Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg

Gabor Wiese et Agnès David
gabor.wiese@uni.lu, agnes.david@uni.lu

Version du 16 décembre 2013

Table des matières

Préface

L'algèbre, c'est quoi ? 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 preuves et les premiers mots du langage mathématique

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'écoles) :
– $\mathbb{N}$, 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 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. 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.
L'entier n n'est pas un nombre premier (sinon avec $k = 1$ et $p_1 = n$ on aurait $n = p_1$).
Comme n n'est pas un nombre premier, 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, il est faux que le lemme est faux ; donc, le lemme est vrai. □

2 Assertions

Maintenant 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.

Assertions

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 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 qui 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.

[1] Il y a des subtilités avec 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.

L'implication $\Rightarrow$

Nous regardons maintenant des relations entre deux assertions.

(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. »
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.

(2) On peut aussi combiner les assertions A et B du point précédent comme ça :
« Il suffit qu'il pleuve pour que la rue soit mouillée. »
Cette assertion est aussi vraie ; son contenu est le même qu'avant. Nous avons seulement utilisé une formulation plus sophistiquée.

(3) 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. »
C'est également une assertion vraie.

(4) Assertion A : « $x = 1$ »
Assertion B : « $2x = 2$ »
Nouvelle assertion vraie : « Si on a $x = 1$, alors on a $2x = 2$. »
Repétons que nous n'avons rien dit sur la vérité des assertions A et B. Nous avons seulement constaté une relation entre les deux assertions.

(5) Assertion A : « $x = 1$ »
Assertion B : « $x^2 = 1$ »
Nouvelle assertion vraie : « Si on a $x = 1$, alors on a $x^2 = 1$. »

(6) (Juste pour montrer qu'on peut aussi obtenir des assertions fausses :)
Assertion A : « $x = 1$ »
Assertion B : « $2x = 4$ »
Nouvelle assertion fausse : « Si on a $x = 1$, alors on a $2x = 4$. »

Dans les définitions, énoncés et démonstrations, nous avons déjà utilisé quelques symboles. On pense que vous avez déjà vu ces symboles au lycée (par exemple « $\leq$ », « $<$ », « $\in$ », « $\mathbb{Z}$ »). On va maintenant en introduire d'autres et surtout discuter leur signification.
Nous introduisons le symbole $\Rightarrow$ pour les *implications*. Il est placé entre deux assertions pour indiquer que la vérité de la première assertion entraîne la vérité de la deuxième. Donc le symbole $\Rightarrow$ se lit comme : « implique », « alors », « en conséquence », « donc », « est suffisant pour » etc.
Nous allons maintenant reprendre les phrases précédentes en utilisant $\Rightarrow$. Notez que $\Rightarrow$ est toujours placé entre deux assertions.

(1) Il pleut. $\Rightarrow$ La rue est mouillée.
(2) Il pleut. $\Rightarrow$ La rue est mouillée.
(3) Je réussis l'examen. $\Rightarrow$ Je reçois les points ECTS.
(4) $x = 1 \ \Rightarrow \ 2x = 2$
(5) $x = 1 \ \Rightarrow \ x^2 = 1$
(6) $x = 1 \ \Rightarrow \ 2x = 4$
Attention : cette assertion est fausse ! ! Mais c'est quand même une assertion.

Repétons pour la dernière fois que la vérité de l'assertion « $A \Rightarrow B$ » (où A et B sont des assertions) ne dit pas que A est vraie, seulement que B est vraie si A l'est.

L'implication $\Leftarrow$

Le symbole $\Leftarrow$ a la même signification que $\Rightarrow$, sauf que les côtés sont inversés.

(1) La rue est mouillée. $\Leftarrow$ Il pleut.
(2) La rue est mouillée. $\Leftarrow$ Il pleut.
(3) Je reçois les points ECTS. $\Leftarrow$ Je réussis l'examen.
(4) $2x = 2 \ \Leftarrow \ x = 1$
(5) $x^2 = 1 \ \Leftarrow \ x = 1$
(6) $2x = 4 \ \Leftarrow \ x = 1$ (c'est encore faux (!), mais c'est une assertion).

Si A et B sont des assertions, l'implication $\Leftarrow$ est une assertion de la forme

$$A \Leftarrow B,$$

qui signifie : si B est vraie, alors A est vraie. Comme ci-dessus, elle ne dit pas (! !) que B est vraie ! **Attention :** « $A \Rightarrow B$ » 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.*

L'équivalence $\Leftrightarrow$

Le symbole $\Leftrightarrow$ indique l'équivalence ; il se dit « est équivalent à », « si et seulement si », etc. Il est employé si les deux implications $\Rightarrow$ et $\Leftarrow$ sont vraies en même temps.

(1) Je reçois les points ECTS si et seulement si je réussis l'examen.
(2) On a $2x = 2$, si et seulement si $x = 1$. (On suppose ici que x est un nombre réel.)
(3) On a $x^2 = 1$, si et seulement si $x = 1$ ou $x = -1$. (On suppose ici que x est un nombre réel.)

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, la formalisation :

(1) Je reçois les points ECTS. $\Leftrightarrow$ Je réussis l'examen.
(2) $2x = 2 \Leftrightarrow x = 1$
(3) $x^2 = 1 \Leftrightarrow (x = 1$ ou $x = -1)$

Si A et B sont des assertions, l'équivalence $\Leftrightarrow$ est une assertion de la forme

$$A \Leftrightarrow B,$$

qui signifie : A est vraie si et seulement si B est vraie.
Voici un autre exemple de proposition.

Proposition 2.1. *Soient n, m des entiers relatifs. Alors les assertions suivantes sont équivalentes :*

(i) *n est pair.*

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

Démonstration. Si on démontre une équivalence, il faut démontrer les deux assertions.
« (i) $\Rightarrow$ (ii) » On suppose ici que n est pair. Il existe $q \in \mathbb{Z}$ tel que $n = 2q$. Alors, $n+2m = 2q+2m = 2(q + m)$. Donc $n + 2m$ est pair.
« (i) $\Leftarrow$ (ii) » On suppose maintenant que $n+2m$ est pair. Il existe $q \in \mathbb{Z}$ 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.

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

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 :

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

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'équaltion 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 initiale.

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

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

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 ? ? ? ? ?

3 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, il peut aider d'utiliser le modèle des circuits électriques comme dans le livre de Schichl/Steinbauer.

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

« Et » en mathématiques a la même signification qu'au quotidien : si A et B sont des assertions, l'assertion A et B et vraie si et seulement si A et B sont vraies. Vous pouvez soit écrire le mot « et », soit utiliser le symbole $\wedge$.
Introduisons maintenant le formalisme (facile !) des tables de vérité (v= vraie, f = fausse) :

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

(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.

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

« Ou » en mathématiques a la signification suivante : si A et B sont des assertions, alors l'assertion « A ou B » est vraie si au moins une des assertions A, B est vraie (en particulier, si les deux sont vraies, alors « A ou B » est vraie). Vous pouvez soit écrire le mot « ou », soit utiliser le symbole $\vee$. Voici, la table de vérité qui exprime ce fait :

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.

