow 18.16, nous avons $s_p \equiv 1 \mod p$, $s_q \equiv 1 \mod q$ et $s_p, s_q \mid pq$. Cela laisse les possibilités $s_p \in \{1, q\}$ et $s_q \in \{1, p\}$. Maintenant l'hypothèse $q \not\equiv 1 \mod p$ intervient pour exclure $s_p = q$, donc $s_p = 1$. Le fait $p < q$ implique aussi $p \not\equiv 1 \mod q$, d'où $s_q = 1$. Il existe donc un unique p-groupe de Sylow P et un unique q-groupe de Sylow Q de cardinal p, q, respectivement. Par le lemme 16.13, nous avons que PQ est un sous-groupe de G, donc égal à G car il est du même cardinal.
Soient maintenant $x \in P$ et $y \in Q$. L'élément $xyx^{-1}y^{-1}$ est dans P (car $yx^{-1}y^{-1} \in P$ à cause de la normalité de P) et dans Q (car $xyx^{-1} \in Q$ à cause de la normalité de Q). Comme $P \cap Q = \{1\}$ (corollaire 15.9), on a $xyx^{-1}y^{-1} = 1$, donc $xy = yx$. Le groupe G est donc abélien.
Soit $g \in P \setminus \{1\}$ et $h \in Q \setminus \{1\}$. L'ordre de gh est $\operatorname{ppcm}(p, q) = pq$. Donc G est cyclique. □

Exemple 18.20. *Si G est un groupe d'ordre 35, alors G est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/35\mathbb{Z}$. Effectivement, $5 \nmid (7-1)$.*

Définition 18.21. *Un groupe G est dit* simple *si ses seuls sous-groupes normaux sont $\{1\}$ et G.*

Exemple 18.22. *Aucun groupe de cardinal $30 = 2 \cdot 3 \cdot 5$ n'est simple.*
Par le troisième théorème de Sylow 18.16, nous avons $s_p \equiv 1 \mod p$ et $s_p \mid 2 \cdot 3 \cdot 5$ pour $p = 2, 3, 5$. Cela laisse les possibilités

$$s_2 \in \{1, 3, 5, 15\}, \quad s_3 \in \{1, 10\}, \quad s_5 \in \{1, 6\}.$$

Supposons $s_3 > 1$ et $s_5 > 1$, donc $s_3 = 10$ et $s_5 = 6$.
Soient $P_1, \ldots, P_6$ les six 5-groupes de Sylow. Comme $P_i \cap P_j = \{1\}$ pour $i \neq j$, les 5 groupes de Sylow contiennent $6 \cdot 4 = 24$ éléments d'ordre 5.
Soient $Q_1, \ldots, Q_{10}$ les dix 3-groupes de Sylow. Avec le même argument, ils contiennent $10 \cdot 2 = 20$ éléments d'ordre 3.
En tout, nous avons trouvé 44 éléments d'ordre 3 et 5, ce qui est évidemment une contradiction avec le cardinal 30.
En conséquence, soit $s_3 = 1$ (dans ce cas le seul 3-Sylow est normal), soit $s_5 = 1$ (dans ce cas le seul 5-Sylow est normal).

Chapitre IV

Objets de base de l'algèbre linéaire abstraite

Le contenu de ce chapître correspond à peu près à une grande partie de votre cours d'algèbre linéaire. La seule différence est que nous admettons un corps commutatif quelconque au lieu de seulement $\mathbb{R}$. Ce chapître ne sera pas enseigné au cours. Il est inclut pour vous servir comme référence pour votre cours d'algèbre linéaire.

19 Espaces vectoriels

Soit $n \in \mathbb{N}$. On regarde $\mathbb{R}^n$. Comme vous le savez aussi, on peut additioner deux éléments de $\mathbb{R}^n$ de la façon suivante :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}.$$

Une vérification très facile nous montre :

$(\mathbb{R}^n, +, \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix})$ est un groupe abélien.

En plus, on dispose d'une multiplication scalaire : on multiplie un élément de $\mathbb{R}^n$ par un élément r de $\mathbb{R}$ ainsi :

$$r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ ra_2 \\ \vdots \\ ra_n \end{pmatrix}.$$

L'addition et la multiplication sont compatibles de la manière suivante :

- $\forall\, r \in \mathbb{R}, \forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^n : r \cdot (\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}) = r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + r \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$;

- $\forall\, r,s \in \mathbb{R}, \forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n : (r+s)\cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = r\cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + s\cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$;
- $\forall\, r,s \in \mathbb{R}, \forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n : r\cdot (s\cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}) = (r\cdot s)\cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$;
- $\forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n : 1\cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$.

Des structures ayant de telles propriétés sont appelés espaces vectoriels.

Définition 19.1. *Soit $(K, +_K, \cdot_K, 0_K, 1_K)$ un corps commutatif. Soient $(V, +_V, 0_V)$ un groupe abélien et*

$$\cdot_V : K \times V \to V, \quad (a,v) \mapsto a \cdot_V v = av$$

une application (appelée multiplication scalaire*).*
*On appelle $(V, +_V, \cdot_V, 0_V)$ un K-*espace vectoriel *si*

(SM1) $\forall\, a \in K, \forall\, u,v \in V : a \cdot_V (u +_V v) = a \cdot_V u +_V a \cdot_V v$,

(SM2) $\forall\, a,b \in K, \forall v \in V : (a +_K b) \cdot_V v = a \cdot_V v +_V b \cdot_V v$,

(SM3) $\forall\, a,b \in K, \forall v \in V : (a \cdot_K b) \cdot_V v = a \cdot_V (b \cdot_V v)$,

(SM4) $\forall\, v \in V : 1_K \cdot_V v = v$.

Notation 19.2. *Soit $(V, +_V, \cdot_V, 0_V)$ un K-espace vectoriel et $v \in V$. On note $-v$ l'unique élément de V tel que $v +_V (-v) = 0_V$.*

Exemple 19.3. *(a) Soient $n \in \mathbb{N}$ et $(K, +, \cdot, 0, 1)$ un corps. L'ensemble K^n des vecteurs colonnes*

$$K^n = \{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mid a_1, a_2, \ldots, a_n \in K \} \ni \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

pour l'addition

$$+ : K^n \times K^n \to K^n, \quad \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

et la multiplication scalaire

$$+ : K \times K^n \to K^n, \quad r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ ra_2 \\ \vdots \\ ra_n \end{pmatrix}$$

*définit un K-espace vectoriel, appelé K-*espace vectoriel standard de dimension n.

(b) Cas spécial $n = 1$: Le corps $(K, +, \cdot, 0, 1)$ est aussi un K-espace vectoriel $(K, +, \cdot, 0)$.

*(c) Cas spécial $n = 0$: $(\{0\}, +, \cdot, 0)$ s'appelle K-*espace nul*.

(d) Les nombres complexes $\mathbb{C}$ avec leur addition habituelle forment un $\mathbb{R}$-espace vectoriel pour la multiplication scalaire :

$$\mathbb{R} \times \mathbb{C} \to \mathbb{C}, \quad (x, z) \mapsto x \cdot z,$$

où le produit $x \cdot z$ est le produit habituel de $\mathbb{C}$ (on regarde donc le nombre réel x comme un nombre complexe).

Notation 19.4 (Plutôt : non-notation)**.** *Nous n'écrivons pas de flèche pour noter des éléments d'espaces vectoriels.*

La proposition suivante nous produit un grand nombre d'exemples.

Proposition 19.5. *Soit $(K, +_K, \cdot_K, 0_K, 1_K)$ un corps commutatif. Soit E un ensemble. On rappelle la notation*

$$\mathcal{F}(E, K) := \{f \mid f : E \to K \text{ application } \}$$

pour l'ensemble des applications de E dans K. On note l'application $E \to K$ telle que toutes ses valeurs sont 0 par $0_{\mathcal{F}}$ (concrètement : $0_{\mathcal{F}} : E \to K$ définie par la règle $0_{\mathcal{F}}(e) = 0$ pour tout $e \in E$). On définit l'addition

$$+_{\mathcal{F}} : \mathcal{F}(E, K) \times \mathcal{F}(E, K) \to \mathcal{F}(E, K), \quad (f, g) \mapsto f +_{\mathcal{F}} g \text{ où } \forall e \in E : (f +_{\mathcal{F}} g)(e) := f(e) +_K g(e)$$

et la mutliplication scalaire

$$\cdot_{\mathcal{F}} : K \times \mathcal{F}(E, K) \to \mathcal{F}(E, K), \quad (x, f) \mapsto x \cdot_{\mathcal{F}} f \text{ où } \forall e \in E : (x \cdot_{\mathcal{F}} f)(e) := x \cdot_K (f(e)).$$

Alors, $(\mathcal{F}(E, K), +_{\mathcal{F}}, \cdot_{\mathcal{F}}, 0_{\mathcal{F}})$ est un K-espace vectoriel.

Démonstration. Exercice. □

La plupart du temps, on n'écrira pas les indices, mais seulement $f + g$, $f \cdot g$, etc.

Exemple 19.6. *(a) Soient $E = \{1, 2, \ldots, n\}$ et K un corps commutatif. On peut identifier $\mathcal{F}(E, K)$ avec l'espace vectoriel standard K^n comme suit :*

Un élément $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n$ *peut être vu comme l'application $a : E \to K$ donnée par la règle $a(i) = a_i$.*

Il est clair que cela donne une bijection.

(b) Plus généralement, $\mathcal{F}(\mathbb{N}, K)$ est l'ensemble des suites $(a_n)_{n \in \mathbb{N}}$ dans K.

Par exemple, la suite $a_n = \frac{1}{n} \in \mathbb{R}$ peut être obtenue par la fonction $f : \mathbb{N}_{>0} \to \mathbb{R}$, donnée par la règle $f(n) = \frac{1}{n}$. La suite constante 0 est représentée par la fonction constante : $f(n) = 0$ pour tout $n \in \mathbb{N}$.

Lemme 19.7. *Soient $(K, +_K, \cdot_K, 0_K, 1_K)$ un corps commutatif et $(V, +_V, \cdot_V, 0_V)$ un K-espace vectoriel. Alors, les propriétés suivantes sont satisfaites pour tout $v \in V$ et tout $a \in K$:*

(a) $0_K \cdot_V v = 0_V$ *;*

(b) $a \cdot_V 0_V = 0_V$ *;*

(c) $a \cdot_V v = 0_V \Rightarrow a = 0_K \vee v = 0_V$ *;*

(d) $(-1_K) \cdot_V v = -v$.

Démonstration. (a) $0_K \cdot_V v = (0_K +_K 0_K) \cdot_V v = 0_K \cdot_V v + 0_K \cdot_V v$, donc $0_K \cdot_V v = 0_V$.
(b) $a \cdot_V 0_V = a \cdot_V (0_V + 0_V) = a \cdot_V 0_V + a \cdot_V 0_V$, donc $a \cdot_V 0_V = 0_V$.
(c) Supposons $a \cdot_V v = 0_V$. Si $a = 0_K$, l'assertion $a = 0_K \vee v = 0_V$ est vraie. Supposons donc $a \neq 0_K$. Comme K est un corps, $a^{-1} \in K$ (défini par la propriété $a^{-1} \cdot_K a = 1_K$). En conséquence, $v = 1_K \cdot_V v = (a^{-1} \cdot_K a) \cdot_V v = a^{-1} \cdot_V (a \cdot_V v) = a^{-1} \cdot_V 0_V = 0_V$ par (b).
(d) $v +_V (-1_K) \cdot_V v = 1_K \cdot_V v +_V (-1_K) \cdot_V v = (1_K +_K (-1_K)) \cdot_V v = 0_K \cdot_V v = 0_V$ par (a). □

20 Sous-espaces vectoriels

Pour des raisons de concision, lorsqu'on dit que K est un corps et V un K-espace vectoriel, on sous-entend que K est commutatif et que toutes les structures sont fixées : $(K, +_K, \cdot_K, 0_K, 1_K)$ et $(V, +_V, \cdot_V, 0_V)$.

Définition 20.1. *Soient K un corps et V un K-espace vectoriel. On dit qu'un sous-ensemble non-vide $W \subseteq V$ est un* sous-espace vectoriel de V *si*

$$\forall\, w_1, w_2 \in W, \forall a \in K : a \cdot w_1 + w_2 \in W.$$

Notation : $W \leq V$.

Exemple 20.2.

- *Soient K un corps et V un K-espace vectoriel. L'ensemble $\{0\}$ est un sous-espace vectoriel de V, appelé* l'espace zéro, *noté 0 par simplicité (ne pas confondre avec l'élément 0).*
- *Soient $V = \mathbb{R}^2$ et $W = \{\left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right) \mid a \in \mathbb{R}\} \subseteq V$. Alors, W est un sous-espace de V.*
- *Soient $V = \mathbb{R}^3$ et $W = \left\{ \left(\begin{smallmatrix} a \\ b \\ 2b \end{smallmatrix}\right) \mid a, b \in \mathbb{R} \right\} \subseteq V$. Alors, W est un sous-espace de V.*

Lemme 20.3. *Soient K un corps et V un K-espace vectoriel.*

(a) Soit $W \leq V$ un sous-espace vectoriel. Alors, W est un K-espace vectoriel.

(b) Soit $W \subseteq V$ un sous-ensemble. Alors, les assertions suivantes sont équivalentes :

(i) $W \leq V$ est un sous-espace vectoriel ;

(ii) $(W, +, 0)$ est un sous-groupe de $(V, +, 0)$ et $\forall\, a \in K, \forall\, w \in W : a \cdot w \in W$.

Démonstration. (a) L'hypothèse $\forall\, w_1, w_2 \in W, \forall a \in K : a \cdot w_1 + w_2 \in W$ nous assure que les opérations $+$ et $\cdot$ de V se restreignent à W, c'est-à-dire que leurs restrictions à $W \times W$ et $K \times W$ donnent des applications $+ : W \times W \to W$ et $\cdot : K \times W \to W$(pour voir cela pour « $+$ » prendre $a = 1$ et pour « $\cdot$ » prendre $w_2 = 0$). On voit que $0_V \in W$ en prenant $a = -1$ et $w_1 = w_2 = w$ pour n'importe quel $w \in W$ (ici on utilise que W n'est pas vide, ce qui est exigé dans la définition). Les propriétés comme l'associativité sont héritées des mêmes propriétés de V.
(b) « (i) $\Rightarrow$ (ii) » : Pour voir que $(W, +, 0)$ est un sous-groupe de $(V, +, 0)$ on utilise le lemme 12.4 : Soient $w_1, w_2 \in W$. En prenant $a = -1$ on obtient $w_2 - w_1 \in W$, donc le critère pour sous-groupes est satisfait. Pour $w \in W$, en prenant $w_1 = w$ et $w_2 = 0$ on voit aussi $a \cdot w \in W$.
« (ii) $\Rightarrow$ (i) » : Soient $a \in K$ et $w_1, w_2 \in W$. D'abord on a $a \cdot w_1 \in W$, puis $a \cdot w_1 + w_2 \in W$. Donc W est bien un sous-espace vectoriel de V. □

Très important : les solutions d'un système d'équations linéaires homogènes forment un sous-espace !

Proposition 20.4. *Soient K un corps et $n, m \in \mathbb{N}_{\geq 1}$. On considère le système d'équations linéaires*

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{aligned}$$

avec $b_i, a_{i,j} \in K$ pour $1 \leq i \leq m$, $1 \leq j \leq n$.

(a) Soit S l'ensemble de toutes les solutions du système homogène avec $x_1, x_2, \ldots, x_n \in K$, c'est-à-dire

$$S = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n \mid \forall i \in \{1, 2, \ldots, m\} : \sum_{j=1}^{n} a_{i,j}x_j = 0 \right\}.$$

Alors, S est un sous-espace vectoriel du K-espace vectoriel standard K^n.

(b) Soit $\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \in K^n$ une solution du système d'équations linéaires, c'est-à-dire :

$$\forall i \in \{1, 2, \ldots, m\} : \sum_{j=1}^{n} a_{i,j}r_j = b_i.$$

Soit S le sous-espace vectoriel de K^n défini en (a).

Alors, les solutions du système d'équations linéaires sont l'ensemble

$$\left\{ \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} + \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \mid \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in S \right\}.$$

Démonstration. (a) Soient $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in S$ et $\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in S$ et $\lambda \in K$. Alors, pour tout $i \in \{1, 2, \ldots, m\}$

$$\sum_{j=1}^{n} a_{i,j}(\lambda \cdot x_j + y_j) = \lambda \cdot \big(\sum_{j=1}^{n} a_{i,j}x_j\big) + \big(\sum_{j=1}^{n} a_{i,j}y_j\big) = \lambda \cdot 0 + 0 = 0,$$

donc, $\lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in S$.

De plus, S est non vide car il contient la solution $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Ainsi, S est un sous-espace vectoriel de K^n.

(b) On montre d'abord que tout objet de cette forme est une solution. Soit $\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in S$. Pour tout $i \in \{1, 2, \ldots, m\}$ on a

$$\sum_{j=1}^{n} a_{i,j}(r_j + s_j) = \big(\sum_{j=1}^{n} a_{i,j}r_j\big) + \big(\sum_{j=1}^{n} a_{i,j}s_j\big) = b_i + 0 = b_i.$$

Pour finir, on démontre que toute solution est de cette forme. Soit $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ une solution du système : $\forall i \in \{1, 2, \ldots, m\} : \sum_{j=1}^{n} a_{i,j}x_j = b_i$. Alors, pour tout $i \in \{1, 2, \ldots, m\}$

$$0 = b_i - b_i = \big(\sum_{j=1}^{n} a_{i,j}x_j\big) - \big(\sum_{j=1}^{n} a_{i,j}r_j\big) = \sum_{j=1}^{n} a_{i,j}(x_j - r_j).$$

Cela montre

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} := \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} - \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \in S,$$

donc, la solution est de la forme enoncée. □

Lemme 20.5. *Soient K un corps, V un K-espace vectoriel et $W_i \leq V$ des sous-espaces pour $i \in I \neq \emptyset$. Alors, $W := \bigcap_{i \in I} W_i$ est un sous-espace vectoriel de V.*

Démonstration. Soient $v, w \in W$ et $a \in K$. Pour tout $i \in I$ on a $a \cdot v + w \in W_i$ car W_i est un sous-espace de V. Par conséquent, $a \cdot v + w \in W$, ce qui démontre que W est un sous-espace de V. □

Définition 20.6. *Soient K un corps, V un K-espace vectoriel et $E \subseteq V$ un sous-ensemble. On dit que V est* engendré par E (en tant que sous-espace vectoriel) *si le seul sous-espace vectoriel de V qui contient E est V lui-même (comparer avec la définition 12.9).*

Définition-Lemme 20.7. *Soient K un corps, V un K-espace vectoriel et $E \subseteq V$ un sous-ensemble. On pose*

$$\langle E \rangle := \bigcap_{W \leq V \text{ sous-espace t.q. } E \subseteq W} W,$$

l'intersection de tous les sous-espaces W de V qui contiennent E, et on l'appelle le sous-espace vectoriel de V engendré par E.
C'est un sous-espace vectoriel de V qui est engendré par E.