La négation (symbole : $\neg$)

Si A est une assertion, nous écrivons « non A » ou « $\neg A$ » pour sa négation. La table de vérité de la négation 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** $x \leq 0$

Dans les exemples (3) et (4) nous avons vu que « et » et « ou » sont à échanger lors de la négation. Démontrons ce fait par 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

En fait, dans les tables de vérité nous pouvons considérer les assertions comme des variables qui peuvent avoir une des deux valeurs : « v,f ». On peut exprimer le contenu du tableau précédent comme l'égalité :

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

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 « $x = 1$ ».

Calculs avec les symboles $\vee, \wedge, \neg$

Théorème 3.1. *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) $A \vee f = A$,
$A \wedge v = A$ *;*

(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).*

La démonstration par tables de vérité va être faite dans des exercices.

La contraposée

Soient A et B deux assertions. Alors, l'assertion « $A \Rightarrow B$ » est vraie, si et seulement si « $(\neg A) \Leftarrow (\neg B)$ » est vraie. On appelle l'assertion « $(\neg A) \Leftarrow (\neg B)$ » la *contraposée de* $(A \Rightarrow B)$.

(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 $x \leq 0$) $\Leftrightarrow x \neq 1$

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

Proposition 3.2. *Si* $x^7 + x + 1 = 0$, *alors* $x \neq 1$.

Démonstration. Nous ne cherchons pas à calculer les solutions ce 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 $1^7 + 1 + 1 = 3 \neq 0$. □

Voici un autre exemple de proposition.

Proposition 3.3. *Soit* n *un entier relatif. Alors les assertions suivantes sont équivalentes :*

(i) n *est pair.*

(ii) n^2 *est pair.*

Démonstration. Si on démontre une équivalence, il faut démontrer les deux assertions.
« (i) $\Rightarrow$ (ii) » C'est le contenu de la proposition 1.3.
« (i) $\Leftarrow$ (ii) » La contraposée de l'assertion recherchée est : « Si n est impair, alors n^2 est impair. » Vous avez démontré cette assertion en cours.

□

Attention : Ne pas confondre la contraposée 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.

La table de vérité de l'implication

Finalement, on regarde la table de vérité de l'assertion $(A \Rightarrow B)$.

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

Cette table doit être comprise comme une définition du symbole « $\Rightarrow$ ». 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 3.4. *Soient A, B des assertions. Alors :*

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

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

La démonstration sera faite dans des exercices. La partie (a) de la proposition vérifie ce que nous avons dit sur la contraposée juste avant. La partie (b) donne une explication formelle pour les démonstrations par l'absurde : l'assertion « l'hypothèse A est vraie et la conclusion B est fausse » est fausse. Elle justifie aussi la table de vérité définissant l'implication (« On ne peut pas avoir à la fois A vraie et B fausse »).

4 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 précisément 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.

L'existence $\exists$

Voici quelques exemples d'assertions vraies :

(1) Il y a un étudiant dans cette salle.
(2) Il existe un nombre rationnel x tel que $2x = 2$.
(3) Il existe un et un seul nombre rationnel x tel que $2x = 2$.

(4) Il existe un nombre rationnel x tel que $x^2 = 1$.

(5) Il existe un et un seul nombre rationnel x tel que $x^2 = 1$ et $x > 0$.

« Il existe » veut dire : il existe au moins un. Il peut y en avoir plus qu'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 « $\exists!$ ».
Avec ces symboles les exemples deviennent :

(1) $\exists$ étudiant dans cette salle.

(2) $\exists\, x \in \mathbb{Q}$ t.q. $2x = 2$.

(3) $\exists!\, x \in \mathbb{Q}$ t.q. $2x = 2$.

(4) $\exists\, x \in \mathbb{Q}$ t.q. $x^2 = 1$.

(5) $\exists!\, x \in \mathbb{Q}$ t.q. $x^2 = 1$ et $x > 0$.

En revanche, l'assertion « $\exists!\, x \in \mathbb{Q}$ t.q. $x^2 = 1$ » est fausse.
On remplace souvent le « t.q. » par deux points « : ».
Voici un exemple d'une proposition.

Proposition 4.1. *L'équation*

$$a^2 + b^2 = c^2$$

possède une solution en entiers positifs non nuls.

Démonstration. L'existence peut être montrée par un exemple : $3^2 + 4^2 = 5^2$. □

Pour tout $\forall$

Voici quelques exemples d'assertions vraies :

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

(2) Pour tout nombre rationnel x, on a $x^2 \geq 0$.

Proposition 4.2. *Le carré de tout entier relatif pair est divisible par* 4.

Démonstration. Soit $n = 2m$ un entier pair. Alors $n^2 = 4m^2$ est divisible par 4. □

On utilise le symbole $\forall$ pour « pour tout ». Voici, les exemples de façon plus formels :

(1) $\forall$ étudiant dans cette salle : il étudie à l'Université du Luxembourg.

(2) $\forall\, x \in \mathbb{Q} :\ x^2 \geq 0$.

(3) L'assertion de la proposition 4.2 s'exprime ainsi :

$$\forall\, n \in \mathbb{Z} : (2 \mid n \Rightarrow 4 \mid n^2).$$

Encore une fois la négation

(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 « $\vee$ ».

On peut démontrer qu'une assertion « pour tout » est fausse en donnant un **contrexemple**. Par ex. :
– « Tout nombre impair est un nombre premier. »
Cette assertion est fausse car on a le contrexemple : $9 = 3 \cdot 3$ est impair, mais pas premier.
– « Toutes les équations $x^2 + ax + b = 0$ avec $a, b \in \mathbb{Z}$ possèdent une solution $x \in \mathbb{R}$. »
Cette assertion est aussi fausse car $x^2 + 1 = 0$ ne possède pas de solution x dans $\mathbb{R}$. C'est donc aussi un contrexemple. (L'équation possède deux solutions $i, -i$ dans les nombres complexes ; mais, cela n'était pas la question.)

5 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 :
$A_{1,1}, A_{1,2}, \dots A_{1,e_1}$
$A_{2,1}, A_{2,2}, \dots A_{2,e_2}$
...
$A_{n,1}, A_{n,2}, \dots A_{n,e_n}$
On peut imaginer cet exemple comme une matrice, sauf que la longueur des lignes varie d'une ligne à l'autre.

Définition 5.1. *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 « ... ». 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 :

$$p(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^i.$$

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 5.2. *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.

6 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 6.1 (« 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 $n = 1$:

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

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

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

(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 6.2 (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 6.3. *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 6.4 (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 6.5. *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 6.6.
– *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 6.7. *Pour $n, k \in \mathbb{N}$ et $k \leq n$ nous avons :*

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

Lemme 6.8. *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 6.9 (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 6.10. *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 $1,\dots,n$. Par hypothèse de récurrence, il existe $\binom{n}{k-1}$ possibilités de choisir $k-1$ nombres parmi $1,2,\dots,n$. Donc, il existe $\binom{n}{k-1}$ possibilités de choisir k éléments parmi $1,2,\dots,n+1$ sous la condition que $n+1$ est choisi.

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

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

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

par la formule de Pascal (proposition 6.9).

□

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

Théorème 6.11 (Formule du binôme de Newton)**.** *Soit $n\in\mathbb{N}$. Pour tout a,b (nombres réels, rationnels, complexes, entiers, etc.) nous avons :*

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

Démonstration. Par récurrence.

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

Hérédité : « $n\Rightarrow n+1$ » : Nous supposons que pour $n\in\mathbb{N}$ l'égalité $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$

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 6.9).

□

7 Ensembles

Nous utilisons la notion d'ensemble de Georg Cantor :[2]

> 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.

On peut décrire un ensemble en écrivant ses éléments. Par exemple :
- $\mathcal{A} = \{A, B, C, D, \ldots, X, Y, Z\}$, l'alphabet.
- $\mathcal{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = \{4, 2, 3, 9, 0, 7, 6, 8, 1, 5\}$, l'ensemble des chiffres. Notez pour la dernière égalité qu'un ensemble ne dépend pas de l'ordre dans lequel on écrit ses éléments.

On peut aussi définir des ensembles par des propriétés. Par exemple :
- $\mathcal{X} = \{ \underbrace{xy}_{\text{éléments}} \mid \underbrace{x \in \mathcal{Z}, y \in \mathcal{Z}}_{\text{propriétés}} \} = \{00, 01, 02, 03, \ldots, 99\}$.
- $\mathcal{E} = \{P \mid P \text{ est étudiant(e) de ce cours }\}$, l'ensemble des étudiants de ce cours.

[2] Il y a des subtilités avec les ensembles que vous n'allez pas rencontrer pendant vos études (sauf dans un cours de logique mathématique). Par exemple, la collection de tous les ensembles n'est pas un ensemble.

– $\mathcal{L} = \{P \mid P$ 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 en 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 $]a, b[$ ($]a, b]$).)

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 d'un ensemble.

Par exemple :
– $7 \in \mathbb{R}$
– $7 \in [2, 10]$
– $7 \notin [8, 10]$
– $A \in \mathcal{A}$ (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 $\mathcal{Z}$.)
– $ABC \in \mathcal{B}$
– Henri $\in \mathcal{L}$.
– $\#\mathcal{A} = 26$
– $\#\mathcal{Z} = 10$

Définition 7.1. *Soient A, B des ensembles.*
– *B est appelé* sous-ensemble 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*

$$A \cap B := \{a \mid a \in A, a \in B\}$$

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 $a, b \in \mathbb{N}$.
– $\mathcal{A} \times \mathcal{Z} = \{(A, 0), (A, 1), \ldots, (A, 9), (B, 0), (B, 1), \ldots, (B, 9), (C, 0), \ldots, (Z, 9)\}$.

Lemme 7.2. *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 théorème 3.1.

(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) Avec la même argumentation 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 (b). □

Lemme 7.3. *Soient E un ensemble, A et B des parties de E et $\overline{A} = E \setminus A$ et $\overline{B} = E \setminus B$, les complémentaire 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) $E \setminus (E \setminus A) = A$ *;*

(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) Démontrons d'abord l'implication « $\Rightarrow$ ». On suppose donc $A \subseteq B$ et on veut démontrer $\overline{B} \subseteq \overline{A}$. Pour cela, soit x dans $\overline{B} = E \setminus B$. Supposons par l'absurde que x n'appartient pas à $\overline{A}$. Alors, x

appartient à A, donc à B (par l'hypothèse $A \subseteq B$). Ceci est impossible, car x appartient à $\overline{B}$. On en déduit que x est dans $\overline{A}$ et finalement l'inclusion voulue.

Démontrons maintenant l'implication « $\Leftarrow$ ». On suppose donc $\overline{B} \subseteq \overline{A}$ et on veut démontrer $A \subseteq B$. D'après l'implication « $\Rightarrow$ », l'hypothèse $\overline{B} \subseteq \overline{A}$ implique : $\overline{\overline{A}} \subseteq \overline{\overline{B}}$. Or, d'après le point (b), on a $\overline{\overline{A}} = E \setminus (E \setminus A) = A$ et de même $\overline{\overline{B}} = B$. On obtient donc la conclusion voulue.

(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) :

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

□

8 Applications et fonctions

Définition 8.1. *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.
– *On appelle l'ensemble*

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

le graphe de *f.*
– *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 $f(A)$ 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 antécédent) 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.*

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

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

est vraie. Notez la formulation équivalente : f est injective 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 $f(a) = b$. Notez que f est surjective si et seulement si $f(A) = B$.*
– *L'application f est appelée* bijective *si f est injective et surjective.*

Voici, des exemples :
– $A = \{1, 2, 3\}$, $B = \{X, Y\}$. On définit l'application $f : A \to B$ par $f(1) = X$, $f(2) = Y$, $f(3) = X$.
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 $f(1) = X = f(3)$.
– On peut définir l'application sexe : $\mathcal{L} \to \{\text{homme, femme}\}$ par la règle $\text{sexe}(P) = \text{homme}$ si la personne P de l'ensemble $\mathcal{L}$ de tous les Luxembourgeois est un homme, et $\text{sexe}(P) = \text{femme}$ sinon.
Cette application est surjective : il existe au moins un Luxembourgeois masculin et au moins une Luxembourgeoise (probablement présente dans cette salle). Elle n'est pas injective : il y a plus qu'une Luxembourgeoise ou il y a plus qu'un Luxembourgeois masculin (probablement aussi présents dans cette salle).
L'image réciproque de homme par l'application sexe est l'ensemble de tous les Luxembourgeois masculins.
– Considérons l'application $f : \mathbb{R} \to \mathbb{R}$ donnée par la règle $f(x) = x^2$ pour tout $x \in \mathbb{R}$. 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 $f(\mathbb{R}) = \{x \mid x \in \mathbb{R}, x \geq 0\}$. Alors, f n'est pas surjective. Elle n'est pas injective non plus, puisque $f(-1) = 1 = f(1)$.
L'application

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

est surjective mais pas injective.
L'application

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

est injective mais pas surjective.
L'application

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

est injective et surjective.

– Considérons l'application $f : \mathbb{N} \to \mathbb{N}$ donnée par la règle $f(n) = 2n$ pour tout $n \in \mathbb{N}$.
Son image est $f(\mathbb{N}) = \mathcal{G}$, l'ensemble de tous les nombres naturels 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 $f : \mathbb{N} \to \mathcal{G}$ donnée par la règle $f(n) = 2n$ pour tout $n \in \mathbb{N}$.
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.

Les images directes et réciproques de sous-ensembles vérifient les propriétés suivantes.

Lemme 8.2. *Soient E et F des ensembles et f une application de E dans F.*

1. *Soient A et B des parties de E ; on a :*
   (a) $A \subseteq f^{-1}(f(A))$ *(Attention, on n'a pas toujours égalité ici) ;*
   (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).*
2. *Soient C et D des parties de F ; on a :*
   (a) $f\left(f^{-1}(C)\right) \subseteq C$ *(Attention, on n'a pas toujours égalité ici) ;*
   (b) $C \subseteq D \Rightarrow f^{-1}(C) \subseteq f^{-1}(D)$ *;*
   (c) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ *;*
   (d) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

Démonstration.