Démonstration. La démonstration se fait de la même manière que celle de la définition-lemme 12.11. □

Définition 20.8. *Soient K un corps, V un K-espace vectoriel et $W_i \leq V$ des sous-espaces de V pour $i \in I \neq \emptyset$. On pose*

$$\sum_{i\in I} W_i := \langle \bigcup_{i\in I} W_i \rangle,$$

le sous-espace de V engendré par tous les éléments de tous les W_i. On l'appelle la somme des W_i, *$i \in I$.*

Proposition 20.9. *Soient K un corps et V un K-espace vectoriel.*

(a) Soit $E \subseteq V$ un sous-ensemble. Alors,

$$\langle E \rangle = \left\{ \sum_{i=1}^{n} a_i e_i \mid n \in \mathbb{N}, a_1, \ldots, a_n \in K, e_1, \ldots, e_n \in E \right\}.$$

(Comparer avec la proposition 12.13.)

(b) Soient $W_i \leq V$ des sous-espaces de V pour $i \in I \neq \emptyset$. Alors,

$$\sum_{i\in I} W_i = \left\{ \sum_{i\in I} w_i \mid w_i \in W_i \text{ pour } i \in I \text{ t.q. } w_i = 0 \text{ sauf pour un nombre fini de } i \in I \right\}.$$

On utilisera la notation $\sum'_{i\in I} w_i$ avec $w_i \in W_i$ et la condition que seulement un nombre fini de w_i sont $\neq 0$.

Démonstration. (a) Appelons U l'ensemble à droite. On a $U \subseteq \langle E \rangle$ parce que $E \subseteq \langle E \rangle$, et, $\langle E \rangle$ étant un sous-espace vectoriel, les combinaisons K-linéaires des éléments de E appartiennent à $\langle E \rangle$. D'autre part, il est clair que U est un sous-espace vectoriel de V et que U contient E. Comme $\langle E \rangle$ est l'intersection de tous les sous-espace de V qui contiennent E, on obtient $\langle E \rangle \subseteq U$.
(b) Appelons W l'ensemble à droite. On a $W \subseteq \sum_{i\in I} W_i$ parce que $W_j \subseteq \sum_{i\in I} W_i$ pour tout $j \in I$ et, $\sum_{i\in I} W_i$ étant un sous-espace vectoriel, les sommes finies d'éléments de $\sum_{i\in I} W_i$ y sont aussi contenues. D'autre part, il est clair que W est un sous-espace vectoriel de V et que W contient $\bigcup_{i\in I} W_i$. Comme $\sum_{i\in I} W_i$ est l'intersection de tous les sous-espace de V qui contiennent $\bigcup_{i\in I} W_i$, on obtient $\sum_{i\in I} W_i \subseteq W$. □

Quand est-ce que les $w_i \in W_i$ dans l'écriture $w = \sum'_{i\in I} w_i$ sont uniques ?

Définition 20.10. *Soient K un corps, V un K-espace vectoriel et $W_i \leq V$ des sous-espaces de V pour $i \in I \neq \emptyset$.*
On dit que la somme $W = \sum_{i\in I} W_i$ est directe *si pour tout $i \in I$ on a*

$$W_i \cap \sum_{j\in I\setminus\{i\}} W_j = 0.$$

Notation pour les sommes directes : $\bigoplus_{i\in I} W_i$.
Si $I = \{1, \dots, n\}$*, on note parfois les éléments d'une somme directe* $\bigoplus_{i=1}^n W_i$ *par* $w_1 \oplus w_2 \oplus \cdots \oplus w_n$ *(où, évidemment,* $w_i \in W_i$ *pour* $i \in I$*).*

Proposition 20.11. *Soient* K *un corps,* V *un* K*-espace vectoriel,* $W_i \leq V$ *des sous-espaces de* V *pour* $i \in I \neq \emptyset$ *et* $W = \sum_{i\in I} W_i$*. Alors les assertions suivantes sont équivalentes :*

(i) $W = \bigoplus_{i\in I} W_i$ *;*

(ii) pour tout $w \in W$ *et tout* $i \in I$ *il existe un unique* $w_i \in W_i$ *tel que* $w = \sum'_{i\in I} w_i$*.*

Démonstration. « (i) $\Rightarrow$ (ii) » : L'existence de tels $w_i \in W_i$ provient de la proposition 20.9 (b). Démontrons donc l'unicité en prenant

$$w = \sum_{i\in I}{}' w_i = \sum_{i\in I}{}' w'_i$$

avec $w_i, w'_i \in W_i$ pour tout $i \in I$ (rappelons que la notation $\sum'$ indique que seul un nombre fini de w_i, w'_i est non nul). Cela implique pour $i \in I$:

$$w_i - w'_i = \sum_{j\in I\setminus\{i\}}{}' (w'_j - w_j) \in W_i \cap \sum_{j\in I\setminus\{i\}} W_j = 0.$$

Donc, $w_i - w'_i = 0$, alors $w_i = w'_i$ pour tout $i \in I$, montrant l'unicité.
« (ii) $\Rightarrow$ (i) » : Soient $i \in I$ et $w_i \in W_i \cap \sum_{j\in I\setminus\{i\}} W_j$. Donc, $w_i = \sum'_{j\in I\setminus\{i\}} w_j$ avec $w_j \in W_j$ pour tout $j \in I$. Nous pouvons maintenant écrire 0 de deux façons

$$0 = \sum_{i\in I}{}' 0 = -w_i + \sum_{j\in I\setminus\{i\}}{}' w_j.$$

Donc, l'unicité implique $-w_i = 0$. Alors, nous avons montré $W_i \cap \sum_{j\in I\setminus\{i\}} W_j = 0$. □

21 Bases et dimension

Bases

Définition 21.1. *Soient* K *un corps et* V *un* K*-espace vectoriel. Soit* $E \subseteq V$ *un sous-ensemble. Rappelons d'abord que l'on dit que* E *engendre* V *(en tant que* K*-espace vectoriel) si* $\langle E\rangle = V$*, c'est-à-dire que tout* $v \in V$ *s'écrit sous la forme* $v = \sum_{i=1}^n a_i e_i$ *avec* $n \in \mathbb{N}$*,* $a_1, \dots, a_n \in K$ *et* $e_1, \dots, e_n \in E$*.*
On dit que E *est* K-linéairement indépendant *si*

$$\forall\, n \in \mathbb{N}\, \forall\, a_1, \dots, a_n \in K\, \forall\, e_1, \dots, e_n \in E : \big(\sum_{i=1}^n a_i e_i = 0 \in V \Rightarrow a_1 = a_2 = \cdots = a_n = 0\big)$$

(c'est-à-dire, la seule combinaison K*-linéaire d'éléments de* E *représentant* $0 \in V$ *est celle dans laquelle tous les coefficients sont* 0*). Dans le cas contraire, on dit que* E *est* K-linéairement dépendant.
On appelle E *une* K-base de V *si* E *engendre* V *et* E *est* K*-linéairement indépendant.*

Exemple 21.2. *Soit K un corps et $d \in \mathbb{N}_{>0}$. On pose* $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_d = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ *et* $E = \{e_1, e_2, \ldots, e_d\}$. *Alors :*

- *E engendre K^d :*

  Tout vecteur $v = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_d \end{pmatrix}$ *s'écrit comme K-combinaison linéaire :* $v = \sum_{i=1}^{d} a_i e_i$.

- *E est K-linéairement indépendant :*

  Si l'on a une combinaison K-linéaire $0 = \sum_{i=1}^{d} a_i e_i$, *alors clairement* $a_1 = \cdots = a_d = 0$.

- *E est donc une K-base de K^d, car E engendre K^d et est K-linéairement indépendant. On l'appelle la* base canonique *de K^d.*

Le prochain théorème caractérise les bases.

Théorème 21.3. *Soit K un corps, V un K-espace vectoriel et $E = \{e_1, e_2, \ldots, e_n\} \subseteq V$ un sous-ensemble fini. Alors, les assertions suivantes sont équivalentes :*

(i) *E est une K-base.*

(ii) *E est un ensemble minimal de générateurs de V, c'est-à-dire : E engendre V, mais pour tout $e \in E$, l'ensemble $E \setminus \{e\}$ n'engendre pas V.*

(iii) *E est un ensemble maximal K-linéairement indépendant, c'est-à-dire : E est K-linéairement indépendant, mais pour tout $e \in V \setminus E$, l'ensemble $E \cup \{e\}$ est K-linéairement dépendant.*

(iv) *Tout $v \in V$ s'écrit comme $v = \sum_{i=1}^{n} a_i e_i$ avec des uniques $a_1, \ldots, a_n \in K$.*

Démonstration. Nous allons démontrer « (i) ⇒ (ii) ⇒ (iv) ⇒ (iii) ⇒ (i) ».
« (i) ⇒ (ii) » : Supposons que $E \setminus \{e_i\}$ pour un $i \in \{1, \ldots, n\}$ engendre V. En particulier, nous pouvons écrire $e_i = \sum_{j=1, j\neq i}^{n} a_j e_j$ avec $a_j \in K$ pour $j \in \{1, \ldots, n\} \setminus \{i\}$. Cela nous donne une K-combinaison linéaire égale à zéro si l'on pose $a_i = -1$:

$$0 = \sum_{j=1}^{n} a_j e_j.$$

Cela est une contradiction à l'indépendance K-linéaire de E.
« (ii) ⇒ (iv) » : Soit E un ensemble minimal de générateurs de V et soit $v \in V$ tel que

$$v = \sum_{i=1}^{n} a_i e_i = \sum_{i=1}^{n} b_i e_i.$$

Supposons qu'il existe $j \in \{1, 2, \ldots, n\}$ tel que $a_j \neq b_j$. Alors on a

$$e_j = \sum_{i=1, i\neq j}^{n} \frac{b_i - a_i}{a_j - b_j} e_i.$$

Donc, E n'est pas minimal car on peut exprimer e_j par les autres éléments de E. Cette contradiction montre l'unicité.
« (iv) $\Rightarrow$ (iii) » : D'abord on montre que E est K-linéairement indépendant. Cela résulte de l'unicité. Soit $0 = \sum_{i=1}^{n} a_i e_i$ une combinaison K-linéaire. Mais, il existe aussi la combinaison K-linéaire $0 = \sum_{i=1}^{n} 0 \cdot e_i$. Donc, l'unicité implique $0 = a_1 = \cdots = a_n$ et l'indépendance K-linéaire est démontrée. Soit maintenant $e \in V \setminus E$. On l'écrit $e = \sum_{i=1}^{n} a_i e_i$. L'ensemble $E \cup \{e\}$ n'est plus K-linéairement indépendant parce que $0 = -1 \cdot e + \sum_{i=1}^{n} a_i e_i$.
« (iii) $\Rightarrow$ (i) » : Soit E un ensemble maximal K-linéairement indépendant. Il faut montrer que E engendre V. Soit donc $v \in V$. Si $v \in E$, alors $v = e_i$ pour un $i \in \{1, \ldots, n\}$, donc $v \in \langle E \rangle$. Si $v \notin E$, on sait par (iii) que $E \cup \{v\}$ est K-linéairement dépendant. Nous avons donc une combinaison K-linéaire

$$0 = av + \sum_{i=1}^{n} a_i e_i$$

dans laquelle au moins un des coefficients est non-zéro. Notons que a doit être non-zéro car le cas contraire donnerait une contradiction à l'indépendance K-linéaire de E. Nous obtenons donc

$$v = \sum_{i=1}^{n} \frac{-a_i}{a} e_i \in \langle E \rangle.$$

Cela montre que E engendre V. □

Corollaire 21.4. *Soient K un corps, V un K-espace vectoriel et $E \subseteq V$ un ensemble fini qui engendre V. Alors, V possède une K-base contenue dans E.*

Démonstration. On enlevant des éléments de E successivement, on obtient un ensemble minimal de générateurs qui est une K-base à cause du théorème 21.3. □

Dans le cours Algèbre 2 nous allons démontrer à l'aide du lemme de Zorn que tout espace vectoriel possède une base.

Exemple 21.5. *(a) Soit* $V = \left\{ \begin{pmatrix} a \\ a \\ b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. *Une base de V est* $\left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$.

(b) Soit $V = \langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 7 \end{pmatrix} \rangle \subseteq \mathbb{Q}^3$.

L'ensemble $E = \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \right\}$ *est une $\mathbb{Q}$-base de V. Raison :*

- *Le système d'équations linéaires*

$$a_1 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + a_2 \cdot \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} + a_3 \cdot \begin{pmatrix} 3 \\ 5 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

  possède une solution non nulle (par exemple $a_1 = 1$, $a_2 = 1$, $a_3 = -1$). Cela implique que E engendre V car on peut exprimer le troisième générateur par les deux premiers.

- *Le système d'équations linéaires*

$$a_1 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + a_2 \cdot \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

  ne possède que $a_1 = a_2 = 0$ comme solution. Donc E est $\mathbb{Q}$-linéairement indépendant.

(c) Le $\mathbb{R}$-espace vectoriel

$$V = \{f : \mathbb{N} \to \mathbb{R} \mid \exists\, S \subseteq \mathbb{N} \text{ fini } \forall\, n \in \mathbb{N} \setminus S : f(n) = 0\}$$

possède $\{e_n \mid n \in \mathbb{N}\}$ avec $e_n(m) = \delta_{n,m}$ (Delta de Kronecker : $\delta_{n,m} = \begin{cases} 1 & \text{si } n = m, \\ 0 & \text{si } n \neq m. \end{cases}$) comme $\mathbb{R}$-base. Cela est donc une base avec une infinité d'éléments.

(d) Similaire à l'exemple précédent, le $\mathbb{R}$-espace vectoriel

$$V = \{f : \mathbb{R} \to \mathbb{R} \mid \exists\, S \subseteq \mathbb{R} \text{ fini } \forall\, x \in \mathbb{R} \setminus S : f(x) = 0\}$$

possède $\{e_x \mid x \in \mathbb{R}\}$ avec $e_x(y) = \delta_{x,y}$ comme $\mathbb{R}$-base. Cela est donc une base qui n'est pas dénombrable.

Dimension

Lemme 21.6. *Soient K un corps et V un K-espace vectoriel avec une K-base $B = \{e_1, \ldots, e_n\}$. Soit $w = \sum_{i=1}^{n} a_i e_i \in V$. Si $a_j \neq 0$, alors $B' = \{e_1, \ldots, e_{j-1}, w, e_{j+1}, \ldots, e_n\}$ est une K-base. On peut donc changer e_j en w (avec $a_j \neq 0$) et on obtient encore une K-base.*

Démonstration. Il faut montrer (1) que B' engendre V et (2) que B' est K-linéairement indépendant. Pour (1), il suffit de montrer que l'on peut exprimer e_j comme combinaison K-linéaire des éléments de B'. On a

$$e_j = \frac{1}{a_j} w + \sum_{i=1, i\neq j}^{n} \frac{-a_i}{a_j} e_i.$$

Pour (2), supposons que nous avons une combinaison K-linéaire

$$0 = bw + \sum_{i=1, i\neq j}^{n} b_i e_i.$$

Cela nous donne

$$0 = b(\sum_{i=1}^{n} a_i e_i \in V) + \sum_{i=1, i\neq j}^{n} b_i e_i = ba_j e_j + \sum_{i=1, i\neq j}^{n} (a_i + b_i) e_i.$$

Comme B est K-linéairement indépendant, nous avons $ba_j = 0$, donc $b = 0$ (car $a_j \neq 0$), alors $0 = \sum_{i=1, i\neq j}^{n} b_i e_i$, ce qui donne bien $b_i = 0$ pour tout $i \in \{1, \ldots, n\} \setminus \{j\}$. Cela montre que B' est K-linéairement indépendant. □

Proposition 21.7 (Basisaustauschsatz)**.** *Soient K un corps et V un K-espace vectoriel avec une K-base $B = \{e_1, \ldots, e_n\}$. Soit $C = \{w_1, \ldots, w_r\} \subseteq V$ un sous-ensemble fini de V, K-linéairement indépendant.*
Alors, $r \leq n$ et il existe des indices $i_1, \ldots, i_r \in \{1, \ldots, n\}$ avec la propriété que si l'on change e_{i_j} en w_j dans B pour $j = 1, \ldots, r$, on obtient une K-base de V.
Autrement dit, si l'on change la numérotation des éléments de B telle que $i_j = j$, alors $B' = \{w_1, \ldots, w_r, e_{r+1}, e_{r+2}, \ldots, e_n\}$ est une K-base de V.

Démonstration. Nous utilisons récurrence en r. Si $r = 0$, l'assertion est triviale (pas d'échange à faire). Donc, supposons que l'assertion de la proposition est vraie pour $r - 1$ et nous allons la démontrer pour $r \geq 1$. Comme $w_1, \ldots, w_r$ sont K-linéairement indépendants, alors $w_1, \ldots, w_{r-1}$ sont K-linéairement indépendants. Après changement de numérotation nous obtenons de l'hypothèse de récurrence pour $r - 1$ que $\{w_1, \ldots, w_{r-1}, e_r, e_{r+1}, \ldots, e_n\}$ est une K-base et que $r - 1 \leq n$. Remarquons d'abord que $r - 1 = n$ est impossible (donc $r \leq n$) car dans ce cas $\{w_1, \ldots, w_{r-1}\}$ serait une K-base et en conséquence un ensemble K-linéairement indépendant maximal (théorème 21.3) ce qui n'est clairement pas le cas. Nous pouvons écrire w_r comme combinaison K-linéaire

$$w_r = \sum_{i=1}^{r-1} a_i w_i + \sum_{i=r}^{n} a_i e_i.$$

On montre maintenant qu'il existe $a_j \neq 0$ pour un j tel que $r \leq j \leq n$. Supposons le contraire. Dans ce cas, $0 = \sum_{i=1}^{r-1} a_i w_i + (-1) \cdot w_r$ ce qui contredit l'indépendance K-linéaire de C. Le lemme 21.6 nous permet de changer e_j en w_r. Cela finit la preuve. □

Corollaire 21.8. *Soient K un corps et V un K-espace vectoriel qui possède une K-base finie. Alors, toutes les K-bases de V sont finies et ont la même cardinalité.*

Démonstration. Soit $B = \{e_1, \ldots, e_n\}$ une K-base de V. La proposition 21.7 implique qu'il n'existe pas d'ensemble K-linéairement indépendant de cardinalité strictement plus grand que n. Donc toute autre K-base B' a au plus n éléments. Si on échange les rôles de B et B', on obtient qu'elles ont le même cardinal. □

Ce corollaire nous permet de faire une définition très importante, celle de la dimension d'un espace vectoriel. La dimension mesure la « taille » ou le « nombre de degrés de liberté » d'un espace vectoriel.

Définition 21.9. *Soient K un corps et V un K-espace vectoriel. Si V possède une K-base finie de cardinalité n, on dit que V est de* dimension n. *Si V ne possède pas de K-base finie, on dit que V est de* dimension infinie.
Notation : $\dim_K(V)$.