1. Soient A et B des parties de E.
   (a) Soit a dans A. Alors on a (par définition de $f(A)$) $f(a) \in f(A)$ donc (par définition de l'image réciproque d'une partie) $a \in f^{-1}(f(A))$. Ceci prouve l'inclusion voulue.
   (b) On suppose $A \subseteq B$ et on veut démontrer $f(A) \subseteq f(B)$. Pour cela, soit y un élément de $f(A)$. Par définition de $f(A)$, il existe un élément a de A vérifiant : $y = f(a)$. Par l'hypothèse $A \subseteq B$, a est aussi un élément de B. On en déduit que $f(a)$, et donc y, appartient à $f(B)$. Ceci prouve l'inclusion voulue.
   (c) Soit y un élément de F ; on a :

$$\begin{aligned} y \in f(A \cup B) &\Leftrightarrow \exists x \in A \cup B, y = f(x) \Leftrightarrow \exists x \in E : x \in A \cup B \wedge y = f(x) \\ &\Leftrightarrow \exists x \in E : (x \in A \vee x \in B) \wedge y = f(x) \\ &\Leftrightarrow \exists x \in E : (x \in A \wedge y = f(x)) \vee (x \in B \wedge y = f(x)) \\ &\Leftrightarrow (\exists x \in A, y = f(x)) \vee (\exists x \in B, y = f(x)) \\ &\Leftrightarrow y \in f(A) \vee y \in f(B) \\ &\Leftrightarrow y \in f(A) \cup f(B). \end{aligned}$$

   Ceci prouve l'égalité des deux ensembles.

(d) Soit y dans $f(A \cap B)$. Alors il existe x dans $A \cap B$ vérifiant $y = f(x)$. Comme x est dans A, on a $y \in f(A)$. De même, comme x est dans B, on a $y \in f(B)$. Ainsi, on a $y \in f(A) \cap f(B)$. Ceci prouve l'inclusion voulue.

2. Soient C et D des parties de F.

(a) Soit y dans $f\big(f^{-1}(C)\big)$. Par définition de l'image directe d'un sous-ensemble, il existe x dans $f^{-1}(C)$ vérifiant $y = f(x)$. Par définition de l'image inverse d'un sous-ensemble, on a $f(x) \in C$, donc $y \in C$. Ceci prouve l'inclusion voulue.

(b) On suppose $C \subseteq D$ et on veut démontrer $f^{-1}(C) \subseteq f^{-1}(D)$. Soit x dans $f^{-1}(C)$. On a donc $f(x) \in C$. Comme on a par hypothèse $C \subseteq D$, $f(x)$ est aussi dans D. Ainsi, x est dans $f^{-1}(D)$. Ceci prouve l'inclusion voulue.

(c) Soit x dans E ; on a :

$$\begin{aligned} x \in f^{-1}(C \cup D) &\Leftrightarrow f(x) \in C \cup D \Leftrightarrow f(x) \in C \vee f(x) \in D \\ &\Leftrightarrow x \in f^{-1}(C) \vee x \in f^{-1}(D) \Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D). \end{aligned}$$

Ceci prouve l'égalité des deux ensembles.

(d) Soit x dans E ; on a :

$$\begin{aligned} x \in f^{-1}(C \cap D) &\Leftrightarrow f(x) \in C \cap D \Leftrightarrow f(x) \in C \wedge f(x) \in D \\ &\Leftrightarrow x \in f^{-1}(C) \wedge x \in f^{-1}(D) \Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D). \end{aligned}$$

Ceci prouve l'égalité des deux ensembles.

□

Définition 8.3. *Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. On appelle*

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

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 8.4 (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 8.5. *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 : Soit $b \in B$. Puisque f est surjective, il existe $a \in A$ telle que $f(a) = b$. D'ailleurs, a est unique puisque si on a $a' \in A$ tel que $f(a') = b$, l'injectivité de f nous permet de conclure de l'égalité $f(a) = b = f(a')$ que $a = a'$. Posons : $g(b) = a$. Il faut vérifier que g a les propriétés requises :
Soit $b \in B$. Nous avons choisi $a \in A$ t.q. $f(a) = b$ et posé $g(b) = a$. Alors :

$$(f \circ g)(b) = f(g(b)) = f(a) = b = \mathrm{id}_B(b).$$

Ce raisonnement est valable pour tout $b \in B$. Nous avons alors démontré que les deux applications $f \circ g$ et id_B sont égales.
Soit $a \in A$. Posons $b := f(a)$. Nous avons choisi $a' \in A$ t.q. $f(a') = b$ et posé $g(b) = a'$. Puisque $f(a) = b = f(a')$, l'injectivité nous donne $a = a'$. Donc :

$$(g \circ f)(a) = g(f(a)) = g(b) = a' = a.$$

Ce raisonnement est valable pour tout $a \in A$. Nous avons alors démontré que les deux applications $g \circ f$ et id_A sont égales.
(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 8.4) 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. □

Lemme 8.6. *Soient A, B, C des ensembles et $f : A \to B$ et $g : B \to C$ des applications. Alors, les assertions suivantes sont vraies :*

(a) $g \circ f$ *est surjective* $\Rightarrow$ g *est surjective.*

(b) $g \circ f$ *est injective* $\Rightarrow$ f *est injective.*

(c) $g \circ f$ *est bijective* $\Rightarrow$ f *est injective et* g *est surjective.*

(d) Si f et g sont toutes les deux injectives (respectivement surjectives, respectivement bijectives), alors $g \circ f$ est injective (respectivement surjective, respectivement bijective).

Démonstration. (a) Si $g \circ f$ est surjective, alors par définition pour tout $c \in C$ il existe $a \in A$ t.q. $(g \circ f)(a) = g(f(a)) = c$. Donc, $b := f(a) \in B$ satisfait $g(b) = c$. Ceci montre que g est surjective.
(b) Soient $c, d \in C$ tels que $f(c) = f(d)$. Donc :

$$(g \circ f)(c) = g(f(c)) = g(f(d)) = (g \circ f)(d).$$

L'injectivité de $g \circ f$ implique par définition $c = d$. Ceci montre l'injectivité de f.
(c) C'est une conséquence directe de (a) et (b).
(d) On suppose d'abord que f et g sont injectives et on veut démontrer que la composée $g \circ f$ est aussi injective. Soient a et a' dans A vérifiant $(g \circ f)(a) = (g \circ f)(a')$. On a donc $g(f(a)) = g(f(a'))$. Par injectivité de g, on obtient $f(a) = f(a')$. Par injectivité de f, on obtient alors $a = a'$. Ceci prouve que $g \circ f$ est injective.
On suppose maintenant que f et g sont surjectives et on veut démontrer que la composée $g \circ f$ est aussi surjective. Soit c dans C ; on veut démontrer qu'il existe a dans A tel que $c = (g \circ f)(a)$. Par surjectivité de g, il existe b dans B vérifiant $c = g(b)$. Par surjectivité de f, il existe a dans A vérifiant $b = f(a)$. On a alors : $c = g(b) = g(f(a)) = (g \circ f)(a)$. Ceci prouve que $g \circ f$ est surjective.
On suppose enfin que f et g sont bijectives et on veut démontrer que la composée $g \circ f$ est aussi bijective. Par hypothèse, f et g sont toutes les deux injectives et toutes les deux surjectives. D'après ce qui précède, on obtient que $g \circ f$ est injective et surjective, donc bijective. □

Corollaire 8.7. *Soient A et B des ensembles et f une application de A dans B. Alors f est bijective si et seulement s'il existe une application g de B dans A vérifiant :* $g \circ f = \mathrm{id}_A$ *et* $f \circ g = \mathrm{id}_B$.