Exemple 21.10. *(a) Soit K un corps. La dimension du K-espace vectoriel standard K^n est égale à n.*

(b) Soit K un corps. Le K-espace vectoriel nul $(\{0\}, +, \cdot, 0)$ est de dimension 0 (et c'est le seul).

(c) Le $\mathbb{R}$-espace vectoriel $\mathcal{F}(\mathbb{N}, \mathbb{R})$ est de dimension infinie.

Lemme 21.11. *Soient K un corps, V un K-espace vectoriel de dimension n et $W \leq V$ un sous-espace.*

(a) $\dim_K(W) \leq \dim_K(V)$.

(b) Si $\dim_K(W) = \dim_K(V)$, *alors* $W = V$.

Démonstration. Soient $B = \{e_1, \ldots, e_n\}$ une K-base de V et $C = \{w_1, \ldots, w_r\} \subseteq W$ un ensemble K-linéairement indépendant. Donc, la proposition 21.7 implique $r \leq n$ et nous pouvons supposer que cet ensemble est maximal et alors une K-base de W (théorème 21.3). Si $r = n$, alors après avoir échangé tous les éléments de B contre ceux de C, on voit que C est une K-base de V ; en particulier, C engendre V ce qui implique $W = V$ (car W est le sous-espace engendré par C). □

Le contenu de la proposition suivante est que tout ensemble K-linéairement indépendant peut être complété pour devenir une K-base.

Proposition 21.12 (Basisergänzungssatz)**.** *Soient K un corps, V un K-espace vectoriel de dimension n, $E \subseteq V$ un ensemble fini tel que E engendre V et $\{e_1, \ldots, e_r\} \subset V$ un sous-ensemble qui est K-linéairement indépendant. (Noter $r \leq n$ par la proposition 21.7.)*
Alors, il existe $e_{r+1}, e_{r+2}, \ldots, e_n \in E$ tels que $\{e_1, \ldots, e_n\}$ est une K-base de V.

Démonstration. Le corollaire 21.4 nous permet de choisir une K-base B parmi les éléments de E. Par la proposition 21.7 nous échangeons des éléments de B par $e_1, \ldots, e_r$ en gardant une K-base. □

La proposition 21.12 se démontre aussi de façon constructive. Supposons que nous avons déjà des éléments $e_1, \ldots, e_r$ qui sont K-linéairement indépendants. Si $r = n$, ces éléments sont une K-base par le lemme 21.11 (b) et il ne reste rien à faire. Supposons donc $r < n$. Nous parcourons maintenant les éléments de E jusqu'à trouver un $e \in E$ tel que $e_1, \ldots, e_r, e$ sont K-linéairement indépendants. Un tel e doit exister car sinon l'ensemble E serait contenu dans le sous-espace engendré par $e_1, \ldots, e_r$, il ne pourrait donc pas engendrer V. On nomme $e =: e_{r+1}$ et on a un ensemble K-linéairement indépendant de cardinalité $r + 1$. Il suffit maintenant de continuer ce processus jusqu'à arriver à un ensemble K-linéairement indépendant de n éléments, qui est automatiquement une K-base.

Proposition 21.13. *Soient K un corps commutatif et V un K-espace vectoriel de dimension finie n. Soit $B \subset V$ un sous-ensemble de cardinal n. Alors, les assertions suivantes sont équivalentes.*

(i) B est un K-base.

(ii) B est K-linéairement indépendant.

(iii) B engendre V.

Démonstration. Pour l'équivalence entre (i) et (ii) il suffit de remarquer qu'un ensemble K-linéairement indépendant de cardinal n est nécessairement maximal (donc une K-base par le théorème 21.3), car s'il n'était pas maximal, il y aurait un ensemble maximal K-linéairement indépendant de cardinal strictement supérieur à n, donc une K-base de cardinal différent de n ce qui n'est pas possible selon le corollaire 21.8.
Similairement, pour l'équivalence entre (i) et (iii) il suffit de remarquer qu'un ensemble de cardinal n qui engendre V est nécessairement minimal (donc une K-base par le théorème 21.3), car s'il n'était pas minimal, il y aurait un ensemble minimal de cardinal strictement inférieur à n qui engendre V, donc une K-base de cardinal différent de n. □

22 Homomorphismes linéaires et matrices

Applications linéaires : les homomorphismes des espaces vectoriels

On rappelle l'idée des (homo-)morphismes : ce sont les applications qui respectent toutes les structures.
Nous allons maintenant introduire les homomorphismes des espaces vectoriels : les applications linéaires.

Définition 22.1. *Soient K un corps et V, W des K-espaces vectoriels. Une application*

$$\varphi : V \to W$$

est appelée K-linéaire *ou* (homo-)morphisme de K-espaces vectoriels *si*

$$\forall\, v_1, v_2 \in V : \varphi(v_1 +_V v_2) = \varphi(v_1) +_W \varphi(v_2)$$

et

$$\forall\, v \in V, \forall a \in K : \varphi(a \cdot_V v) = a \cdot_W \varphi(v).$$

Un homomorphisme bijectif de K-espaces vectoriels s'appelle isomorphisme. *On note souvent les isomorphismes par un tilde : $\varphi : V \xrightarrow{\sim} W$. S'il existe un isomorphisme $V \to W$, on écrit souvent simplement $V \cong W$.*

Remarque 22.2. *Si $\varphi : V \to W$ est un homomorphisme de K-espaces vectoriels, alors φ est en particulier un homomorphisme de groupes $(V, +, 0) \to (W, +, 0)$.*
On peut formuler cela de façon plus forte. Soient V, W des K-espaces vectoriels et $\varphi : V \to W$ une application. Alors, les assertions suivantes sont équivalentes :

(i) *φ est un homomorphisme de K-espaces vectoriels.*

(ii) *φ est un homomorphisme de groupes $(V, +, 0) \to (W, +, 0)$ et pour tout $v \in V$ et tout $a \in K$ on a $\varphi(a \cdot v) = a \cdot \varphi(v)$.*

Exemple 22.3. *(a) On commence par l'exemple le plus important. Soit K un corps et $n \in \mathbb{N}$. Soit*

$$M = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

une matrice à n colonnes, m lignes et à coefficients dans K (on note l'ensemble de ces matrices par $\mathrm{Mat}_{m\times n}(K)$; c'est aussi un K-espace vectoriel). Elle définit l'application K-linéaire

$$\varphi : K^n \to K^m, \quad v \mapsto Mv$$

où Mv est le produit habituel de matrices. Explicitement,

$$\varphi(v) = Mv = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n a_{1,i}v_i \\ \sum_{i=1}^n a_{2,i}v_i \\ \vdots \\ \sum_{i=1}^n a_{m,i}v_i \end{pmatrix}.$$

La K-linéarité s'exprime comme

$$\forall\, a \in K\, \forall\, v, w \in V : M \circ (a \cdot v + w) = a \cdot (M \circ v) + M \circ w.$$

Cette égalité est très facile à vérifier (vous avez du la voir dans votre cours d'algèbre linéaire).

(b) Soit $a \in \mathbb{R}$. Alors, $\varphi : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax$ est $\mathbb{R}$-linéaire (c'est le cas spécial $n = m = 1$ de (a) si l'on regarde le scalaire a comme une matrice (a)). Par contre, si $0 \neq b \in \mathbb{R}$, alors $\mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$ n'est pas $\mathbb{R}$-linéaire !

(c) Soit $n \in \mathbb{N}$. Alors, l'application $\varphi : \mathcal{F}(\mathbb{N}, \mathbb{R}) \to \mathbb{R}$, $f \mapsto f(n)$ est K-linéaire.

Définition 22.4. *Soient K un corps, V, W des K-espaces vectoriels et $\varphi : V \to W$ une application K-linéaire. Le* noyau de φ *est défini comme*

$$\ker(\varphi) = \{v \in V \mid \varphi(v) = 0\}.$$

Proposition 22.5. *Soient K un corps, V, W des K-espaces vectoriels et $\varphi : V \to W$ une application K-linéaire.*

(a) $\mathrm{Im}(\varphi)$ est un sous-espace vectoriel de W.

(b) $\ker(\varphi)$ est un sous-espace vectoriel de V.

(c) φ est surjectif si et seulement si $\mathrm{Im}(\varphi) = W$.

(d) φ est injectif si et seulement si $\ker(\varphi) = 0$.

(e) Si φ est un isomorphisme, son inverse l'est aussi (en particulier, son inverse est aussi K-linéaire).

Démonstration. (a) Soient $w_1 = \varphi(v_1), w_2 = \varphi(v_2) \in \mathrm{Im}(\varphi)$ et $a \in K$. Alors, $aw_1 + w_2 = a\varphi(v_1) + \varphi(v_2) = \varphi(av_1) + \varphi(v_2) = \varphi(av_1 + v_2) \in \mathrm{Im}(\varphi)$.
(b) Soient $v_1, v_2 \in \ker(\varphi)$ et $a \in K$. Alors, $\varphi(av_1 + v_2) = \varphi(av_1) + \varphi(v_2) = a\varphi(v_1) + \varphi(v_2) = a \cdot 0 + 0 = 0$, donc $av_1 + v_2 \in \ker(\varphi)$.
(c) Cela est vrai pour toute application, donc en particulier pour les applications K-linéaires.
(d) Cela est vrai pour tout homomorphisme de groupes, donc par la remarque 22.2 en particulier pour les applications K-linéaires.
(e) Soit ψ l'inverse de φ. Pour les homomorphismes groupes on a déjà vu cette assertion. Il suffit donc de montrer $\psi(a \cdot w) = a \cdot \psi(w)$ pour tout $a \in K$ et tout $w \in W$. On commence par $a \cdot w = a \cdot \varphi(\psi(w)) = \varphi(a \cdot \psi(w))$, dont on déduit $\psi(a \cdot w) = \psi(\varphi(a \cdot \psi(w))) = a \cdot \psi(w)$. □

Matrices et représentation des applications linéaires

Dans l'exemple 22.3 (a) nous avons vu que les matrices donnent lieu à des applications K-linéaires. Il est très important et parfois appelé *théorème principal de l'algèbre linéaire* que l'assertion inverse est aussi vraie : **après choix de bases** toute application K-linéaire est donnée par une matrice.

Notation 22.6. *Soient K un corps, V un K-espace vectoriel et $S = \{v_1, \ldots, v_n\}$ une K-base de V. Nous rappelons que l'on a $v = \sum_{i=1}^{n} b_i v_i$ avec des uniques $b_1, \ldots, b_n \in K$; ce sont les coordonnées de v pour la base S. Nous utilisons la notation suivante :*

$$v_S = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in K^n.$$

Exemple 22.7. *(a) Soient K un corps, $n \in \mathbb{N}$ et $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$. Donc $E = \{e_1, e_2, \ldots, e_n\}$ est la K-base canonique de K^n.*

Alors, pour tout $v = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} \in K^n$ on a $v_E = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix}$.

(b) Soit $V = \mathbb{R}^2$ et $S = \{\binom{1}{1}, \binom{1}{-1}\}$. C'est une $\mathbb{R}$-base de V (car la dimension est 2 et les deux vecteurs sont $\mathbb{R}$-linéairement indépendants). Soit $v = \binom{4}{2} \in V$. Alors, $v = 3 \cdot \binom{1}{1} + \binom{1}{-1}$, donc $v_S = \binom{3}{1}$.

Proposition 22.8. *Soient K un corps et V un K-espace vectoriel de dimension finie n avec K-base $S = \{v_1, \ldots, v_n\}$.*
Alors, l'application $\varphi = ()_S : V \to K^n$ donnée par $v \mapsto v_S$ est un K-isomorphisme.

Démonstration. Soient $v, w \in V$ et $a \in K$. On écrit v et w en coordonnées pour la base S : $v = \sum_{i=1}^{n} b_i v_i$ et $w = \sum_{i=1}^{n} c_i v_i$. Donc, nous avons $av + w = \sum_{i=1}^{n} (ab_i + c_i)v_i$. Ecrit comme vecteurs on trouve alors :

$$v_S = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, \quad w_S = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \text{ et } (av+w)_S = \begin{pmatrix} ab_1 + c_1 \\ ab_2 + c_2 \\ \vdots \\ ab_n + c_n \end{pmatrix},$$

donc l'égalité $(a \cdot v + w)_S = a \cdot v_S + w_S$. Cela montre que l'application φ est K-linéaire. On démontre qu'elle est bijective.

Injectivité : Soit $v \in V$ tel que $v_S = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \ker(\varphi)$. Cela veut dire que $v = \sum_{i=1}^{n} 0 \cdot v_i = 0$. Le noyau de φ ne contient donc que 0, alors, φ est injective.

Surjectivité : Soit $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n$. On pose $v := \sum_{i=1}^{n} a_i \cdot v_i$. Nous avons $\varphi(v) = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ et la surjectivité est démontrée.

□

Théorème 22.9. *Soient K un corps, V, W deux K-espaces vectoriels de dimensions finies n et m et $\varphi : V \to W$ une application K-linéaire. Soient $S = \{v_1, \ldots, v_n\}$ une K-base de V et $T = \{w_1, \ldots, w_m\}$ une K-base de W. Pour tout $1 \leq i \leq n$, le vecteur $\varphi(v_i)$ appartient à W. On peut donc l'exprimer en tant que combinaison K-linéaire des vecteurs dans la base T ainsi :*

$$\varphi(v_i) = \sum_{j=1}^{m} a_{j,i} w_j.$$

Nous « rassemblons » les coefficients $a_{j,i}$ dans une matrice :

$$M_{T,S}(\varphi) := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \in \mathrm{Mat}_{m \times n}(K).$$

Alors, pour tout $v \in V$ on a

$$(\varphi(v))_T = M_{T,S}(\varphi) \circ v_S.$$

C'est-à-dire que le produit matriciel $M_{T,S}(\varphi) \circ v_S$ donne les coordonnées dans la base T de l'image $\varphi(v)$. Alors, la matrice $M_{T,S}(\varphi)$ décrit l'application K-linéaire φ en coordonnées.

Remarquons qu'il est facile d'écrire la matrice $M_{T,S}(\varphi)$: la i-ème colonne de $M_{T,S}(\varphi)$ est $(\varphi(v_i))_T$.

Démonstration. Nous faison un calcul matriciel très facile :

$$M_{T,S}(\varphi) \circ (v_i)_S = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \circ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,i} \\ a_{2,i} \\ \vdots \\ a_{m,i} \end{pmatrix} = (\varphi(v_i))_T,$$

où le 1 est dans la i-ième ligne du vecteur. Nous avons donc obtenu le résultat pour les vecteurs v_i dans la base S.
L'assertion générale suit par linéarité : Soit $v = \sum_{i=1}^n b_i v_i$. Alors nous obtenons

$$\begin{aligned} M_{T,S}(\varphi) \circ (\sum_{i=1}^n b_i v_i)_S &= \sum_{i=1}^n b_i \cdot \big(M_{T,S}(\varphi) \circ (v_i)_S\big) \\ &= \sum_{i=1}^n b_i \cdot (\varphi(v_i))_T = (\sum_{i=1}^n b_i \cdot \varphi(v_i))_T = (\varphi(\sum_{i=1}^n b_i \cdot v_i))_T = (\varphi(v))_T. \end{aligned}$$

Cela montre le théorème. □

Exemple 22.10. *$\mathbb{C}$ possède la $\mathbb{R}$-base $B = \{1, i\}$. Soit $z = x+iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$, donc $z_B = \binom{x}{y}$. Soit $a = r + is$ avec $r, s \in \mathbb{R}$. L'application*

$$\varphi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto a \cdot z$$

est $\mathbb{R}$-linéaire. Nous décrivons $M_{B,B}(\varphi)$. La première colonne est $(a \cdot 1)_B = (r + is)_B = \binom{r}{s}$, et la deuxième colonne est $(a \cdot i)_B = (-s + ir)_B = \binom{-s}{r}$, alors $M_B(\varphi) = \left(\begin{smallmatrix} r & -s \\ s & r \end{smallmatrix}\right)$.

Définition 22.11. *Notons $\mathrm{Hom}_K(V, W)$ l'ensemble de toutes les applications $\varphi : V \to W$ qui sont K-linéaires.*
Dans le cas spécial $W = V$, une application K-linéaire $\varphi : V \to V$ est aussi appelée endomorphisme *de V et nous écrivons*

$$\mathrm{End}_K(V) := \mathrm{Hom}_K(V, V).$$

Corollaire 22.12. *Soient K un corps, V, W deux K-espaces vectoriels de dimensions finies n et m. Soient $S = \{v_1, \ldots, v_n\}$ une K-base de V et $T = \{w_1, \ldots, w_m\}$ une K-base de W.*
Alors, l'application

$$\mathrm{Hom}_K(V, W) \to \mathrm{Mat}_{m \times n}(K), \quad \varphi \mapsto M_{T,S}(\varphi)$$

est une bijection.

Il est important de souligner que les bases dans le corollaire sont fixées ! La même matrice peut exprimer des applications linéaires différentes si on change les bases.

Démonstration. **Injectivité :** Supposons $M_{T,S}(\varphi) = M_{T,S}(\psi)$ pour $\varphi, \psi \in \mathrm{Hom}_K(V, W)$. Alors pour tout $v \in V$, on a $(\varphi(v))_T = M_{T,S}(\varphi) \circ v_S = M_{T,S}(\psi) \circ v_S = (\psi(v))_T$. Comme l'écriture en coordonnées est unique, nous trouvons $\varphi(v) = \psi(v)$ pour tout $v \in V$, donc $\varphi = \psi$.

Surjectivité : Soit $M \in \mathrm{Mat}_{m\times n}(K)$ une matrice. On définit $\varphi \in \mathrm{Hom}_K(V,W)$ par

$$(\varphi(v))_T = M \circ v_S$$

pour $v \in V$. Il est clair que φ est K-linéaire. En plus, nous avons

$$M_{T,S}(\varphi) \circ v_S = (\varphi(v))_T = M \circ v_S$$

pour tout $v \in V$. Prenant $v = v_i$ de façon que $(v_i)_S$ est le vecteur dont la i-ème coordonnée est 1 et le reste est 0, on obtient que les i-èmes colonnes de $M_{T,S}(\varphi)$ et de M sont les mêmes. Cela montre $M = M_{T,S}(\varphi)$.

□

Définition-Lemme 22.13. *Soient K un corps et V un K-espace vectoriel de dimension finie n. Soient S_1, S_2 deux K-bases de V. On pose*

$$C_{S_2,S_1} := M_{S_2,S_1}(\mathrm{id}_V)$$

et on l'appelle matrice de changement de bases.

(a) C_{S_2,S_1} est une matrice à n colonnes et n lignes.

(b) Pour tout $v \in V$:

$$v_{S_2} = C_{S_2,S_1} \circ v_{S_1}.$$

En mots : la multiplication de la matrice de changement de bases par le vecteur v exprimé en coordonnées pour la base S_1, donne le vecteur v exprimé en coordonnées pour la base S_2.

(c) C_{S_2,S_1} est inversible d'inverse C_{S_1,S_2}.

Il est facile d'écrire la matrice C_{S_2,S_1} : sa j-ième colonne est formée des coordonnées dans la base S_2 du j-ième vecteur de la base S_1.

Démonstration. (a) C'est clair.
(b) $C_{S_2,S_1} \circ v_{S_1} = M_{S_2,S_1}(\mathrm{id}_V) \circ v_{S_1} = (\mathrm{id}_V(v))_{S_2} = v_{S_2}$.
(c) $C_{S_1,S_2} \circ C_{S_2,S_1} \circ v_{S_1} = C_{S_1,S_2} \circ v_{S_2} = v_{S_1}$ pour tout $v \in V$. Cela montre que $C_{S_1,S_2} \circ C_{S_2,S_1}$ est l'identité. Le même raisonnement marche avec les rôles de S_1 et S_2 inversés. □

Proposition 22.14. *Soient K un corps et V, W des K-espaces vectoriels de dimension finie, soient S_1, S_2 deux K-bases de V, soient T_1, T_2 deux K-bases de W, et soit $\varphi \in \mathrm{Hom}_K(V,W)$. Alors,*

$$M_{T_2,S_2}(\varphi) = C_{T_2,T_1} \circ M_{T_1,S_1}(\varphi) \circ C_{S_1,S_2}.$$

Démonstration. $C_{T_2,T_1} \circ M_{T_1,S_1}(\varphi) \circ C_{S_1,S_2} \circ v_{S_2} = C_{T_2,T_1} \circ M_{T_1,S_1}(\varphi) v_{S_1} = C_{T_2,T_1} \circ (\varphi(v))_{T_1} = (\varphi(v))_{T_2}$. □

Proposition 22.15. *Soient K un corps et V, W, Z des K-espaces vectoriels de dimension finie, soient S une K-base de V, T une K-base de W et U une K-base de Z. Soient $\varphi \in \mathrm{Hom}_K(V, W)$ et $\psi \in \mathrm{Hom}_K(W, Z)$. Alors,*

$$M_{U,T}(\psi) \circ M_{T,S}(\varphi) = M_{U,S}(\psi \circ \varphi).$$

En mots : le produit matriciel correspond à la composition d'applications.

Démonstration. $M_{U,T}(\psi) \circ M_{T,S}(\varphi) \circ v_S = M_{U,T}(\psi) \circ (\varphi(v))_T = (\psi(\phi(v)))_U = M_{U,T}(\psi \circ \varphi) \circ v_S$. □

Exercices en cours : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós 17/09/2015

(English version on the back.)

1. **Proposition.** *Le carré d'un entier relatif impair est* _____.

   Écrire une démonstration comme celle de la proposition 1.3 du cours. Noter que tout entier relatif impair est de la forme $2n+1$ pour un entier relatif n.

2. **Proposition.** *Il n'existe pas d'entiers relatifs* n, m *tels que*

$$14m + 21n = 50.$$

   Écrire une démonstration. Utiliser le principe de « démonstration par l'absurde » : supposer l'existence de tels entiers et trouver un entier relatif qui divise le côté gauche, mais pas le côté droit.

3. Écrire la négation des phrases suivantes.

   (a) Adrien parle français et allemand.

   (b) Ce triangle a deux côtés de même longueur.

4. Remplir les espaces ci-dessous avec l'un des symboles « $\Rightarrow$ », « $\Leftarrow$ » ou « $\Leftrightarrow$ » de manière à obtenir des assertions vraies. On ne demande pas ici de justifier vos réponses par écrit.

   Soient x, y des nombres réels.

   (a) $3x = 21$ _____ $x = 7$
   (b) $5x = 10$ _____ $x = 2$ ou $x = 1$
   (c) $8x = 4$ _____ $x = 2$ ou $x > 0$
   (d) $3x = 21$ _____ $x \neq 3$
   (e) $x^2 = 9$ _____ $x = -3$
   (f) $x - y = 1$ et $x + 2y = 10$ _____ $x = 4$ et $y = 3$
   (g) $y = x^2$ et $y^2 = 16$ _____ $x = 2$ et $y = 4$

5. Résoudre dans $\mathbb{Q}$ l'équation $2x(x+1)^2 = x^3 + 4x^2 + 2x + 8$. Utiliser « $\Rightarrow$ », « $\Leftarrow$ » et/ou « $\Leftrightarrow$ » !

6. Écrire les expressions suivantes sans utiliser les symboles $\sum$ et $\prod$.

$$\text{(a)} \sum_{i=-6}^{-4} i^2; \qquad \text{(b)} \sum_{i=-4}^{-6} i^2; \qquad \text{(c)} \prod_{k=0}^{n} x^{k-2}; \qquad \text{(d)} \prod_{m=1}^{n} m^2; \qquad \text{(e)} \sum_{i=1}^{n} \sum_{j=1}^{m} 1.$$

7. Écrire les expressions suivantes à l'aide des symboles $\sum$ et $\prod$.

   (a) $1 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot (2n-1)$;

   (b) $x^{11} + 2x^{17} + 4x^{23} + 8x^{29} + 16x^{35} + 32x^{41} + 64x^{47}$;

   (c) $a_1 + 2a_2 + 3a_3 + 3a_1^2 + 6a_2^2 + 9a_3^2 + 9a_1^3 + 18a_2^3 + 27a_3^3 + 27a_1^4 + 54a_2^4 + 81a_3^4$.

1. **Proposition.** *The square of an odd integer is* _____.

   Write a proof like the one of Proposition 1.3 of the lecture. Note that any odd integer is of the form $2n + 1$ with some integer n.

2. **Proposition.** *There are no integers n, m such that*

$$14m + 21n = 50.$$

   Write a proof. Use the principle of 'proof by contradiction': assume the existence of such integers and find an integer that divides the left hand side, but not the right hand side.

3. Write down the negation of the following sentences.

   (a) Adrian speaks French and German.

   (b) The lengths of two sides of this triangles are the same.

4. Fill in the blanks below with one of the symbols '$\Rightarrow$', '$\Leftarrow$' or '$\Leftrightarrow$' such that you obtain true assertions. You are not asked to justify your answers in writing.

   Let x, y be real numbers.

   (a) $3x = 21$ _____ $x = 7$
   (b) $5x = 10$ _____ $x = 2$ or $x = 1$
   (c) $8x = 4$ _____ $x = 2$ or $x > 0$
   (d) $3x = 21$ _____ $x \neq 3$
   (e) $x^2 = 9$ _____ $x = -3$
   (f) $x - y = 1$ and $x + 2y = 10$ _____ $x = 4$ and $y = 3$
   (g) $y = x^2$ and $y^2 = 16$ _____ $x = 2$ and $y = 4$

5. Solve the equation $2x(x + 1)^2 = x^3 + 4x^2 + 2x + 8$ in $\mathbb{Q}$. Use '$\Rightarrow$', '$\Leftarrow$' and/or '$\Leftrightarrow$'!

6. Write the following expressions without using the symbols $\sum$ and $\prod$.

$$\text{(a) } \sum_{i=-6}^{-4} i^2; \qquad \text{(b) } \sum_{i=-4}^{-6} i^2; \qquad \text{(c) } \prod_{k=0}^{n} x^{k-2}; \qquad \text{(d) } \prod_{m=1}^{n} m^2; \qquad \text{(e) } \sum_{i=1}^{n}\sum_{j=1}^{m} 1.$$

7. Write the following expressions using the symbols $\sum$ and $\prod$.

   (a) $1 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot (2n - 1)$;

   (b) $x^{11} + 2x^{17} + 4x^{23} + 8x^{29} + 16x^{35} + 32x^{41} + 64x^{47}$;

   (c) $a_1 + 2a_2 + 3a_3 + 3a_1^2 + 6a_2^2 + 9a_3^2 + 9a_1^3 + 18a_2^3 + 27a_3^3 + 27a_1^4 + 54a_2^4 + 81a_3^4$.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 1

16/09/2015

Les exercices sont à rendre le 23/09/2015 au début du cours.

(English version on p. 3.)

Vos solutions aux exercices vont être notées A (très bien), A/B (bien), B (moins bien), B/C, C (insuffisant). La note que vous obtenez pour vos exercices ainsi que pour vos résultats aux devoirs surveillés compte pour la note finale du cours : une moyenne de A compte 2 points sur 20, une moyenne de B 1 point et C 0 points. Par exemple, si vous avez eu une moyenne de B dans vos exercices et si vous obtenez un 13 dans l'examen, la note finale sera 14.

1. **Proposition.** *Soit n un entier impair. Alors $n^2 - 1$ est divisible par 8.*

   Écrire une démonstration.

2. **Proposition.** *Il n'existe pas d'entiers relatifs impairs n, m tels que*

$$m^2 - n^2 = 101.$$

   Écrire une démonstration. Utiliser le principe de « démonstration par l'absurde » ; la proposition précédente vous donne un diviseur du côté gauche qui donne une contradiction.

3. Soient a, b et c dans $\mathbb{Z}$.

   (a) Démontrer : si $c \mid a$ et $c \mid b$, alors $c \mid (a + b)$.

   (b) L'assertion réciproque est-elle vraie ? C'est-à-dire, est-ce que $c \mid (a + b)$ implique $c \mid a$ et $c \mid b$? Démontrer votre réponse.

   (c) Démontrer que les assertions suivantes sont équivalentes :

   (i) $c \mid a$

   (ii) $c \mid (a + bc)$

4. Dans une ferme, il y a des cochons. Chaque cochon est soit vieux, soit jeune (pas les deux en même temps). Chaque cochon est soit malade, soit en bonne santé (pas les deux en même temps). Chaque vieux cochon est vorace. Chaque cochon qui est en bonne santé est vorace. Dans la ferme, il y a des cochons voraces et il y a des cochons qui ne sont pas voraces.

   Parmi les assertions suivantes, lesquelles sont correctes ? Justifier (de façon concise !) vos réponses !

   (a) Il existe des jeunes cochons dans la ferme.

   (b) Il existe des vieux cochons dans la ferme.

   (c) Tous les cochons qui ne sont pas voraces sont jeunes.

   (d) Il existe des jeunes cochons malades.

   (e) Tous les jeunes cochons sont malades.

5. Lesquelles des égalités suivantes sont correctes ? Si une égalité est incorrecte, corriger le côté droit.

   (a) $\sum_{i=1}^{9} a_i = \sum_{j=3}^{11} a_{j-2}$;

   (b) $\sum_{i=1}^{n} a_{3i+1} = \sum_{j=-n+1}^{0} a_{4-3j}$;

   (c) $\sum_{i=0}^{n} \sum_{j=0}^{n} a_i b_j = \sum_{k=0}^{n} \sum_{\ell=0}^{k} a_\ell b_k + \sum_{k=0}^{n} \sum_{\ell=0}^{k} a_k b_\ell$.

6. (Cet exercice n'est pas à rendre.) Analyser la structure logique de phrases que vous lisez dans des journaux.

À propos.

Une vérité mathématique en elle-même n'est ni simple ni compliquée, elle est.
Émile Lemoine, mathématicien français (1840 – 1912)

Die Mathematiker sind eine Art Franzosen: Redet man zu ihnen, so übersetzen sie es in ihre Sprache, und dann ist es alsbald ganz etwas anderes.
Johan Wolfgang von Goethe (1749 – 1832)

Your solutions to the exercises will be marked A (very good), A/B (good), B (less good), B/C, C (insufficient). The mark that you obtain for your exercises and for the supervised coursework count for the final mark of the course: an average of A counts 2 points of 20, an average of B counts 1 point, and C 0 points. For example, if you have an average of B in the exercises and if you obtain 13 in the exam, the final mark will be 14.

1. **Proposition.** *Let n be an odd integer. Then $n^2 - 1$ is divisible by 8.*

   Write a proof.

2. **Proposition.** *There are no odd integers n, m such that*

   $$m^2 - n^2 = 101.$$

   Write a proof. Use the principle of 'proof by contradiction'; the preceding proposition gives you a divisor of the left hand side which leads to a contradiction.

3. Let a, b and c in $\mathbb{Z}$.

   (a) Prove: if $c \mid a$ and $c \mid b$, then $c \mid (a + b)$.

   (b) Is the converse assertion true? That is, does $c \mid (a + b)$ imply $c \mid a$ and $c \mid b$?
   Prove your answer.

   (c) Show that the following two assertions are equivalent:

   (i) $c \mid a$

   (ii) $c \mid (a + bc)$

4. In a farm there are pigs. Every pig is either old or young (not both). Every pig is either ill or in good health (not both). Every old pig is greedy. Every pig that is in good health is greedy. In the farm there are pigs that are greedy and there are pigs that are not greedy.

   Which of the following assertions are correct? Justify your answers (in a concise way)!

   (a) There is a young pig in the farm.

   (b) There is an old pig in the farm.

   (c) All pigs that are not greedy are young.

   (d) There is an ill young pig.

   (e) All young pigs are ill.

5. Which of the following equalities are correct? If an inequality is incorrect, then correct the right hand side.

   (a) $\sum_{i=1}^{9} a_i = \sum_{j=3}^{11} a_{j-2}$;

   (b) $\sum_{i=1}^{n} a_{3i+1} = \sum_{j=-n+1}^{0} a_{4-3j}$;

   (c) $\sum_{i=0}^{n} \sum_{j=0}^{n} a_i b_j = \sum_{k=0}^{n} \sum_{\ell=0}^{k} a_\ell b_k + \sum_{k=0}^{n} \sum_{\ell=0}^{k} a_k b_\ell$.

6. (This exercise is not to be handed in.) Analyse the logical structure of sentences that you read in newspapers.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 2

23/09/2015

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au dévoir surveillé qui aura lieu le 28/09/2015.

(English version on p. 3.)

1. Soit $a \in \mathbb{Q}$. Démontrer par récurrence

$$(1-a) \cdot \sum_{i=0}^{n} a^i = 1 - a^{n+1}$$

pour tout $n \in \mathbb{N}$.

2. (a) Soit p un nombre premier différent de 3. Démontrer : $3 \mid (p-1)$ ou $3 \mid (p+1)$.

   (b) Soient $a, b \in \mathbb{Z}$ tels que $3 \mid (a-1)$ et $3 \mid (b-1)$. Utiliser l'égalité

$$ab - 1 = (a-1)b + (b-1)$$

   pour démontrer $3 \mid (ab-1)$.

   (c) Soient $p_1, p_2, \ldots, p_n$ des nombres premiers tels que pour tout $i = 1, \ldots, n$ on a : $3 \mid (p_i - 1)$. En utilisant (b), démontrer par récurrence : $3 \mid \big((\prod_{i=1}^{n} p_i) - 1\big)$.

   (d) Soient $a, b \in \mathbb{Z}$ tels que $3 \mid (a+1)$ et $3 \mid (b+1)$. Utiliser l'égalité

$$ab - 1 = (a+1)b - (b+1)$$

   pour démontrer : $3 \mid (ab-1)$.

   (e) Soient $a, b \in \mathbb{Z}$ tels que $3 \mid (a-1)$ et $3 \mid (b+1)$. Démontrer : $3 \mid (ab+1)$.

   (f) Soient $p_1, p_2, \ldots, p_n$ des nombres premiers tels que pour tout $i = 1, \ldots, n$ on a : $3 \mid (p_i + 1)$. Démontrer par récurrence : $3 \mid \big((\prod_{i=1}^{n} p_i) - (-1)^n\big)$.

   (g) Démontrer qu'il existe une infinité de nombres premiers p tels que $3 \mid (p+1)$.
   Indication. Généraliser la démonstration du théorème sur l'infinité des nombres premiers par Euclide : supposer que $p_1 = 2, p_2 = 5, p_3 = 11, p_4, \ldots, p_n$ sont les seuls nombres premiers ayant la propriété demandée ; considérer

$$m := \big(\prod_{i=1}^{n} p_i\big) + \begin{cases} 3 & \text{si } n \text{ est impair,} \\ 1 & \text{si } n \text{ est pair ;} \end{cases}$$

   montrer $3 \nmid m$ et $p_i \nmid m$ pour tout $i = 1, \ldots, n$; conclure que m doit être divisible par un nombre premier p différent de $3, p_1, p_2, \ldots, p_n$ tel que $3 \mid (p+1)$.

3. Écrire la négation des assertions suivantes :

   (a) Tous les étudiants de ce cours sont Luxembourgeois.

   (b) Il existe des triangles ayant exactement deux angles droits.

4. Soit A la matrice $\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & a_{2,3} & \dots & a_{2,m} \\ a_{3,1} & a_{3,2} & a_{3,3} & \dots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \dots & a_{n,m} \end{pmatrix}$ avec $n = 4$, $m = 6$ et les $a_{i,j}$ donnés par la formule $a_{i,j} = \delta_{i,j+1}$, où $\delta_{x,y}$ est le symbole de Kronecker (voir le cours). Écrire la matrice A.

À propos. Pour illustrer qu'une assertion fausse comme $0 = 1$ implique tout, on dit qu'Einstein a donné l'exemple suivant : « Si $0 = 1$, alors $1 = 2$. Le pape et moi, ce sont deux personnes. Mais, puisque $1 = 2$, c'est la même personne, ce qui implique que je suis le pape. »

1. Let $a \in \mathbb{Q}$. Prove by induction
$$(1-a) \cdot \sum_{i=0}^{n} a^i = 1 - a^{n+1}$$
for all $n \in \mathbb{N}$.

2. (a) Let p be a prime number different from 3. Prove: $3 \mid (p-1)$ or $3 \mid (p+1)$.

   (b) Let $a, b \in \mathbb{Z}$ such that $3 \mid (a-1)$ and $3 \mid (b-1)$. Use the equality
   $$ab - 1 = (a-1)b + (b-1)$$
   for proving $3 \mid (ab-1)$.

   (c) Let $p_1, p_2, \ldots, p_n$ be prime numbers such that for all $i = 1, \ldots, n$ one has: $3 \mid (p_i - 1)$. Using (b), prove by induction: $3 \mid \big((\prod_{i=1}^{n} p_i) - 1\big)$.

   (d) Let $a, b \in \mathbb{Z}$ such that $3 \mid (a+1)$ and $3 \mid (b+1)$. Use the equality
   $$ab - 1 = (a+1)b - (b+1)$$
   for proving: $3 \mid (ab-1)$.

   (e) Let $a, b \in \mathbb{Z}$ such that $3 \mid (a-1)$ and $3 \mid (b+1)$. Prove: $3 \mid (ab+1)$.

   (f) Let $p_1, p_2, \ldots, p_n$ be prime number such that for all $i = 1, \ldots, n$ one has: $3 \mid (p_i + 1)$. Prove by induction: $3 \mid \big((\prod_{i=1}^{n} p_i) - (-1)^n\big)$.

   (g) Prove that there are infinitely many prime numbers p such that $3 \mid (p+1)$.
   Hint. Generalise the prove of the theorem on the infinitness of the set of prime numbers by Euclid: suppose that $p_1 = 2, p_2 = 5, p_3 = 11, p_4, \ldots, p_n$ are the only prime numbers having the demanded property; consider:
   $$m := \big(\prod_{i=1}^{n} p_i\big) + \begin{cases} 3 & \text{if } n \text{ is odd,} \\ 1 & \text{if } n \text{ is even;} \end{cases}$$
   prove $3 \nmid m$ and $p_i \nmid m$ for all $i = 1, \ldots, n$; conclude that m is divisible by a prime number p different from $3, p_1, p_2, \ldots, p_n$ such that $3 \mid (p+1)$.