Démonstration. L'expression « si et seulement si » désigne une équivalence ; nous allons démontrer les deux implications.
On suppose d'abord que f est bijjective. Alors l'existence d'une fonction g avec les propriétés du corollaire est donnée par le lemme 8.5. Ceci démontre la première implication.
Pour démontrer la deuxième implication, on suppose qu'il existe une fonction g de B dans A vérifiant : $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. On veut démontrer que f est bijective. On remarque que les fonctions id_A et id_B sont bijectives. La relation $f \circ g = \mathrm{id}_B$, la surjectivité de id_B et la partie (a) du lemme 8.6 donnent que f est surjective. La relation $g \circ f = \mathrm{id}_A$, l'injectivité de id_A et la partie (b) du lemme 8.6 donnent que f est injective. Ainsi, on obtient que f est bijective. □

9 Relations binaires

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

Vocabulaire 9.2. *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 9.3. *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 $((xRy \text{ et } yRx) \Rightarrow x = y)$;*
– transitive *si pour tout (x, y, z) dans $E \times E \times E$ on a $((xRy \text{ et } yRz) \Rightarrow xRz)$;*
– totale *si pour tout (x, y) dans $E \times E$ on a $(xRy$ ou $yRx)$.*

Exemples 9.4.

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

Exemples 9.6.

(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 9.7.
– *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 9.8. *Le plus grand et plus petit élément d'un ensemble ordonné n'existent pas toujours, mais lorsqu'ils existent ils sont uniques.*

Définition 9.9. *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 9.10. *Une partie qui possède un majorant (respectivement un minorant) est dite* majorée *(respectivement* minorée*).*

Relations d'équivalence

Définition et premiers exemples

Définition 9.11. *Soit E un ensemble ; on appelle* relation d'équivalence sur E *une relation binaire sur E qui est réflexive, symétrique et transitive.*

Exemples 9.12.

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

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

(c) 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.

Définitions 9.13. *(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 9.14. *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 9.15. *(a) Pour l'égalité sur un ensemble E, on a : $\bar{x} = \{x\}$.*

(b) 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 9.16. *(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 9.17. *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 9.18. *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 9.19. *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 fleche avec deux pointes $\twoheadrightarrow$, celles qui sont injectives par la flèche $\hookrightarrow$, et les bijections par une tilda 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 $xR_f x'$. 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 $xR_f x'$, 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

10 Les entiers naturels $\mathbb{N}$

Les axiomes de Peano

Définition 10.1. *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 10.2. *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 10.3 (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 10.4. *Soit $(N, S, 0)$ un système des nombres naturels. Alors, $S(N) = N \setminus \{0\}$ (tout $n \in N \setminus \{0\}$ 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 10.5. *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 10.6. *Soit $(N, S, 0)$ un système des nombres naturels. Un sous-ensemble $I \subseteq N$ est appelé* partie initiale *si*

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

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

Lemme 10.7. *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 $S(n) \in I_{S(n)}$. 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) exclue $S(S(n)) = S(n)$ à cause du lemme 10.5, 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 $n \in I_n$. □

Proposition 10.8. *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. Soit $\varphi : N \to N'$ l'application qui satisfait

$$\varphi(0) = 0'$$

et la règle *récursive*

$$\varphi(S(n)) = S'(\varphi(n))$$

pour tout $n \in N \setminus \{0\}$.
Il faut s'en assurer qu'une telle application existe et est unique. L'idée est de poser $\varphi(0) := 0'$ et de définir $\varphi(1) := S'(\varphi(0))$, $\varphi(2) := S'(\varphi(1))$, etc. Nous allons faire ceci de façon formelle en utilisant les parties initiales I_n du lemme 10.7.
Par récurrence, nous allons démontrer l'assertion suivante :

$$A(n) : \ \exists! \varphi_n : I_n \to N' : \ \varphi_n(0) = 0' \wedge \big(\forall\, m \in N : (S(m) \in I_n \Rightarrow \varphi_n(S(m)) = S'(\varphi_n(m))\big).$$

Initialisation : Pour $n = 0$ on pose $\varphi_0(0) = 0'$. L'existence et l'unicité sont claires.

Hérédité : « $A(n) \Rightarrow A(S(n))$ » : On se rappelle que $I_{S(n)} = I_n \sqcup \{S(n)\}$. On pose $\varphi_{S(n)}(m) := \varphi_n(m)$ pour $m \in I_n$ et $\varphi_{S(n)}(S(n)) := S'(\varphi_n(n))$. L'unicité est claire (nous avons définie la valeur de $\varphi_{S(n)}$ pour chacun des éléments de $I_{S(n)}$). Il faut vérifier les propriétés :
- $\varphi_{S(n)}(0) = \varphi_n(0) = 0'$ par hypothèse de récurrence.
- Soit $m \in N$ tel que $S(m) \in I_{S(n)}$. Pour $m = n$, on a $\varphi_{S(n)}(S(n)) = S'(\varphi_n(n))$ par définition. Pour $m \neq n$, on a $\varphi_{S(n)}(S(m)) = \varphi_n(S(m)) = S'(\varphi_n(m))$ par hypothèse de récurrence.