3. Write down the negation of the following assertions:

   (a) All students in this lecture are luxembourgish.

   (b) There are triangles having exactly two right angles.

4. Let A be the matrix $\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \ldots & a_{1,m} \\ a_{2,1} & a_{2,2} & a_{2,3} & \ldots & a_{2,m} \\ a_{3,1} & a_{3,2} & a_{3,3} & \ldots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \ldots & a_{n,m} \end{pmatrix}$ with $n = 4$, $m = 6$ and the $a_{i,j}$ are given by the formula $a_{i,j} = \delta_{i,j+1}$, where $\delta_{x,y}$ is the Kronecker symbol (see the lecture). Write the matrix A.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 3

28/09/2015

Les exercices sont à rendre le 12/10/2015 au début du cours.

(English version on p. 3.)

1. Soient A, B et C des assertions. Écrire des tables de vérité ou utiliser le théorème 2.3 pour vérifier les assertions suivantes:

   (a) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$;

   (b) $(A \Leftrightarrow B) = (\neg A \wedge \neg B) \vee (A \wedge B)$;

   (c) $\neg\big(\neg A \wedge (B \vee A)\big) = A \vee \neg B$;

   (d) $\neg\big((A \vee B) \wedge (B \wedge A)\big) = \neg A \vee \neg B$;

   (e) $\neg\big(A \wedge (\neg(B \vee C))\big) \wedge (A \vee B) = B \vee (A \wedge C)$.

2. Dire si les assertions suivantes sont vraies ou fausses et démontrer votre réponse :

   (a) $\forall\, x \in \mathbb{N} : \exists\, y \in \mathbb{N} : x = y$;

   (b) $\exists\, y \in \mathbb{N} : \forall\, x \in \mathbb{N} : x = y$;

   (c) $\forall\, x \in \mathbb{N} : \exists\, y \in \mathbb{Z} : x > y$;

   (d) $\exists\, y \in \mathbb{Z} : \forall\, x \in \mathbb{N} : x \geq y$.

3. (a) Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction et $x_0 \in \mathbb{R}$. Écrire la négation de l'assertion suivante:
   $\forall\, \epsilon > 0 : \exists\, \delta > 0 : \forall\, x \in \mathbb{R} : \big(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon\big)$
   Dans votre cours d'Analyse 1 vous verrez que ceci est la définition de la continuité de la fonction f au point x_0.

   (b) On définit le "ou exclusif" (XOR) par la table de vérité:

A	B	A XOR B
v	v	f
v	f	v
f	v	v
f	f	f

   Exprimer XOR en utilisant seulement $\wedge$, $\vee$ et $\neg$. Démontrer votre réponse par une table de vérité.

4. (a) Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. Démontrer: $g \circ f$ est surjectif $\Rightarrow$ g est surjectif.
   [Comme nous avons l'assertion: "$g \circ f$ est injectif $\Rightarrow$ f est injectif", nous pouvons déduire l'assertion: "$g \circ f$ est bijectif $\Rightarrow$ f est injectif et g est surjectif".

   (b) Soient A et B des ensembles et f une application de A dans B. Démontrer:
   f est bijectif si et seulement s'il existe une application g de B dans A vérifiant: $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$.

5. Soient E et F des ensembles et f une application de E dans F. Soient A et B des parties de E. Démontrer:

   (a) $A \subseteq f^{-1}(f(A))$. Attention, on n'a pas toujours égalité ici; donner un contre-exemple.

   (b) $A \subseteq B \Rightarrow f(A) \subseteq f(B)$;

   (c) $f(A \cup B) = f(A) \cup f(B)$;

   (d) $f(A \cap B) \subseteq f(A) \cap f(B)$. Attention, on n'a pas toujours égalité ici; donner un contre-exemple.

6. Soit E un ensemble à n éléments. L'objectif de cette question est de démontrer: $\#\mathcal{P}(E) = 2^n$ où $\mathcal{P}(E)$ est l'ensemble des parties de E. Par exemple, pour $E = \{1, 2, 3\}$ on a
   $\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

   (a) Vérifier le résultat pour n égal à 0, 1, 2 et 3.

   (b) On suppose n supérieur ou égal à 1. On fixe un élément x dans E et on note $\mathcal{P}_x$ l'ensemble des parties de E qui contiennent x, $\mathcal{Q}_x$ l'ensemble des parties de E qui ne contiennent pas x.
   Démontrer $\mathcal{P}(E) = \mathcal{P}_x \sqcup \mathcal{Q}_x$, puis que $\mathcal{P}_x$ et $\mathcal{Q}_x$ ont même cardinal, égal à celui de $\mathcal{P}(E \setminus \{x\})$.
   Indication: donner une bijection entre $\mathcal{P}_x$ et $\mathcal{P}(E \setminus \{x\})$ et une bijection entre $\mathcal{Q}_x$ et $\mathcal{P}(E \setminus \{x\})$.

   (c) Démontrer par récurrence sur n qu'on a $\#\mathcal{P}(E) = 2^n$.

7. Donner une bijection $[0, 1] \to [0, 1)$.

À propos. L'hôtel de Hilbert à Göttingen possède un nombre infini de chambres. Aujourd'hui, toutes les chambres sont occupées. Malgré cela, l'hôtelier Hilbert peut toujours accueillir un nouveau client.

En effet, supposons que les chambres sont numérotées par tous les nombres entiers (à partir de 1). Il suffit que l'hôtelier demande à l'occupant de la première chambre de s'installer dans la seconde, à celui de la seconde de s'installer dans la troisième, et ainsi de suite. Les clients déjà logés le restent. La première chambre est libre et peut accueillir le nouveau client.

Mais l'hôtelier peut aussi accueillir une infinité de nouveaux clients. Pour ce faire, il faut que le client occupant la chambre numéro 1 prenne la chambre numéro 2, l'occupant de la numéro 2 la numéro 4, celui de la numéro 3 la numéro 6, et ainsi de suite. Chacun occupe une chambre de numéro double de celui de sa chambre précédente, de telle sorte que toutes les chambres de numéro impair deviennent libres. Et puisqu'il existe une infinité de nombres impairs, l'hôtelier peut accueillir une infinité de nouveaux clients.

(Adapté et corrigé de: `http://fr.wikipedia.org/wiki/Hôtel_de_Hilbert`)

1. Let A, B and C be assertions. Write truth tables or by using Theorem 2.3 in order to prove:

   (a) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$;

   (b) $(A \Leftrightarrow B) = (\neg A \wedge \neg B) \vee (A \wedge B)$;

   (c) $\neg\big(\neg A \wedge (B \vee A)\big) = A \vee \neg B$;

   (d) $\neg\big((A \vee B) \wedge (B \wedge A)\big) = \neg A \vee \neg B$;

   (e) $\neg\big(A \wedge (\neg(B \vee C))\big) \wedge (A \vee B) = B \vee (A \wedge C)$.

2. State if the following assertions are true or false and prove your answer:

   (a) $\forall\, x \in \mathbb{N} : \exists\, y \in \mathbb{N} : x = y$;

   (b) $\exists\, y \in \mathbb{N} : \forall\, x \in \mathbb{N} : x = y$;

   (c) $\forall\, x \in \mathbb{N} : \exists\, y \in \mathbb{Z} : x > y$;

   (d) $\exists\, y \in \mathbb{Z} : \forall\, x \in \mathbb{N} : x \geq y$.

3. (a) Let $f : \mathbb{R} \to \mathbb{R}$ be a function and $x_0 \in \mathbb{R}$. Write down the negation of the following assertion:
   $\forall\, \epsilon > 0 : \exists\, \delta > 0 : \forall\, x \in \mathbb{R} : \big(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon\big)$
   In your lecture Analyse 1 you are going to see that this is the definition of continuity of the function f in the point x_0.

   (b) One defines the 'exclusive OR' (XOR) by the truth table:

A	B	A XOR B
t	t	f
t	f	t
f	t	t
f	f	f

   (t=true, f=false)
   Express XOR only with $\wedge$, $\vee$ and $\neg$. Prove your answer by using a truth table.

4. (a) Let A, B, C be sets and $f : A \to B$ and $g : B \to C$ be maps. Prove:
   $g \circ f$ is surjective $\Rightarrow$ g is surjective.
   [Since we have seen the assertion: "$g \circ f$ is injective $\Rightarrow$ f is injective", we can derive the assertion: "$g \circ f$ is bijective $\Rightarrow$ f is injective and g is surjective".

   (b) Let A and B be sets and f be a map from A to B. Prove:
   f is bijective if and only if there exists a map g from B to A such that: $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

5. Let E and F be sets and f a map from E to F. Let A and B be subsets of E. Prove:

   (a) $A \subseteq f^{-1}\,(f(A))$. Attention, one does not always have equality here; give a counter example.

   (b) $A \subseteq B \Rightarrow f(A) \subseteq f(B)$;

   (c) $f\,(A \cup B) = f(A) \cup f(B)$;

   (d) $f\,(A \cap B) \subseteq f(A) \cap f(B)$. Attention, one does not always have equality here; give a counter example.

6. Let E be a set with n elements. The goal of this question is to show: $\#\mathcal{P}(E) = 2^n$ where $\mathcal{P}(E)$ is the set of all subsets of E. For example, for $E = \{1, 2, 3\}$ we have
$\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

   (a) Verify the result for n equal to 0, 1, 2 and 3.

   (b) We suppose that n is at least 1 and we fix un element x in E and denote by $\mathcal{P}_x$ the set of all subsets of E which contain x, and by $\mathcal{Q}_x$ the set of all subsets of E which do not contain x.
   Prove first $\mathcal{P}(E) = \mathcal{P}_x \sqcup \mathcal{Q}_x$, and then that $\mathcal{P}_x$ and $\mathcal{Q}_x$ have the same cardinality, equal to the cardinality of $\mathcal{P}(E \setminus \{x\})$.
   Hint: give a bijection between $\mathcal{P}_x$ and $\mathcal{P}(E \setminus \{x\})$ and a bijection between $\mathcal{Q}_x$ and $\mathcal{P}(E \setminus \{x\})$.

   (c) Show by induction on n that one has $\#\mathcal{P}(E) = 2^n$.

7. Exhibit a bijection $[0, 1] \to [0, 1)$.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 4

12/10/2015

Les exercices sont à rendre le 19/10/2015 au début du cours.

(English translation on page 3)

1. (a) On considère sur $\mathbb{R}$ la relation binaire $<$ définie par : pour tout (x, y) dans $\mathbb{R}^2$, $x < y$ si et seulement si x est strictement plus petit que y. Cette relation est-elle réflexive ? Symétrique ? Antisymétrique ? Transitive ? Totale ? Est-ce une relation d'ordre ?

   (b) Soit E l'ensemble des nombres premiers différents de 2. On définit sur E une relation binaire R par :

   $$\forall (x, y) \in E \times E,\ x \sim_R y \iff \frac{x+y}{2} \in E.$$

   (i) Donner un exemple de couple (x, y) tel que x et y sont en relation, puis un exemple de couple (x, y) tel que x et y ne sont pas en relation.

   (ii) La relation R est-elle une relation d'équivalence ?

2. Soit n un entier naturel ; on définit sur $\mathbb{Z}$ une relation binaire R_n par :

   $$\forall\, (a, b) \in \mathbb{Z}^2 :\ a \sim_{R_n} b \iff n|(a-b).$$

   (a) Démontrer que R_n est une relation d'équivalence sur $\mathbb{Z}$.
   On l'appelle la « congruence modulo n ». Lorsque a et b sont en relation pour R_n, on note

   $$a \equiv b \mod n$$

   et on dit que *a et b sont congrus modulo n*.

   (b) Donner la classe d'équivalence d'un entier relatif a pour la relation R_n avec $n \in \mathbb{N}_{\geq 2}$. Même question pour R_0 et R_1.

3. Soient $(N, S, 0)$ et $(N', S', 0')$ deux systèmes des nombres naturels. Démontrer qu'il existe une bijection $\varphi : N \to N'$ telle que $\varphi(0) = 0'$ et $\varphi \circ S = S' \circ \varphi$.

   Indication. Définir l'application φ récursivement. Pour montrer la bijectivité, définir une application $\varphi' : N' \to N$ récursivement. Noter que l'identité donne une application $\mathrm{id}_N : N \to N$ telle que $S \circ \mathrm{id}_N = \mathrm{id}_N \circ S$; utiliser l'unicité dans la définition récursive pour obtenir $\varphi' \circ \varphi = \mathrm{id}_N$; ne pas oublier de montrer aussi $\varphi \circ \varphi' = \mathrm{id}_{N'}$.

4. Soit $(N, S, 0)$ un système des nombres naturels.

   (a) Démontrer : pour tout n dans N, on a $n \neq S(n)$.

   (b) Démontrer l'associativité de l'addition définie en cours. C'est-à-dire, démontrer que, pour tous m, n et ℓ dans N, on a : $(m + n) + \ell = m + (n + \ell)$.

Tourner la page, s.v.p.

5. Donner soit une démonstration soit un contrexemple à chacune des deux assertions suivantes :

   (a) Soient E et F des ensembles et $\mathcal{P}(E)$ (respectivement $\mathcal{P}(F)$) l'ensemble de toutes les parties de E (respectivement de F). Alors $\mathcal{P}(E \cap F) = \mathcal{P}(E) \cap \mathcal{P}(F)$;

   (b) Soient E, F etc. comme dans (a). Alors $\mathcal{P}(E \cup F) = \mathcal{P}(E) \cup \mathcal{P}(F)$.

   (c) Il existe une relation d'ordre totale sur $\mathbb{Q} \times \mathbb{Q}$ telle que pour tout $x, x_1, x_2, y, y_1, y_2 \in \mathbb{Q}$ on a :

$$x_1 \leq x_2 \Rightarrow (x_1, y) \preceq (x_2, y) \ \wedge \ y_1 \leq y_2 \Rightarrow (x, y_1) \preceq (x, y_2).$$

À propos.

Charles a un méchant prof qui lui dit : « Au cours d'une des six prochaines heures, je vais faire une « interrogation surprise » ». Charles se dit que le prof n'a pas bien réfléchi, parce qu'il est impossible de faire une telle « interrogation surprise ». Voici son argumentation :

Si l'interrogation n'a pas eu lieu pendant les cinq premières heures, alors, forcément, elle sera faite la sixième heure ; ça ne sera pas une surprise ! Alors, forcément, l'interrogation doit être faite pendant une des cinq premières heures.

Si l'interrogation n'a pas eu lieu pendant les quatre premières heures, alors, forcément, elle sera faite la cinquième heure ; ça ne sera pas une surprise ! Alors, forcément, l'interrogation doit être faite pendant une des quatre premières heures.

Continuant ainsi, l'interrogation doit forcément avoir lieu la première heure, ce qui ne serait pas une surprise non plus. Alors, il est effectivement impossible de faire une telle « interrogation surprise ».

La deuxième heure, le prof fait l'interrogation. Charles est très surpris et la rate complètement.

Comment est-ce possible ?

1. (a) Consider the binary relation $<$ on $\mathbb{R}$ defined by : for all (x, y) in $\mathbb{R}^2$, $x < y$ if and only if x is strictly smaller than y. Is this relation reflexive ? Symmetric ? Antisymmetric ? Transitive ? Total ? Is it an order relation ?

   (b) Let E be the set of prime numbers different from 2. On E we define the binary relation R by :

$$\forall (x, y) \in E \times E,\ x \sim_R y \iff \frac{x+y}{2} \in E.$$

   (i) Give an example of a pair (x, y) such that x and y are in relation, and an example of a pair (x, y) such that x and y are not in relation.

   (ii) Is the relation R an equivalence relation ?

2. Let n be a natural number ; on $\mathbb{Z}$ one defines a binary relation R_n by :

$$\forall\, (a, b) \in \mathbb{Z}^2 :\ a \sim_{R_n} b \iff n|(a-b).$$

   (a) Show that R_n is an equivalence relation on $\mathbb{Z}$.

   One calls it « congruence modulo n ». If a and b are related for R_n, one writes

$$a \equiv b \mod n$$

   and one says that *a and b are congruent modulo n*.

   (b) Exhibit the equivalence class of an integer a for the relation R_n with $n \in \mathbb{N}_{\geq 2}$. Same question for R_0 et R_1.

3. Let $(N, S, 0)$ and $(N', S', 0')$ be two systems of natural numbers.

   Prove that there is a bijection $\varphi : N \to N'$ such that $\varphi(0) = 0'$ and $\varphi \circ S = S' \circ \varphi$.

   Hint : Define the map φ recursively. In order to prove the bijectivity, define a map $\varphi' : N' \to N$ recursively. Note that the identity gives a map $\mathrm{id}_N : N \to N$ such that $S \circ \mathrm{id}_N = \mathrm{id}_N \circ S$; use the uniqueness in the recursive definition in order to obtain $\varphi' \circ \varphi = \mathrm{id}_N$; do not forget to also prove $\varphi \circ \varphi' = \mathrm{id}_{N'}$.

4. Let $(N, S, 0)$ be a system of natural numbers.

   (a) Show that for all n in N, one has $n \neq S(n)$.

   (b) Prove the associativity of the addition defined in the lecture. That is, show that for all m, n and ℓ in N, one has : $(m + n) + \ell = m + (n + \ell)$.

5. Either give a proof or a counterexample for each of the following assertions :

   (a) Let E and F be sets and $\mathcal{P}(E)$ (respectively, $\mathcal{P}(F)$) the set of all subsets of E (respectively, of F). Then $\mathcal{P}(E \cap F) = \mathcal{P}(E) \cap \mathcal{P}(F)$;

   (b) Let E, F etc. be as in (a). Then $\mathcal{P}(E \cup F) = \mathcal{P}(E) \cup \mathcal{P}(F)$.

   (c) There is a total order relation on $\mathbb{Q} \times \mathbb{Q}$ such that for all $x, x_1, x_2, y, y_1, y_2 \in \mathbb{Q}$ one has :

$$x_1 \leq x_2 \Rightarrow (x_1, y) \preceq (x_2, y)\ \wedge\ y_1 \leq y_2 \Rightarrow (x, y_1) \preceq (x, y_2).$$

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 5

19/10/2015

Les exercices sont à rendre le 26/10/2015 au début du cours.

(English translation on page 3)

1. Soient E, F deux ensembles finis. Démontrer :
   $\#F \leq \#E \Leftrightarrow$ il existe une surjection de E dans F.
2. Soit S_4 le groupe symétrique en $\{1, 2, 3, 4\}$. Dresser la liste de ses éléments. Utiliser l'écriture en cycles.
3. (a) Faire les calculs suivants dans le groupe S_{10} :
   (1) $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 7 & 4 & 10 & 9\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\end{pmatrix} = ?$
   (2) $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 7 & 4 & 10 & 9\end{pmatrix} = ?$
   (3) $\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}5 & 6\end{pmatrix}\begin{pmatrix}7 & 8\end{pmatrix}\begin{pmatrix}9 & 10\end{pmatrix} \circ \begin{pmatrix}1 & 10\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}4 & 5\end{pmatrix}\begin{pmatrix}6 & 7\end{pmatrix}\begin{pmatrix}8 & 9\end{pmatrix} = ?$

   (b) Trouver les inverses dans le groupe S_{10} des éléments suivants :
   (1) $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\end{pmatrix}$,
   (2) $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 7 & 4 & 10 & 9\end{pmatrix}$,
   (3) $\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}5 & 6\end{pmatrix}\begin{pmatrix}7 & 8\end{pmatrix}\begin{pmatrix}9 & 10\end{pmatrix}$.
4. Soit $(G, *, e)$ un groupe. On note l'inverse de $a \in G$ par a^{-1}.
   (a) On suppose que $(a*b)^{-1} = a^{-1}*b^{-1}$ pour tout $a, b \in G$. Démontrer que G est un groupe abélien.
   (b) On suppose que $a^2 * b^2 = (a*b)^2$ pour tout $a, b \in G$. Démontrer que G est un groupe abélien.
   (c) Supposons que $a^2 = e$ pour tout $a \in G$. Démontrer que G est un groupe abélien.
   Indication. Vous pouvez utiliser (b).
   (d) Démontrer que tout groupe de cardinal 4 est abélien.
5. Soit $n \in \mathbb{N}_{\geq 2}$ et soit $(a_1 \ \ a_2 \ \ \cdots \ \ a_r)$ un cycle dans S_n.
   (a) Démontrer que ce cycle peut être écrit en utilisant (plusieurs fois, si nécessaire) les 2-cycles (transpositions) $(1 \ \ 2), (1 \ \ 3), \ldots, (1 \ \ n)$.
   (b) Démontrer que ce cycle peut être écrit en utilisant (plusieurs fois, si nécessaire) les 2-cycles (transpositions) $(1 \ \ 2), (2 \ \ 3), \ldots, (n-1 \ \ n)$.
   (c) Démontrer que ce cycle peut aussi être écrit en utilisant (plusieurs fois, si nécessaire) le n-cycle $(1 \ \ 2 \ \ \cdots \ \ n)$ et le 2-cycle $(1 \ \ 2)$.

À propos. *L'argument de la diagonale de Cantor.*

On souhaite démontrer que l'ensemble $\mathbb{R}$ n'est pas dénombrable. En fait, nous allons démontrer que l'ensemble $[0, 1]$ n'est pas dénombrable (ce qui implique que $\mathbb{R}$ ne l'est pas non plus).

On raisonne par l'absurde en supposant que $[0, 1]$ est dénombrable, énuméré à l'aide d'une suite $r = (r_1, r_2, r_3, \dots)$. Chaque terme de cette suite a une écriture décimale avec une infinité de chiffres après la virgule, soit :

$$r_i = 0, r_{i,1} r_{i,2}, r_{i,3} \dots$$

On construit maintenant un nombre réel x dans $[0, 1]$ en considérant le n-ième chiffre après la virgule de r_n. Le nombre réel x est construit par la donnée de ses décimales suivant la règle : si la n-ième décimale de r_n est différente de 1, alors la n-ième décimale de x est 1, sinon la n-ième est 2.

Le nombre x est clairement dans l'intervalle $[0, 1]$ mais ne peut pas être dans la suite $(r_1, r_2, r_3, \dots)$, car il n'est égal à aucun des nombres de la suite : il ne peut pas être égal à r_1 car la première décimale de x est différente de celle de r_1, de même pour r_2 en considérant la deuxième décimale, etc.

On obtient une contradiction et on en déduit que $[0, 1]$ n'est pas dénombrable.

(Adapté de : `fr.wikipedia.org/wiki/Argument_de_la_diagonale_de_Cantor`)

1. Let E and F be finite sets. Prove:
   $\#F \leq \#E \Leftrightarrow$ there is a sujrective map from E to F.
2. Let S_4 be the symmetric group on $\{1, 2, 3, 4\}$. List its elements. Use the the cycle notation.
3. (a) Make the following calculations in the group S_{10}:
   (1) $\big(1\ \ 3\big)\ \big(2\ \ 7\ \ 4\ \ 10\ \ 9\big) \circ \big(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10\big) = ?$
   (2) $\big(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10\big) \circ \big(1\ \ 3\big)\ \big(2\ \ 7\ \ 4\ \ 10\ \ 9\big) = ?$
   (3) $\big(1\ \ 2\big)\ \big(3\ \ 4\big)\ \big(5\ \ 6\big)\ \big(7\ \ 8\big)\ \big(9\ \ 10\big) \circ \big(1\ \ 10\big)\ \big(2\ \ 3\big)\ \big(4\ \ 5\big)\ \big(6\ \ 7\big)\ \big(8\ \ 9\big) = ?$

   (b) Find the inverses in the group S_{10} of the following elements:
   (1) $\big(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10\big)$,
   (2) $\big(1\ \ 3\big)\ \big(2\ \ 7\ \ 4\ \ 10\ \ 9\big)$,
   (3) $\big(1\ \ 2\big)\ \big(3\ \ 4\big)\ \big(5\ \ 6\big)\ \big(7\ \ 8\big)\ \big(9\ \ 10\big)$.
4. Let $(G, *, e)$ be a group. Denote the inverse of $a \in G$ by a^{-1}.

   (a) Suppose that $(a * b)^{-1} = a^{-1} * b^{-1}$ for all $a, b \in G$. Show that G is an abelian group.

   (b) Suppose that $a^2 * b^2 = (a * b)^2$ for all $a, b \in G$. Show that G is an abelian group.

   (c) Suppose that $a^2 = e$ for all $a \in G$. Show that G is an abelian group.
   Hint. You can use (b).

   (d) Prove that every group of cardinality 4 is abelian.
5. Let $n \in \mathbb{N}_{\geq 2}$ and let $(a_1\ \ a_2\ \ \cdots\ \ a_r)$ be a cycle in S_n.

   (a) Prove that this cycle can be written using (several times, if necessary) the 2-cycles (transpositions) $(1\ \ 2), (1\ \ 3), \ldots, (1\ \ n)$.

   (b) Prove that this cycle can also be written using (several times, if necessary) the 2-cycles (transpositions) $(1\ \ 2), (2\ \ 3), \ldots, (n-1\ \ n)$.

   (c) Prove that this cycle can also be written using (several times, if necessary) the n-cycle $(1\ \ 2\ \ \cdots\ \ n)$ and the 2-cycle $(1\ \ 2)$.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 6

26/10/2015

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au dévoir surveillé qui aura lieu le 05/11/2015.

(English translation on page 3.)

1. Sur $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ on définit la relation binaire :

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

   Démontrer que c'est une relation d'équivalence.

   Remarque : En fait, l'ensemble quotient est par définition $\mathbb{Q}$, l'ensemble des *nombres rationnels* : la classe de (a, x) est formée de tous les (b, y) tel que $ay = bx$, ce qui justifie la notation $\frac{a}{x}$ pour la classe $\overline{(a, x)}$.

2. Soient E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble des parties de E. Nous définissons sur $\mathcal{P}(E)$ une relation binaire $\supsetneq$ par : pour A et B dans $\mathcal{P}(E)$

$$A \sim_R B \iff A \supsetneq B \quad (\text{c'est-à-dire } A \supseteq B \text{ et } A \neq B).$$

   Lesquelles des propriétés suivantes sont satisfaites par R (justifier votre réponse) ?

   (1) Réflexivité ; (2) symétrie ; (3) antisymétrie ; (4) transitivité ; (5) totalité. (6) Est-ce une relation d'ordre ? (7) Est-ce une relation d'équivalence ?

3. Soient C et D des parties de F. Démontrer :

   (1) $f\left(f^{-1}(C)\right) \subseteq C$. Attention, on n'a pas toujours égalité ici ; donner un contre-exemple.

   (2) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

4. (a) *(Involution)* Soient E un ensemble et f une application de E dans E vérifiant : $f \circ f = \mathrm{id}_E$. Démontrer que f est bijectif. Quel est son inverse ?

   (b) Soient E, F, G des ensembles et $f : E \to F$, $g : F \to G$ des applications. Démontrer que si f et g sont injectifs, alors $g \circ f$ est injectif.

   (c) Si A, B sont des ensembles, on note $\mathcal{F}(A, B)$ l'ensemble de toutes les applications $A \to B$. Soient E, F et G des ensembles.

   (1) Soit f une application injective de F dans G. Démontrer :

$$\forall (g, h) \in \mathcal{F}(E, F), (f \circ g = f \circ h \Longrightarrow g = h).$$

   En d'autres termes, on démontre que l'application

$$\begin{array}{ccc} \mathcal{F}(E, F) & \longrightarrow & \mathcal{F}(E, G) \\ g & \longmapsto & f \circ g \end{array}$$

   est injective.

(2) Soit f une application surjective de E dans F. Démontrer :

$$\forall (g,h) \in \mathcal{F}(F,G), (g \circ f = h \circ f \Longrightarrow g = h).$$

En d'autres termes, on démontre que l'application

$$\begin{array}{ccc} \mathcal{F}(F,G) & \longrightarrow & \mathcal{F}(E,G) \\ g & \longmapsto & g \circ f \end{array}$$

est injective.

5. Démontrer la variante suivante de récurrence.

   Soit $A(n)$ une assertion qui dépend de $n \in \mathbb{N}$. Supposons que $A(0)$ soit vrai. Pour tout $n \in \mathbb{N}$, supposons aussi vrai l'assertion $(\forall\, m \leq n : A(m)) \Rightarrow A(n+1)$.

   Démontrer : $A(n)$ est vrai pour tout $n \in \mathbb{N}$.

   Indication : utiliser que $\mathbb{N}$ *est bien ordonné, c'est-à-dire que toute partie non-vide de* $\mathbb{N}$ *possède un plus petit élément.*

6. Est-ce qu'il existe une bijection entre $\mathbb{R}$ et $\mathbb{R} \times \mathbb{R}$? Si oui, en donner une ; si non, le démontrer.

7. Soit $(G, \cdot, e)$ un groupe et soit $a \in G$. On définit $* : G \times G \to G$ par $x * y := x \cdot a \cdot y$.

   Démontrer qu'il existe $b \in G$ tel que $(G, *, b)$ est un groupe.

8. Soient $n \in \mathbb{N}$ et $\sigma, \tau \in S_n$. Supposons que σ s'écrit en cycles :

$$\sigma = (a_{1,1} \;\; a_{1,2} \;\; \ldots \;\; a_{1,m_1})(a_{2,1} \;\; a_{2,2} \;\; \ldots \;\; a_{2,m_2}) \ldots (a_{r,1} \;\; a_{r,2} \;\; \ldots \;\; a_{r,m_r}).$$

   Démontrer que $\tau\sigma\tau^{-1}$ s'écrit en cycles :

$$\tau\sigma\tau^{-1} = \big(\tau(a_{1,1}) \;\; \tau(a_{1,2}) \;\; \ldots \;\; \tau(a_{1,m_1})\big) \big(\tau(a_{2,1}) \;\; \tau(a_{2,2}) \;\; \ldots \;\; \tau(a_{2,m_2})\big) \ldots \big(\tau(a_{r,1}) \;\; \tau(a_{r,2}) \;\; \ldots \;\; \tau(a_{r,m_r})\big).$$

9. Soit $(A, +, \cdot, 0, 1)$ un corps. Démontrer que A est un anneau intègre.

À propos. Tous les entiers naturels sont exceptionnels !

En effet, supposons par l'absurde que ce n'est pas le cas, c'est-à-dire qu'il existe un entier naturel non exceptionnel. Formellement, si on appelle X le sous-ensemble de $\mathbb{N}$ formé des entiers non exceptionnels, l'hypothèse est que X est non vide.

D'après la propriété de bon ordre sur $\mathbb{N}$, l'ensemble X, non vide, possède un plus petit élément ; notons le n_0. Alors, n_0 est le plus petit entier de $\mathbb{N}$ qui n'est pas exceptionnel... ce qui est une propriété exceptionnelle ! Ainsi, n_0 lui-même est exceptionnel, ce qui contredit le fait que n_0 appartient à X (ensemble des entiers non exceptionnels).

On en déduit que tous les entiers naturels sont exceptionnels.

1. On $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ one defines the binary relation :

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

Prove that it is an equivalence relation.

Remark : In fact, the quotient set is by definition $\mathbb{Q}$, the set of *rational numbers* : the class of (a, x) is fomed by all (b, y) such that $ay = bx$, justifying the notation $\frac{a}{x}$ for the class $\overline{(a, x)}$.

2. Let E be a non-empty set and $\mathcal{P}(E)$ the power set of E (that is, the set of all subsets of E). On $\mathcal{P}(E)$ we define a binary relation $\supsetneq$ by : for A and B in $\mathcal{P}(E)$

$$A \sim_R B \iff A \supsetneq B \quad (\text{that is } A \supset B \text{ and } A \neq B)\,.$$

Which of the following properties hold for R (justify your answer) ?

(1) Reflexive ; (2) symmetric ; (3) antisymmetric ; (4) transitive ; (5) total. (6) Is it an order relation ? (7) Is it an equivalence relation ?

3. Let C and D be subsets of F. Prove :

(1) $f\left(f^{-1}(C)\right) \subseteq C$. Attention, one does not always have equality here ; give a counter example.

(2) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

4. (a) *(Involution)* Let E be a set and f a map from E into E such that : $f \circ f = \mathrm{id}_E$. Prove that f is bijective. What is its inverse ?

(b) Let E, F, G be sets and $f : E \to F$, $g : F \to G$ maps. Prove that if f and g are injective, then $g \circ f$ is injective.

(c) If A, B are sets, we denote by $\mathcal{F}(A, B)$ the set of all maps $A \to B$. Let E, F and G be sets.

(1) Let f be an injective map from F to G. Prove :

$$\forall (g, h) \in \mathcal{F}(E, F), (f \circ g = f \circ h \Longrightarrow g = h).$$

In other words, show that the map

$$\begin{array}{ccc} \mathcal{F}(E, F) & \longrightarrow & \mathcal{F}(E, G) \\ g & \longmapsto & f \circ g \end{array}$$

is injective.

(2) Let f be a surjective map from E to F. Prove :

$$\forall (g, h) \in \mathcal{F}(F, G), (g \circ f = h \circ f \Longrightarrow g = h).$$

In other words, show that the map

$$\begin{array}{ccc} \mathcal{F}(F, G) & \longrightarrow & \mathcal{F}(E, G) \\ g & \longmapsto & g \circ f \end{array}$$

is injective.

5. Prove the following variant of induction.

Let $A(n)$ be an assertion that depends on $n \in \mathbb{N}$. Suppose that $A(0)$ is true. For all $n \in \mathbb{N}$, suppose also that the assertion $(\forall\, m \leq n : A(m)) \Rightarrow A(n + 1)$ is true.

Prove : $A(n)$ is true for all $n \in \mathbb{N}$.

Hint : use that $\mathbb{N}$ is well-ordered, i.e. that every non-empty subset of $\mathbb{N}$ has a smallest element.

6. Does there exist a bijection between $\mathbb{R}$ and $\mathbb{R} \times \mathbb{R}$? If yes, write down one ; if not, prove it.
7. Let $(G, \cdot, e)$ be a group, and let $a \in G$. Define $* : G \times G \to G$ by $x * y := x \cdot a \cdot y$.

   Prove that there exists $b \in G$ such that $(G, *, b)$ is a group.
8. Let $n \in \mathbb{N}$ and $\sigma, \tau \in S_n$. Suppose that σ is written in cycles as :

$$\sigma = (a_{1,1} \;\; a_{1,2} \;\; \dots \;\; a_{1,m_1})(a_{2,1} \;\; a_{2,2} \;\; \dots \;\; a_{2,m_2}) \dots (a_{r,1} \;\; a_{r,2} \;\; \dots \;\; a_{r,m_r}).$$

   Prove that $\tau\sigma\tau^{-1}$ is written in cycles as :

$$\tau\sigma\tau^{-1} = \big(\tau(a_{1,1}) \;\; \tau(a_{1,2}) \;\; \dots \;\; \tau(a_{1,m_1})\big) \big(\tau(a_{2,1}) \;\; \tau(a_{2,2}) \;\; \dots \;\; \tau(a_{2,m_2})\big) \dots \big(\tau(a_{r,1}) \;\; \tau(a_{r,2}) \;\; \dots \;\; \tau(a_{r,m_r})\big).$$

9. Let $(A, +, \cdot, 0, 1)$ be a field. Show that A is an integral domain.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 7

02/11/2015

Les exercices sont à rendre le 16/11/2015 au début du cours.

(English translation on page 3.)

1. (a) Soit n un entier naturel, s'écrivant dans le système décimal $n = c_r c_{r-1} \dots c_1 c_0$ (avec les chiffres c_i dans $\{0, 1, \dots, 9\}$; par exemple, pour $n = 235$ on a $c_0 = 5$, $c_1 = 3$ et $c_2 = 2$). Utiliser le calcul de congruences pour démontrer :
   (1) n est divisible par 3 (ou 9) si et seulement si la somme $\sum_{i=0}^{r} c_i$ l'est ;
   (2) n est divisible par 11 si et seulement si la somme $\sum_{i=0}^{r} (-1)^i c_i$ l'est.
   (b) Donner et démontrer une règle facile pour le calcul, en fonction de n, du dernier chiffre de 3^n (utiliser les congruences modulo 10).
   (c) Calculer le plus grand diviseur commun de 462 et 143, ainsi qu'une relation de Bézout.
2. Soit $n \in \mathbb{N}$. Nous définissons

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$$

   et

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}.$$

   Démontrer : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un anneau commutatif.

   Indication. Utiliser le lemme 10.6 du cours pour démontrer que $+$ et $\cdot$ sont bien définis (indépendants des choix des représentants) et le fait que $(\mathbb{Z}, +, \cdot, 0, 1)$ est un anneau commutatif.
3. (a) Écrire les tables d'addition et de multiplication de l'anneau $\mathbb{Z}/5\mathbb{Z}$.
   (b) Trouver un diviseur de zéro différent de $\bar{0}$ dans l'anneau quotient $\mathbb{Z}/57\mathbb{Z}$. *Cela démontre, entre autres, que $\mathbb{Z}/57\mathbb{Z}$ n'est pas un anneau intègre.*
   (c) Calculer l'inverse de la classe $\overline{16}$ dans $\mathbb{Z}/57\mathbb{Z}$.

4. Soient $x, y \in \mathbb{N}_{>0}$. Démontrer :

   (a) Un plus petit commun multiple de x et y existe et il est unique.

   (b) On a l'identité $xy = \mathrm{ppcm}(x, y) \cdot \mathrm{pgcd}(x, y)$.