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

$$\varphi(n) := \varphi_n(n).$$

Elle satisfait

– $\varphi(0) = \varphi_0(0) = 0'$,
– pour $n \in N$ on a $\varphi(S(n)) = \varphi_{S(n)}(S(n)) = S'(\varphi_n(n)) = S'(\varphi(n))$.
Nous avons montré l'existence à cause de $N = S(N) \cup \{0\}$ (lemme 10.4). Pour l'unicité on suppose que $\widetilde{\varphi}$ est une deuxième application avec les mêmes propritétés que φ. On considère l'ensemble

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

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

$$\varphi(S(n)) = S'(\varphi(n)) = S'(\widetilde{\varphi}(n)) = \widetilde{\varphi}(S(n)),$$

donc par (PA3) $V = N$, montrant l'unicité.
Les mêmes arguments nous fournissent aussi une unique application

$$\psi : N' \to N \text{ t.q. } \psi(0') = 0 \text{ et } \forall\, n' \in N' \setminus \{0'\} : \psi(S'(n')) = S(\psi(n')).$$

On observe maintenant
– $\psi(\varphi(0)) = \psi(0') = 0$ et par récurrence pour $n \in N$:

$$\psi(\varphi(S(n))) = \psi(S'(\varphi(n))) = S(\psi(\varphi(n))) = S(n).$$

Alors $\psi \circ \varphi = \mathrm{id}_N$.
– $\varphi(\psi(0')) = \varphi(0) = 0'$ et par récurrence pour $n' \in N'$:

$$\varphi(\psi(S'(n'))) = \varphi(S(\psi(n'))) = S'(\varphi(\psi(n'))) = S'(n).$$

Alors $\varphi \circ \psi = \mathrm{id}_{N'}$.
Nous avons vu que ψ est une inverse pour φ. Le corollaire 8.7 implique que φ est une bijection. □

La démonstration précédente est le seul endroit où nous donnons tous les détails pour l'existence et l'unicité d'une fonction définie par une règle récursive.
A cause de l'unicité dans la proposition 10.8 nous allons parler *des nombres naturels* et on les note $(\mathbb{N}, S, 0)$. Plus tard, on n'écrira que $\mathbb{N}$.

Addition et multiplication

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

Proposition 10.9. *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) $\forall\, m \in \mathbb{N}, \forall\, n \in \mathbb{N} : m + S(n) = f(m, S(n)) = S(f(m, n)) = S(m + n)$.

Esquisse de la démonstration. Soit $m \in \mathbb{N}$. Nous définissons l'application $f_m : \mathbb{N} \to \mathbb{N}$ récursivement par

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

Des arguments très similaires à ceux de la construction et l'unicité de φ dans démonstration de la proposition 10.8 montrent l'existence et l'unicité de f_m.
Pour finir la preuve, nous posons $f(m,n) := f_m(n)$. Les deux propriétés sont satisfaites par construction. □

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 10.10. *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) $m + 0 = f(m, 0) = f_m(0) = m$ est vrai par définition. L'égalité $m = 0 + m$ se démontre par récurrence.

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

Hérédité : « $m \Rightarrow m + 1$ » : $0 + S(m) = f_0(S(m)) = S(f_0(m)) = S(0 + m) = S(m)$.

(b) On démontre d'abord pour tout $m, n \in \mathbb{N}$ que $S(m) + n = f(S(m), n) = S(f(m, n)) = S(m + n)$. Soit $m \in \mathbb{N}$. Récurrence pour $n \in \mathbb{N}$:

Initialisation : $S(m) + 0 = S(m) = S(m + 0)$.

Hérédité : « $n \Rightarrow n + 1$ » : $S(m) + S(n) = f(S(m), S(n)) = S(f(S(m), n)) = S(S(f(m, n))) = S(f(m, S(n))) = S(m + S(n))$.

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

Initialisation : $m + 0 = 0 + m$.

Hérédité : « $n \Rightarrow n + 1$ » : $m + S(n) = f(m, S(n)) = S(f(m, n)) = S(m + n) = S(n + m) = S(n) + m$ où la dernière égalité provient de l'assertion précédente.

(c) Exercice.
(d) Récurrence pour n.

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

Hérédité : « $n \Rightarrow n+1$ » : Supposons $m+S(n) = \ell+S(n)$. Par définition on a $S(m+n) = S(\ell+n)$. 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 faison une démonstration par l'absurde. Pour cela on suppose (sans perte de généralité à cause de la comuutativité de (b)) $n \neq 0$. Donc $n = S(\ell)$ pour un $\ell \in \mathbb{N}$. En conséqence $0 = m+n = m+S(\ell) = S(m+\ell)$ ce qui contredit $0 \notin S(N)$ (PA1). □

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

Proposition 10.11. *Il existe une unique application (appelée* multiplication*)*

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

(noter que $m \cdot n$ n'est qu'une façon d'écrire $g(m,n)$) telle que
(A1) $\forall\, m \in \mathbb{N} : 0 = g(m,0)$,
(A2) $\forall\, m \in \mathbb{N}, \forall\, n \in \mathbb{N} : m \cdot S(n) = g(m,n) + m = m \cdot n + m$.

Esquisse de la démonstration. Soit $m \in \mathbb{N}$. Nous définissons l'application $g_m : \mathbb{N} \to \mathbb{N}$ récursivement par

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

Des arguments très similaires à ceux de la construction et l'unicité de φ dans démonstration de la proposition 10.8 montrent l'existence et l'unicité de g_m.
Pour finir la preuve, nous posons $g(m,n) := g_m(n)$. Les deux propriétés sont satisfaites par construction. □

Proposition 10.12. *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 10.10. □

La relation d'ordre

Définition 10.13. *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 10.14. *(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) Par récurrence on montre l'assertion $A(n) : n = 0 \vee 1 \leq n$.

Initialisation : $A(0), A(1)$ sont trivialement vraies.

Hérédité : « $(A(n) \Rightarrow A(n+1))$ pour $n \neq 0$ » : L'assertion $A(n)$ nous affirme : $1 \leq n$. Il en suit que $1 \leq 1 + 1 \leq n + 1$.

(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 10.10 (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 10.15. *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. C'est une vérification facile dont nous ne donnons pas les détails ici. Elle peut être faite comme un exercice instructif. □

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

Proposition 10.16 ($\mathbb{N}$ 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 10.14.

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 10.14, $n + 1 \in M$ est le plus petit élément de M.

□

En fait, on peut aussi déduire le principe de récurrence de la proposition 10.16 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 10.17. *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 $\mathcal{M}$. □

Proposition 10.18 (Principe de descente infinie de Fermat)**.** *Il n'existe pas de suite d'entiers naturels strictement décroissante.*

Démonstration. Exercice. □

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 maintenant 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 10.19. *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 : la* cardinalité*) 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.

Exemple 10.20. – $|\emptyset| = 0$ *(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 (exercice).*
– $\mathbb{Z}$ *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).*

Lemme 10.21. *Soient $n, m \in \mathbb{N}$ deux nombres naturels distincts. Alors, il n'existe pas de bijection entre les ensembles E_n et E_m. Donc E_n et E_m n'ont pas le même cardinal.*

Démonstration. On fait une récurrence pour démontrer l'assertion :

$$A(n) : \forall\, k \in \mathbb{N} : \text{ il n'existe pas de bijection } E_{n+k+1} \to E_n$$

pour tout $n \in \mathbb{N}$.

Initialisation : Pour $n = 0$ on a $E_0 = \emptyset$ et $\forall\, k \in \mathbb{N} : E_{k+1} \neq \emptyset$, donc $A(0)$ est vraie car il n'existe pas de bijection entre l'ensemble vide et un ensemble non vide.

Hérédité : « $A(n) \Rightarrow A(n+1)$ » : Supposons donc que pour $n \in \mathbb{N}$ l'assertion $A(n)$ est vraie. Supposons aussi qu'il existe une bijection $f : E_{n+k+2} \to E_{n+1}$ pour un $k \in \mathbb{N}$. On écrit $a := f(n+k+2)$. On définit l'application qui échange a et $n+1$:

$$h : E_{n+1} \to E_{n+1}, \quad \begin{cases} a \mapsto n+1, \\ n+1 \mapsto a, \\ m \mapsto m \text{ si } m \notin \{a, n+1\}. \end{cases}$$

Elle est bijective. Donc l'application

$$g := h \circ f : E_{n+k+2} \to E_{n+1}$$

est aussi bijective, et on a $g(n+k+2) = n+1$. On définit maintenant la restriction de g à E_{n+k+1} qui prend ses valeurs dans E_n :

$$g' : E_{n+k+1} \to E_n, \quad m \mapsto g(m).$$

Elle est aussi bijective ; ceci contredit l'assertion $A(n)$. Donc, l'assertion $A(n+1)$ est vraie.

Conclusion : Pour tout $n \in \mathbb{N}$ l'assertion $A(n)$ est vraie, donc la proposition est vraie.

□

Proposition 10.22. *Soient E, F deux ensembles finis. Les deux assertions suivantes sont équivalentes :*

(i) $\#E = \#F$.

(ii) Il existe une bijection $f : E \to F$.

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.
« (i) $\Rightarrow$ (ii) » : Comme $n = m$ on peut former la composée $h \circ g^{-1} : E \to F$ qui est une bijection car c'est la composée de deux bijections.
« (ii) $\Rightarrow$ (i) » : Supposons que $f : E \to F$ est une bijection. Donc, la composée $h^{-1} \circ f \circ g : E_m \to E_n$ est une bijection. Par le lemme 10.21 on obtient $n = m$. □

Proposition 10.23. *Soient E, F des ensembles finis. Alors :*

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

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

(c) Si on suppose $\#E = \#F$, alors :
f bijective $\Leftrightarrow$ f injective $\Leftrightarrow$ f surjective.

Attention : Pour $E = F = \mathbb{N}$ les équivalences dans (c) sont fausses.

Démonstration. Exercice. □

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

Proposition 10.24. *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. Il est un bon exercice de démontrer les parties qui n'ont pas été traitées. □

11 Groupes

Le monoïde $(\mathbb{N}, +, 0)$

Les propriétés suivantes des nombres naturels ont été démontrées dans la proposition 10.10.

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 11.1. *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 11.2. *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 11.3.

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

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

Rappelons que nous avons déjà démontré *l'associativité de la composition d'applications* dans le lemme 8.4. 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 corollaire 8.7. 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 11.4. *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 11.5. *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 11.6. *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 11.7. *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 :

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

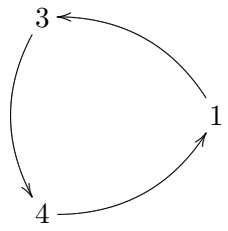
Exemple 11.8. *(a)* $M = \{1, 2, 3, 4, 5, 6\}$.

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

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 : $\big(3 \;\; 4 \;\; 1\big)$ *et* $\big(4 \;\; 1 \;\; 3\big)$. *(Attention ! Le cycle* $\big(1 \;\; 4 \;\; 3\big)$ *est différent : il représente l'application* $1 \mapsto 4, \quad 4 \mapsto 3, \quad 3 \mapsto 1$.*)*
Le cycle qui contient 2 *est* $\big(2 \;\; 6\big)$, *et le cycle qui contient* 5 *est* $\big(5\big)$.
L'écriture en cycles de f *est*

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

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

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

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

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

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

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

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

Définition 11.9.

(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 11.10. *(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 :

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

Définition 11.11. *Un élément $\tau \in S_n$ est appelé* transposition *s'il existe $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$ tels que $\tau = \begin{pmatrix}i & j\end{pmatrix}$.*

Proposition 11.12. *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 $\begin{pmatrix}a_1 & a_2 & a_3 \ldots a_r\end{pmatrix}$ s'écrit comme un produit de transpositions. C'est le cas car :

$$\begin{pmatrix}a_1 & a_2 & a_3 \ldots a_r\end{pmatrix} = \begin{pmatrix}a_r & a_1\end{pmatrix} \circ \begin{pmatrix}a_{r-1} & a_1\end{pmatrix} \circ \cdots \circ \begin{pmatrix}a_3 & a_1\end{pmatrix} \circ \begin{pmatrix}a_2 & a_1\end{pmatrix}.$$

□

12 Les entiers relatifs

Cette section ne sera pas traitée dans le cours. Nous la rajoutons aux notes du cours pour montrer comment les entiers relatifs sont **constuits** à partir des entiers naturels. Donc vous pouvez vous convaincre à l'aide de cette section que les entiers relatifs ont aussi une fondation solide.

Construction de $\mathbb{Z}$

But : Construction formelle de $\mathbb{Z}$ avec addition et multiplication.
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 12.1. *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 10. □

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 12.2. *Soit $\mathcal{Z}$ l'ensemble quotient de $\mathbb{N}$ par la relation d'équivalence définie dans le lemme 12.1.*

(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 $(\mathbb{N}, +, 0)$:

$$\begin{aligned}(\overline{(a, b)} +_{\mathcal{Z}} \overline{(c, d)}) +_{\mathcal{Z}} \overline{(e, f)} &= \overline{(a + c, b + d)} + \overline{(e, f)} = \overline{((a + c) + e, (b + d) + f)} \\ \overset{\text{assoc. de}\mathbb{N}}{=} \overline{(a + (c + e), b + (d + f))} &= \overline{(a, b)} +_{\mathcal{Z}} \overline{(c + e, d + f)} = \overline{(a, b)} +_{\mathcal{Z}} (\overline{(c, d)} +_{\mathcal{Z}} \overline{(e, f)}).\end{aligned}$$

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 12.3. *Pour tout* $\overline{a-b} = \overline{(a,b)} \in \mathcal{Z} \backslash i(\mathbb{N})$ *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 12.4. *(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 12.5. *(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 12.6. *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 $n \in \mathbb{N}$).

13 Anneaux

Les entiers relatifs $\mathbb{Z}$ sont un ensemble avec deux lois, l'addition et la multiplication,

$$\begin{aligned}
+ &: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a,b) \mapsto a+b, \\
\cdot &: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a,b) \mapsto a \cdot b,
\end{aligned}$$

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 exemples 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 13.1. *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 fait également la convention que la multiplication doit toujours être éxécutée avant l'addition : $a + b \cdot c = a + (b \cdot c)$.

Lemme 13.2. *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 13.3. *D'autres exemples d'anneaux sont :*
– *$(\mathbb{Q}, +, \cdot, 0, 1)$ est un anneau commutatif. Voir la section 15 pour une construction formelle.*

– $(\mathbb{R}, +, \cdot, 0, 1)$ *est un anneau commutatif. Il est connu des cours d'analyse et d'algèbre linéaire. Voir la fin de la section 15 pour 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 13.4. *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 13.5. $\mathbb{Z}^\times = \{-1, 1\}$.