   (c) Nous savons (appendice du cours) que tout nombre naturel $n \geq 1$ s'écrit comme produit fini de nombres premiers de façon unique à l'ordre près. Soient

   $$x = p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}, \quad y = p_1^{f_1} \cdot \cdots \cdot p_r^{f_r}$$

   avec $e_i, f_i \geq 0$ et $p_1, \ldots, p_r$ des nombres premiers les écritures de x et y.
   Exprimer la décomposition de $\mathrm{pgcd}(x, y)$ et $\mathrm{ppcm}(x, y)$ en facteurs premiers. Démontrer la réponse.

Indication : Il y a plusieurs possibilités pour démontrer (a). Par exemple :

- *Si, pour l'existence du ppcm, on montre que* $\mathrm{pgcd}(x, y)$ *divise* xy *et que* $\frac{xy}{\mathrm{pgcd}(x,y)}$ *est un ppcm de* x *et* y*, alors la partie (b) est déjà traitée.*
- *Si, pour l'existence du ppcm, on le décrit comme produit de nombres premiers, alors la partie (c) peut être traitée en même temps. Puis, il n'est pas difficile de déduire (b) aussi.*

5. Soit $\mathbb{Q}$ l'ensemble des nombres rationnels comme défini dans la feuille 6. Démontrer :

   (a) Les deux applications

   $$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$

   et

   $$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$

   sont bien définies, c'est-à-dire, leurs définitions ne dépendent pas des choix des représentant (a, x) et (b, y) des classes $\frac{a}{x}$ et $\frac{b}{y}$.

   (b) $(\mathbb{Q}, +, \cdot, \frac{0}{1}, \frac{1}{1})$ est un corps.

   (c) L'application

   $$\iota : \mathbb{Z} \to \mathbb{Q}, \quad n \mapsto \frac{n}{1}$$

   est injective et on a $\iota(n + m) = \iota(n) + \iota(m)$ et $\iota(n \cdot m) = \iota(n) \cdot \iota(m)$.

6. Construire un corps à 4 éléments en donnant la table d'addition et la table de multiplication. (Ne pas démontrer vérifier les axiomes.)

À propos. Il a été démontré que fêter son anniversaire est bon pour la santé. Des statistiquent prouvent clairement que les personnes qui célèbrent leurs anniversaires le plus de fois deviennent les plus vieilles.

Sander den Hartog (cité de C. Hesse, "Warum Mathematik glücklich macht")

1. (a) Let n be a natural number written in the decimal system as $n = c_r c_{r-1} \dots c_1 c_0$ (the digits c_i being in $\{0, 1, \dots, 9\}$; for exemple, for $n = 235$ one has $c_0 = 5$, $c_1 = 3$ and $c_2 = 2$). Use a computation with congruences to prove:

   (1) n is divisible by 3 (or 9) if and only if the sum $\sum_{i=0}^{r} c_i$ is;

   (2) n is divisible by 11 if and only if the sum $\sum_{i=0}^{r} (-1)^i c_i$ is.

   (b) Give and prove an easy rule for the calculation, as a function of n, of the last digi of 3^n (use congruences modulo 10).

   (c) Compute the greatest common divisor of 462 and 143, as well as a Bézout relation.

2. Let $n \in \mathbb{N}$. We define

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$$

   and

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}.$$

   Prove: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ is a commutative ring.

   Hint: Use Lemma 10.6 from the lecture notes in order to prove that $+$ and $\cdot$ are well defined (independent of the choice of representatives) and the fact that $(\mathbb{Z}, +, \cdot, 0, 1)$ is a commutative ring.

3. (a) Write the addition and the multiplication table of the ring $\mathbb{Z}/5\mathbb{Z}$.

   (b) Find a zero divisor different from $\overline{0}$ in the quotient ring $\mathbb{Z}/57\mathbb{Z}$. *This shows, among other things, that $\mathbb{Z}/57\mathbb{Z}$ is not an integral domain.*

   (c) Compute the inverse of the class $\overline{16}$ in $\mathbb{Z}/57\mathbb{Z}$.

4. Let $x, y \in \mathbb{N}_{>0}$. Prove:

   (a) A lowest common multiple of x and y exists and is unique.

   (b) One has the identity $xy = \mathrm{ppcm}(x, y) \cdot \mathrm{pgcd}(x, y)$.

   (c) We know (appendix in the lecture notes) that every natural number $n \geq 1$ can be written as a finite product of prime numbers in a unique way up to permuting the factors. Let

$$x = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}, \quad y = p_1^{f_1} \cdot \dots \cdot p_r^{f_r}$$

   with $e_i, f_i \geq 0$ and $p_1, \dots, p_r$ distinct prime numbers.

   Express $\mathrm{pgcd}(x, y)$ and $\mathrm{ppcm}(x, y)$ as products of prime numbers. Prove your answer.

   Hint: There are several ways to prove (a). For example:

   - *If for the existence of the lcm one proves that $\mathrm{lcm}(x, y)$ divides xy and that $\frac{xy}{\mathrm{gcd}(x,y)}$ is an lcm of x and y, then part (b) is already done.*
   - *If for the existence of the lcm one writes it as a product of primes, then part (c) can be treated at the same time. After that, it is not difficult to deduce (b) as well.*

5. Let $\mathbb{Q}$ be the set of rational numbers as defined on sheet 6. Prove:

   (a) The two maps
   $$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$
   and
   $$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$
   are well-defined, i.e. their definitions do not depend on the choice of representatives (a, x) and (b, y) of the classes $\frac{a}{x}$ and $\frac{b}{y}$.

   (b) $(\mathbb{Q}, +, \cdot, \frac{0}{1}, \frac{1}{1})$ is a field.

   (c) The map
   $$\iota : \mathbb{Z} \to \mathbb{Q}, \quad n \mapsto \frac{n}{1}$$
   is injective and one has $\iota(n + m) = \iota(n) + \iota(m)$ and $\iota(n \cdot m) = \iota(n) \cdot \iota(m)$.

6. Construct a field with 4 elements by giving its addition and its multiplication table. (You don't have to verify all the axioms.)

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 8

16/11/2015

Les exercices sont à rendre le 23/11/2015 au début du cours.

(English translation on page 2.)

1. Montrer que les groupes suivants sont cycliques. Donner un générateur.
   (a) $(\mathbb{Z}/6\mathbb{Z}, +, \overline{0})$
   (b) $(\mathbb{Z}/10\mathbb{Z}, +, \overline{0})$
   (c) $((\mathbb{Z}/6\mathbb{Z})^\times, \cdot, \overline{1})$
   (d) $((\mathbb{Z}/10\mathbb{Z})^\times, \cdot, \overline{1})$

2. (a) Dresser la liste complète de tous les sous-groupes de S_3. Lesquels sont cycliques ? Donner un générateur pour tout sous-groupe cyclique.
   (b) Soient $n \in \mathbb{N}_{\geq 1}$ et $(S_n, \circ, (1))$ le groupe symétrique. On rappelle que l'application *signe* ou *signature* est définie par

$$\mathrm{sgn} : S_n \to \{+1, -1\}, \quad \pi \mapsto \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$

   Démontrer que c'est un homomorphisme de groupes.
   (c) Le noyau de sgn est noté A_n et appelé le *groupe alterné*.
   Dresser la liste de tous les éléments du groupe A_4.

3. Dans ce jeu, extrait du livre *Gödel, Escher, Bach* de D. Hofstadter, nous produisons des chaînes de symboles M, I, U, en appliquant successivement une des quatre règles suivantes :

   Soit x une chaîne.

   Règle 1 De la chaîne xI faire la chaîne xIU.
   Exemple : MIUMI $\mapsto$ MIUMIU

   Règle 2 De la chaîne Mx faire la chaîne Mxx.
   Exemple : MIUMI $\mapsto$ MIUMIIUMI

   Règle 3 Remplacer III par U.
   Exemple : MIUIIIMI $\mapsto$ MIUUMI

   Règle 4 Effacer UU de la chaîne.
   Exemple : MIUUIMUUUI $\mapsto$ MIIMUI

   Est-il possible d'obtenir la chaîne MU en commençant par la chaîne MI et en utilisant les règles ci-dessus ? *Indication : les quatres règles conservent la propriété « le nombre de I dans la chaîne n'est pas congru à* 0 *mod* 3 *» (Le démontrer !).*

4. Le but de cet exercice est de construire les nombres réels à partir de $\mathbb{Q}$ (en tant que « complétion de $\mathbb{Q}$ par rapport à la valeur absolue »). Dans cet exercice nous utilisons des connaissances du cours d'analyse. Si $a_0, a_1, a_2, \ldots$ est une suite, nous écrivons comme abréviation $(a_n)_{n\in\mathbb{N}}$. Si tous les a_n appartiennent à $\mathbb{Q}$, nous parlons d'une suite rationnelle et écrivons $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$.

   Nous rappelons du cours d'analyse qu'une suite $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ est appelée *suite de Cauchy* si pour tout $\epsilon > 0$ il existe $N \in \mathbb{N}$ tel que pour tout $n, m \geq N$ on a $|a_n - a_m| < \epsilon$.

   Nous rappelons également qu'une suite $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ est dite de *converger vers zéro* si pour tout $\epsilon > 0$ il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$ on a $|a_n| < \epsilon$. Il est clair (et ne doit pas être démontré ici) que toute suite qui converge vers zéro est une suite de Cauchy.

   Soit $\mathcal{C}$ l'ensemble de toutes les suites de Cauchy et $\mathcal{N}$ le sous-ensemble de toutes les suites qui convergent vers zéro. On note par 0 la suite dont tous les termes sont 0 et par 1 la suite de Cauchy dont tous les termes sont 1.

   Soit $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$. Il est connu du cours d'analyse que les suites $(a_n + b_n)_{n\in\mathbb{N}}$ et $(a_n \cdot b_n)_{n\in\mathbb{N}}$ sont aussi des suites de Cauchy (vous ne devrez pas le démontrer ici). Cela nous permet de définir deux applications

$$+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}, \quad (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}}$$

   et

$$\cdot : \mathcal{C} \times \mathcal{C} \to \mathcal{C}, \quad (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (a_n \cdot b_n)_{n\in\mathbb{N}}.$$

   (a) Sur $\mathcal{C}$ on définit la relation binaire

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \Leftrightarrow \exists\, (c_n)_{n\in\mathbb{N}} \in \mathcal{N} : (a_n)_{n\in\mathbb{N}} + (c_n)_{n\in\mathbb{N}} = (b_n)_{n\in\mathbb{N}}.$$

   Démontrer qu'il s'agit d'une relation d'équivalence.

   La classe d'équivalence de $(a_n)_{n\in\mathbb{N}}$ est notée $\overline{(a_n)_{n\in\mathbb{N}}}$. L'ensemble des classes d'équivalence est noté $\mathbb{R}$. Noter que cela a comme conséquence (évidente/par définition) que toute suite de Cauchy rationnelle définit ('converge vers') un élément de $\mathbb{R}$.

   (b) Soit $c_0 \in \mathbb{N}$ et pour $n \in \mathbb{N}_{\geq 1}$ soit $c_n \in \{0, 1, \ldots, 9\}$. Pour $n \in \mathbb{N}$ on définit $a_n := \sum_{i=0}^{n} c_n 10^{-i}$. Montrer que $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy (et donc définit un élément de $\mathbb{R}$). (Cette partie vous montre que les nombres écrits en dévelopement décimal définissent un élément de $\mathbb{R}$; vous voyez donc que ce que vous connaissez probablement comme nombres réels du lycée est en effet un nombre réel. Plus loin on verra une assertion réciproque.)

   (c) Définir des applications $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ et $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ telles que $(\mathbb{R}, +, \cdot, \overline{0}, \overline{1})$ est un corps commutatif. Démontrer vos assertions.

À propos. « Je suis content de ne pas aimer les asperges. Car, si j'aimais les asperges, je devrais en manger, mais je les déteste. »

Lewis Carrol (cité de C. Hesse : Warum Mathematik glücklich macht)

1. Prove that the following groups are cyclic. Give a generator.

   (a) $(\mathbb{Z}/6\mathbb{Z}, +, \overline{0})$

   (b) $(\mathbb{Z}/10\mathbb{Z}, +, \overline{0})$

   (c) $((\mathbb{Z}/6\mathbb{Z})^\times, \cdot, \overline{1})$

   (d) $((\mathbb{Z}/10\mathbb{Z})^\times, \cdot, \overline{1})$

2. (a) Write down the complete list of all subgroups of S_3. Which ones are cyclic? Give a generator for every cyclic subgroup.

   (b) Let $n \in \mathbb{N}_{\geq 1}$ and $(S_n, \circ, (1))$ be the symmetric group. We recall that the map *sign* or *signature* is defined by

   $$\mathrm{sgn} : S_n \to \{+1, -1\}, \quad \pi \mapsto \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$

   Prove that it is a group homomorphism.

   (c) The kernel of sgn is denoted A_n and called the *alternating group*.

   Write down the list of all elements of the group A_4.

3. In this game, taken from the book *Gödel, Escher, Bach* by D. Hofstadter, we produce chains of the symbols M, I, U, by successively applying the following four rules:

   Let x be a chain.

   Rule 1 Starting from the chain xI, make the chain xIU.

   Example: MIUMI $\mapsto$ MIUMIU

   Rule 2 Starting from the chain Mx, make the chain Mxx.

   Example: MIUMI $\mapsto$ MIUMIIUMI

   Rule 3 Replace III by U.

   Example: MIUIIIMI $\mapsto$ MIUUMI

   Rule 4 Delete UU from the chain.

   Example: MIUUIMUUUI $\mapsto$ MIIMUI

   Is it possible to obtain the chain MU if one starts from the chain MI by applying the four rules above? *Hint: The four rules preserve the property "the number of I in the chain is not congruent* 0 *mod* 3*" (prove it!).*

4. The aim of this exercise is to construct the real numbers from $\mathbb{Q}$ (as the 'completion with respect to the absolute value of $\mathbb{Q}$'). In this exercise we use some knowledge from your Analysis class. If $a_0, a_1, a_2, \ldots$ is a sequence, we write for short $(a_n)_{n \in \mathbb{N}}$. If all the a_n belong to $\mathbb{Q}$, we speak of a rational sequence and write $(a_n)_{n \in \mathbb{N}} \subset \mathbb{Q}$.

   We recall from your Analysis class that a sequence $(a_n)_{n \in \mathbb{N}} \subset \mathbb{Q}$ is called a *Cauchy sequence* if for all $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$ one has $|a_n - a_m| < \epsilon$.

   We recall further that a sequence $(a_n)_{n \in \mathbb{N}} \subset \mathbb{Q}$ is called a *zero/null sequence* if for all $\epsilon > 0$ there is $N \in \mathbb{N}$ such that for all $n \geq N$ one has $|a_n| < \epsilon$. It is clear (and need not be proved here) that any null sequence is a Cauchy sequence.

   Let $\mathcal{C}$ be the set of all Cauchy sequences and $\mathcal{N}$ the subset of all null sequences. Denote by 0 the null sequence all of whose terms are 0 and by 1 the Cauchy sequence all of whose terms are 1.

Let $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$. It is also known from Analysis that the sequences $(a_n + b_n)_{n\in\mathbb{N}}$ and $(a_n \cdot b_n)_{n\in\mathbb{N}}$ are also Cauchy sequences (you don't have to prove this in this exercise). This allows us to define two maps

$$+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}, \quad (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}}$$

and

$$\cdot : \mathcal{C} \times \mathcal{C} \to \mathcal{C}, \quad (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (a_n \cdot b_n)_{n\in\mathbb{N}}.$$

(a) On $\mathcal{C}$ one defines the binary relation

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \Leftrightarrow \exists\, (c_n)_{n\in\mathbb{N}} \in \mathcal{N} : (a_n)_{n\in\mathbb{N}} + (c_n)_{n\in\mathbb{N}} = (b_n)_{n\in\mathbb{N}}.$$

Prove that this relation is an equivalence relation.

The equivalence class of $(a_n)_{n\in\mathbb{N}}$ is denoted $\overline{(a_n)_{n\in\mathbb{N}}}$. The set of equivalence classes is denoted by $\mathbb{R}$. Note that this has the (obvious/by definition) consequence that every rational Cauchy sequence defines ('converges to') an element of $\mathbb{R}$.

(b) Let $c_0 \in \mathbb{N}$ and for $n \in \mathbb{N}_{\geq 1}$ let $c_n \in \{0, 1, \ldots, 9\}$. For $n \in \mathbb{N}$ define $a_n := \sum_{i=0}^{n} c_n 10^{-i}$.
Prove that $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence (and hence defines an element of $\mathbb{R}$). (This part is to show you that numbers written in a decimal expansion define an element of $\mathbb{R}$, so that you see how what you probably know as the real numbers from school is really a real number. Below you'll prove a converse.)

(c) Define maps $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ such that $(\mathbb{R}, +, \cdot, \overline{0}, \overline{1})$ is a (commutative) field. Prove your statements.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 9

23/11/2015

Les exercices sont à rendre le 30/11/2015 au début du cours.

(English version on page 3.)

1. Soient G, H des groupes et $\varphi : G \to H$ un homomorphisme. Soit $g \in G$ un élément d'ordre fini.

   Démontrer : $\varphi(g)$ est aussi d'ordre fini et $\mathrm{ord}(\varphi(g)) \mid \mathrm{ord}(g)$.

2. Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Démontrer qu'il existe précisement six différent isomorphismes $G \to G$.

   En d'autres mots, le groupe $\mathrm{Aut}(G)$ des automorphismes de G est de cardinal 6. Est-ce qu'il est isomorphe à S_3 ou à $\mathbb{Z}/6\mathbb{Z}$? Justifier votre réponse.

3. Soit G un groupe.

   (a) Soient $E, F \subseteq G$ des sous-ensemble. Nous définissons

   $$E \cdot F = \{e \cdot f \mid e \in E, f \in F\}.$$

   Démontrer l'associativité : $E_1 \cdot (E_2 \cdot E_3) = (E_1 \cdot E_2) \cdot E_3$ pour tous sous-ensembles $E_1, E_2, E_3 \subseteq G$.

   (b) Soit $H \subseteq G$ un sous-groupe. Démontrer : $H \cdot H = H$.

   (c) Soient $H \subseteq G$ et $g \in G$. Nous abusons (légèrement) la notation pour écrire $g \cdot H$ pour $\{g\} \cdot H$, la classe à gauche suivant H représentée par g. Supposons que $H \trianglelefteq G$ soit distingué.

   Conclure de ce qui précède que pour $g_1, g_2, g_3 \in G$ on a :

   (1) $(g_1 \cdot H) \cdot (g_2 \cdot H) = (g_1 \cdot g_2) \cdot H$,

   (2) $(g_1 \cdot H) \cdot H = H \cdot (g_1 \cdot H) = g_1 \cdot H$,

   (3) $\big((g_1 \cdot H) \cdot (g_2 \cdot H)\big) \cdot (g_3 \cdot H) = (g_1 \cdot H) \cdot \big((g_2 \cdot H) \cdot (g_3 \cdot H)\big)$,

   (4) $(g_1 \cdot H) \cdot (g_1^{-1} \cdot H) = H$.

   Cela donne une autre démonstration du fait que G/H est un groupe.

4. Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal.

   Soient $HN := \{hn \mid h \in H, n \in N\}$ et $NH := \{nh \mid n \in N, h \in H\}$.

   Démontrer :

   (a) $H \cap N$ est un sous-groupe normal de H.

   (b) $HN = NH$.

   (c) HN est un sous-groupe de G.

   (d) N est un sous-groupe normal de HN.

   (e) Si H est aussi un sous-groupe normal de G, alors HN est un sous-groupe normal de G.

5. (Exercice supplémentaire, pour bonus A+) Dans cet exercice on établit des propriétés des nombres réels comme l'existence d'un ordre totale. Il est une continuation de l'exercice 5 de la feuille 8 dont on utilise la notation.

   (a) On définit l'application
   $$\iota : \mathbb{Q} \to \mathbb{R}, \quad x \mapsto \overline{x},$$
   où $\overline{x}$ est la suite de Cauchy dont tous les termes sont x.
   Démonter que ι est injectif et satisfait pour tout $x, y \in \mathbb{Q}$:
   $$\iota(x+y) = \iota(x) + \iota(y) \text{ et } \iota(x \cdot y) = \iota(x) \cdot \iota(y).$$
   La signification de cette assertion est que nous pouvons voir $\mathbb{Q}$ comme un sous-ensemble de $\mathbb{R}$ (notamment l'image de $\mathbb{Q}$ par ι).

   (b) Soit $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ une suite de Cauchy. Dans cet exercice nous écrivons le dévelopement décimal du nombre réel défini par une suite de Cauchy. Comme cela est bien connu pour $\mathbb{Q}$, nous pouvons et allons supposer que $\overline{(a_n)_{n\in\mathbb{N}}}$ n'appartient pas à $\mathbb{Q}$.
   Démontrer l'assertion suivante : pour tout $m \in \mathbb{N}$ il existe $b_m \in \mathbb{Z}$ et $N_m \in \mathbb{N}$ tels que pour tout $n \geq N_m$ on a
   $$\frac{b_m}{10^m} < a_n < \frac{b_m + 1}{10^m}.$$
   On définit $c_0 := b_0$ et pour tout $m \geq 1$ on définit $c_m := b_m - 10b_{m-1}$. Démontrer $c_m \in \{0, 1, \ldots, 9\}$ pour tout $m \geq 1$.
   En plus, pour $n \in \mathbb{N}$ on définit $d_n := \sum_{i=0}^{n} c_n 10^{-i}$. Démontrer que $(d_n)_{n\in\mathbb{N}}$ est une suite de Cauchy rationnelle qui défnit le même élément de $\mathbb{R}$ que $(a_n)_{n\in\mathbb{N}}$. Noter que si $c_0 \in \mathbb{N}$, cela est le dévelopement décimal standard de $(a_n)_{n\in\mathbb{N}}$.

   (c) Pour $\overline{(a_n)_{n\in\mathbb{N}}}, \overline{(b_n)_{n\in\mathbb{N}}} \in \mathbb{R}$, on définit
   $$\overline{(a_n)_{n\in\mathbb{N}}} \leq \overline{(b_n)_{n\in\mathbb{N}}} \Leftrightarrow \exists\, (c_n)_{n\in\mathbb{N}} \in \mathcal{C} : \forall\, n \in \mathbb{N} : c_n \geq 0 \wedge \overline{(a_n)_{n\in\mathbb{N}}} + \overline{(c_n)_{n\in\mathbb{N}}} = \overline{(b_n)_{n\in\mathbb{N}}}.$$
   Démontrer que cela définit une relation d'ordre totale sur $\mathbb{R}$.

   (d) Pour $\overline{(a_n)_{n\in\mathbb{N}}} \in \mathbb{R}$, définir sa valeur absolue comme $\overline{(|a_n|)_{n\in\mathbb{N}}} \in \mathbb{R}$.
   Démontrer que pour tout $\overline{(a_n)_{n\in\mathbb{N}}} \in \mathbb{R}$ et pour tout $\epsilon > 0$, il existe $x \in \mathbb{Q}$ tel que $|\overline{x} - \overline{(a_n)_{n\in\mathbb{N}}}| < \epsilon$.
   Cela signifie que « $\mathbb{Q}$ est dense dans $\mathbb{R}$ » : tout élément de $\mathbb{R}$ peut être approximé par un nombre rationnel.

À propos. Concernant les déductions logiques...

"Hering ist gut. Schlagsahne ist gut.
Wie gut muss erst Hering mit Schlagsahne sein - !"
Kurt Tucholsky, zitiert nach : Thiele, Mathematische Beweise.

Traduction belge libre : "Les gaufres sont bonnes. Les frites sont bonnes.
Comme les gaufres aux frites doivent être bonnes !"

1. Let G, H be groups and $\varphi : G \to H$ a homomorphism. Let $g \in G$ be an element of finite order.

   Prove that $\varphi(g)$ is also of finite order and $\mathrm{ord}(\varphi(g)) \mid \mathrm{ord}(g)$.

2. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Prove that there are exactly six different isomorphisms $G \to G$.

   In other words, the group $\mathrm{Aut}(G)$ of automorphisms of G is of cardinality 6. Is it isomorphic with S_3 or with $\mathbb{Z}/6\mathbb{Z}$? Justify your answer.

3. Let G be a group.

   (a) Let $E, F \subseteq G$ be subsets. We define

   $$E \cdot F = \{e \cdot f \mid e \in E, f \in F\}.$$

   Prove associativity: $E_1 \cdot (E_2 \cdot E_3) = (E_1 \cdot E_2) \cdot E_3$ for all subsets $E_1, E_2, E_3 \subseteq G$.

   (b) Let $H \subseteq G$ be a subgroup. Prove: $H \cdot H = H$.

   (c) Let $H \subseteq G$ and $g \in G$. We (slightly) abuse notation by writing $g \cdot H$ for $\{g\} \cdot H$, the left coset modulo H represented by g. Suppose that $H \trianglelefteq G$ is a normal subgroup.

   Conclude from the preceding statements that for $g_1, g_2, g_3 \in G$ one has:

   (1) $(g_1 \cdot H) \cdot (g_2 \cdot H) = (g_1 \cdot g_2) \cdot H$,

   (2) $(g_1 \cdot H) \cdot H = H \cdot (g_1 \cdot H) = g_1 \cdot H$,

   (3) $\big((g_1 \cdot H) \cdot (g_2 \cdot H)\big) \cdot (g_3 \cdot H) = (g_1 \cdot H) \cdot \big((g_2 \cdot H) \cdot (g_3 \cdot H)\big)$,

   (4) $(g_1 \cdot H) \cdot (g_1^{-1} \cdot H) = H$.

   This gives a different proof of the fact that G/H is a group.

4. Let G be a group, $H \leq G$ a subgroup and $N \leq G$ a normal subgroup.

   Let $HN := \{hn \mid h \in H, n \in N\}$ and $NH := \{nh \mid n \in N, h \in H\}$.

   Prove:

   (a) $H \cap N$ is a normal subgroup of H.

   (b) $HN = NH$.

   (c) HN is a subgroup of G.

   (d) N is a normal subgroup of HN.

   (e) If H is also a normal subgroup of G, then HN is a normal subgroup of G.

5. (Supplementary exercise, for extra bonus A+) In this exercise we are going to establish some properties of the real numbers like the existence of a total ordering. It is a continuation of Exercise 5 from sheet 8 the notation of which we use.

   (a) Define the map

   $$\iota : \mathbb{Q} \to \mathbb{R}, \quad x \mapsto \overline{x},$$

   where $\overline{x}$ is the Cauchy sequence all of whose terms are equal to x.

   Prove that ι is injective and satisfies for all $x, y \in \mathbb{Q}$:

   $$\iota(x + y) = \iota(x) + \iota(y) \text{ and } \iota(x \cdot y) = \iota(x) \cdot \iota(y).$$

   The meaning of this statement is that we can see $\mathbb{Q}$ as a subset of $\mathbb{R}$ (namely as the image of $\mathbb{Q}$ under ι).

(b) Let $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ be a given Cauchy sequence. In this exercise we write down the decimal expansion of the real number defined by the Cauchy sequence. Since doing this for rationals is well known, we may and do assume that $\overline{(a_n)_{n\in\mathbb{N}}}$ is not in $\mathbb{Q}$.

Prove the following statement: for all $m \in \mathbb{N}$ there are $b_m \in \mathbb{Z}$ and $N_m \in \mathbb{N}$ such that for all $n \geq N_m$ one has

$$\frac{b_m}{10^m} < a_n < \frac{b_m + 1}{10^m}.$$

Define $c_0 := b_0$ and for all $m \geq 1$, define $c_m := b_m - 10b_{m-1}$. Prove that $c_m \in \{0, 1, \ldots, 9\}$ for all $m \geq 1$.

Moreover, for $n \in \mathbb{N}$ define $d_n := \sum_{i=0}^{n} c_n 10^{-i}$. Prove that $(d_n)_{n\in\mathbb{N}}$ is a rational Cauchy sequence defining the same element of $\mathbb{R}$ as $(a_n)_{n\in\mathbb{N}}$. Note that if $c_0 \in \mathbb{N}$, this is the standard decimal expansion of $(a_n)_{n\in\mathbb{N}}$.

(c) For $\overline{(a_n)_{n\in\mathbb{N}}}, \overline{(b_n)_{n\in\mathbb{N}}} \in \mathbb{R}$, we define

$$\overline{(a_n)_{n\in\mathbb{N}}} \leq \overline{(b_n)_{n\in\mathbb{N}}} \Leftrightarrow \exists\, (c_n)_{n\in\mathbb{N}} \in \mathcal{C} : \forall\, n \in \mathbb{N} : c_n \geq 0 \wedge \overline{(a_n)_{n\in\mathbb{N}}} + \overline{(c_n)_{n\in\mathbb{N}}} = \overline{(b_n)_{n\in\mathbb{N}}}.$$

Prove that this defines a total order relation on $\mathbb{R}$.

(d) For $\overline{(a_n)_{n\in\mathbb{N}}} \in \mathbb{R}$, define its absolute value as $\overline{(|a_n|)_{n\in\mathbb{N}}} \in \mathbb{R}$.

Prove that for all $\overline{(a_n)_{n\in\mathbb{N}}} \in \mathbb{R}$ and for all $\epsilon > 0$, there is $x \in \mathbb{Q}$ such that $|\overline{x} - \overline{(a_n)_{n\in\mathbb{N}}}| < \epsilon$.

This means that '$\mathbb{Q}$ is dense in $\mathbb{R}$': any element in $\mathbb{R}$ can be approximated arbitrarily closely by a rational number.

Exercices : Algèbre 1

Semestre d'hiver 2015/2016

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Chun Yin Hui, Laia Amorós

Feuille 10

30/11/2015

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé qui aura lieu le 10/12/2015.

(English version on page 3.)

1. Soient G un groupe fini et $H_1 \subseteq H_2 \subseteq G$ des sous-groupes. Démontrer la généralisation suivante du théorème de Lagrange :
$$(G : H_1) = (G : H_2) \cdot (H_2 : H_1).$$
Indication : Il suffit d'écrire l'indice comme un quotient de cardinaux.

2. Soit $(G, \star, e)$ un groupe.

   (a) Le *centre de* G est défini comme $\mathcal{Z}(G) := \{g \in G \mid \forall\, h \in G : \ g \star h = h \star g\}$. Démontrer que $\mathcal{Z}(G)$ est un sous-groupe normal de G. (Le fait que c'est un sous-groupe a été démontré dans le dernier devoir surveillé.)

   (b) Pour tout h dans G on définit
$$\sigma_h : G \to G, \quad g \mapsto h \star g \star h^{-1}.$$
Démontrer que, pour tout h dans G, l'application σ_h est un morphisme de groupes.

   (c) Démontrer que, pour tout $h \in G$, σ_h est un automorphisme de G (c'est-à-dire $\sigma_h \in \mathrm{Aut}(G)$) en donnant un inverse.

   (d) Démontrer que l'application
$$\begin{array}{rccc} \varphi : & G & \to & \mathrm{Aut}(G) \\ & h & \mapsto & \sigma_h \end{array}$$
est un morphisme de groupes.

   (e) Un automorphisme $\sigma : G \to G$ est dit *intérieur* s'il existe h dans G tel que, pour tout g dans G, on a $\sigma(g) = h \star g \star h^{-1}$ (c'est-à-dire $\sigma = \sigma_h$). On pose $\mathrm{Inn}(G) := \{\sigma \in \mathrm{Aut}(G) \mid \sigma \text{ est intérieur}\}$. Démontrer que $\mathrm{Inn}(G)$ est un sous-groupe normal de $\mathrm{Aut}(G)$.

   (f) En utilisant le théorème d'isomorphisme, écrire et démontrer un isomorphisme $G/\mathcal{Z}(G) \to \mathrm{Inn}(G)$.

3. Soit $(G, \star, e)$ un groupe. Supposons que $G/\mathcal{Z}(G)$ est cyclique. Démontrer que G est abélien.

4. Soient E un ensemble et G un groupe. On suppose que G agit sur E. Démontrer que la relation binaire $\sim_G$ définie sur E par
$$\forall (x, y) \in E^2, \ x \sim_G y \iff \exists g \in G, y = g \cdot x$$
est une relation d'équivalence sur E.

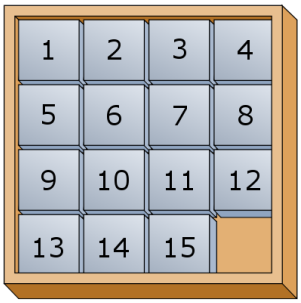
   Conclure que pour tout x dans E, la classe d'équivalence de x pour cette relation est l'orbite de x sous l'action de G.

Conclure aussi que nous avons la réunion disjointe

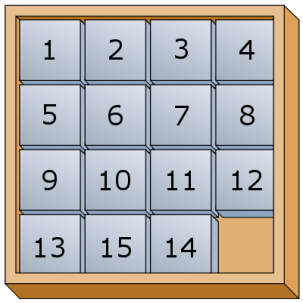
$$E = \bigsqcup_{\omega \in G \setminus E} \omega.$$

5. Déterminer le nombre de différentes chaînes à 6 perles mobiles coloriées en vert, jaune, bleu et noir sur un fil.
6. Soit G un groupe et $H \subseteq G$ un sous-groupe d'indice 2. Démontrer que H est un sous-groupe normal.
7. Vous connaissez certainement le jeu représenté dans l'image. Un coup consiste en le déplacement du trou d'une case vers la droite, la gauche, le haut ou le bas.

Position initiale



Position finale



   (a) Supposons qu'au début du jeu le trou est en bas à droite comme dans l'image ci-dessus.
   Démontrer : si après n coups le trou se trouve aussi en bas à droite, alors n est pair.
   Indication : il peut aider de colorier le tableau comme un jeu d'échec.

   (b) Démontrer qu'il est impossible d'obtenir la position finale (ci-dessus) à partir de la position initiale.
   Indication : utiliser S_{16}, le signe d'une permutation et (a).

À propos.

La mère de Philippe et Jacques a fait un super gâteau au chocolat pour ses deux garçons. La dernière fois, les garçons se sont bagarrés pour avoir le morceau qui semblait le plus grand. Pour éviter que la même chose ne se reproduise, la mère demande à Philippe de couper le gâteau en deux et de laisser ensuite son frère Jacques choisir un des deux morceaux. Comme ça aucun des deux garçons ne peut être mécontent : ni Jacques, parce qu'il a pu choisir le morceau qui lui semble le plus grand ; ni Philippe, parce que c'est lui qui a pu couper le gâteau en deux morceaux de taille égale.

1. Let G be a finite group and $H_1 \subseteq H_2 \subseteq G$ des subgroups. Prove the following generalisation of the Theorem of Lagrange:
$$(G : H_1) = (G : H_2) \cdot (H_2 : H_1).$$
Hint: It suffices to write the index as a quotient of cardinalities.

2. Let $(G, \star, e)$ be a group.

   (a) The *centre of* G is defined as $\mathcal{Z}(G) := \{g \in G \mid \forall\, h \in G :\ g \star h = h \star g\}$. Prove that $\mathcal{Z}(G)$ is a normal subgroup of G. (The fact that it is a subgroup was proved in the last *devoir surveillé*.)

   (b) For h in G one defines
   $$\sigma_h : G \to G, \quad g \mapsto h \star g \star h^{-1}.$$
   Show that for all h in G, the map σ_h is a group homomorphism.

   (c) Show that for all $h \in G$, σ_h is an automorphism of G (i.e. $\sigma_h \in \mathrm{Aut}(G)$) by exhibiting an inverse.

   (d) Prove that the map
   $$\begin{array}{rccc} \varphi : & G & \to & \mathrm{Aut}(G) \\ & h & \mapsto & \sigma_h \end{array}$$
   is a group homomorphism.

   (e) An automorphism $\sigma : G \to G$ is called *inner* if there is h in G such that for all g in G, one has $\sigma(g) = h \star g \star h^{-1}$ (i.e. $\sigma = \sigma_h$). One puts $\mathrm{Inn}(G) := \{\sigma \in \mathrm{Aut}(G) \mid \sigma \text{ is inner}\}$.
   Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

   (f) Using the isomorphism theorem, write and prove an isomorphism $G/\mathcal{Z}(G) \to \mathrm{Inn}(G)$.

3. Let $(G, \star, e)$ be a group. Suppose that $G/\mathcal{Z}(G)$ is cyclic. Prove that G is abelien.

4. Let E be a set and G a group. We suppose that G acts on E. Prove that the binary relation $\sim_G$ defined on E by
$$\forall (x, y) \in E^2,\ x \sim_G y \iff \exists g \in G, y = g \cdot x$$
is an equivalence relation.

   Conclude that for all x in E, the equivalence class of x for this relation is the orbit of x under the action of G.

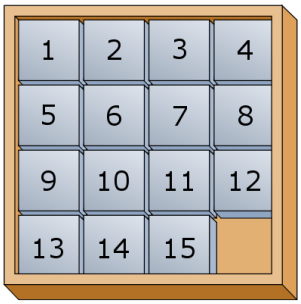
   Conclude also that we have a disjoint union
$$E = \bigsqcup_{\omega \in G\backslash E} \omega.$$

5. Determine the number of different necklaces with 6 movable coloured pearls that are green, yellow, blue or black on a string.

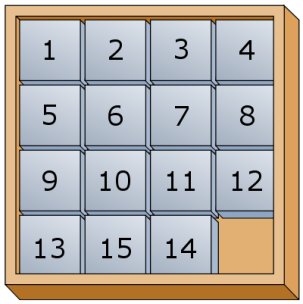
6. Let G be a group and $H \subseteq G$ a subgroup of index 2. Prove that H is a normal subgroup.

7. You certainly know the game in the picture. A move consists in moving the hole one place to the right, the left, up or down.

Initial position



Final position



(a) Suppose that in the beginning the hole is in the bottom right position as shown in the above picture. Prove: if after n moves the hole is also in the bottom right position, then n is even.
Hint: it can be useful to color the board like a chess board.

(b) Prove that it is impossible to obtain the final position (see above) when starting from the initial position.
Hint: use S_{16}, the sign of a permutation and (a).