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 $\mathbb{Q}$ est l'objet de la section 15 (qui ne sera pas traitée en cours). 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 13.6. *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 10.12. 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 13.7. *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 13.8. *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 13.9. *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 13.10.
– $(\mathbb{Q}, +, \cdot, 0, 1)$ *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 13.11. *Soit $(A, +, \cdot, 0, 1)$ un corps. Alors, A est un anneau intègre.*

Démonstration. Exercice. □

14 L'anneau des entiers relatifs revisité

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^{123} est 7 ;
– 3^{2012} est 3. Effectivement, $3^{2013} =$

$$\begin{array}{c}
27866713376602130822679197147504591347876064921551320632834027306540487600302685399136705830940679830533980891007304258068397344387903485734311233939245359853350672845621926865630984618644414120188914535174041778796721487194530816\\
94324657596637081838927198183223795601985217806377146773173971774454690265778357048302831091424814607519400511444574229008283009956853759080353505491697617383558658631394097310235950400194290557589875213356506804044034529194186645\\
43244373907525256438590973477105885307366458520642779949580502841735099300151805094266571470269023203372385066060381523437995644778055486711170504764227379068465248657755052438393829855079042137547654012694236859045604629436879481962714924868939015324504746928077473164998935884135550360007363208349762222536510310845211484412738180896011956145411234589178695439995100776731225317623717190795682025855273988741445018520042845424552955912662553425080560376276718\\
166892440831676080753782158065190337143 23
\end{array}$$

– (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 14.1. *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 13.5, 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 14.2 (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 14.3. *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 14.4. *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 14.5. *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 14.6. *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 14.7. *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 14.6 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 14.8. *(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 14.9. *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 14.10. *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 14.11. $r_0 = 99$ *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 14.12. *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 14.13. *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 $((x \mid n$ et $y \mid n) \Rightarrow m \mid n)$.*

Proposition 14.14. *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 14.15. *Soit $n \in \mathbb{N}_{>1}$. Soit $x \in \mathbb{Z}$ tel que $\operatorname{pgcd}(x, n) = 1 = ax + bn$ 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 14.16. *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*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \mid x \in \mathbb{Z}, \operatorname{pgcd}(x, n) = 1\}.$$

Démonstration. Dans le lemme 14.15 nous avons vu que toutes les classes $\overline{x}$ pour $x \in \mathbb{Z}$ tel que $\operatorname{pgcd}(x, n) = 1$ 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 14.17. *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 14.16 $\overline{a} \neq \overline{0}$ 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 $\operatorname{pgcd}(a, n) = 1$, 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. Dans le prochain semestre cette caractérisation va nous servir comme 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 14.18. *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 14.19. *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 14.18. 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 14.18 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 14.20. *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 14.1 (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 14.21 (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 14.20 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

$$p_1 p_2 \dots p_r = n = q_1 q_2 \dots q_s.$$

Comme $p_1 \mid n$, il suit du corollaire 14.19 qu'il existe un $j \in \{1, \dots, s\}$ 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

$$p_2 \dots p_r = \frac{n}{p_1} = q_1 q_2 \dots q_{j-1} q_{j+1} \dots q_s.$$

Comme $1 \leq \frac{n}{p_1} < n$, par hérédité $r - 1 = s - 1$ (donc $r = s$) et il existe une bijection $\sigma : \{1, \dots, j-1, j+1, \dots, r\} \to \{2, 3, \dots, r\}$ telle que $q_i = p_{\sigma(i)}$ pour tout $i \in \{1, \dots, j-1, j+1, \dots, r\}$. Nous prolongeons $\sigma : \{1, \dots, r\} \to \{1, \dots, r\}$ en posant $\sigma(j) = 1$. Evidemment, σ est une bijection. □

15 Les nombres rationnels

Cette section ne sera pas traitée dans le cours. Nous la rajoutons aux notes du cours pour montrer 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 15.1. *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.

Réflexivité $(a, x) \sim (a, x)$ parce que $ax = ax$.

Symétrie Si $(a, x) \sim (b, y)$, alors $ay = bx$, donc $bx = ay$, donc $(b, y) \sim (a, x)$.

Transitivité Soient $(a, x) \sim (b, y)$ et $(b, y) \sim (c, z)$. Alors, $ay = bx$ et $bz = cy$. Donc $ayz = bxz$ et $bxz = cyx$, donc $ayz = cyx$, donc par la proposition 13.8 on obtient $az = cx$, donc $(a, x) \sim (c, z)$.

□

Proposition 15.2. *Soit $\mathbb{Q}$ l'ensemble quotient du lemme 15.1.*

(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. Nous démontrons (a) pour $+$; le reste est un exercice.
Supposons $(a, x) = (a', x')$ et $(b, y) = (b', y')$, donc $ax' = a'x$ et $by' = b'y$. On calcule

$$(ay + bx)x'y' = ax'yy' + by'xx' = a'xyy' + b'yxx' = (a'y' + b'x')xy,$$

donc $(ay + bx, xy) \sim (a'y' + b'x', x'y')$. □

L'ordre naturel sur $\mathbb{Q}$

Définition-Lemme 15.3. *(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 15.4. *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 15.5. *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 15.6. *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 en 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 15.7 (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.

16 Sous-groupes et homomorphismes

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 à 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 et des applications entre groupes qui « respectent » l'opération de groupes : les homomorphismes. D'abord les 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 16.1. *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 16.2. – *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 $(\mathbb{Z}, +, 0)$.*
– *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 3 lettres. L'ensemble $H := \{(1\ \ 2\ \ 3), (1\ \ 3\ \ 2), (1)\}$ en 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 16.3. *Soit $(G, \star, e)$ un groupe et $H \leq G$ un sous-groupe. Alors, $(H, \star, e)$ est un groupe.*

Démonstration. 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. □

Le lemme prochain donne un critère qui permet souvent de raccourcir la preuve qu'un sous-ensemble donné est un sous-groupe.

Lemme 16.4 (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 16.5. *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 16.6. *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 16.7. – *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 16.8. *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 16.9. *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 16.10. *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 16.4 : $g^n \star (g^m)^{-1} = g^{n-m} \in H$. 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. Pour cela, nous devons d'abord considérer des intersections de sous-groupes d'un groupe.

Lemme 16.11. *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 16.4 H est un sous-groupe de G.

□

Définition-Lemme 16.12. *Soient $(G, \star, e)$ un groupe et $M \subseteq G$ un sous-ensemble. On pose $\langle M \rangle := \bigcap_{H \leq G, M \subseteq H} H$, l'intersection de tous les sous-groupes H de G qui contiennent M.*
Alors, $\langle M \rangle$ est un sous-groupe de G qui est engendré par M. Pour cette raison on l'appelle aussi le sous-groupe de G engendré par M.

Démonstration. Nous savons du lemme 16.11 que $\langle M \rangle$ est un groupe. Il contient M par définition. Soit $H \leq \langle M \rangle$ un sous-groupe qui contient M. Donc H est aussi un sous-groupe de G. Alors, H fait partie des groupes dont $\langle M \rangle$ est l'intersection. En conséquence $\langle M \rangle \subseteq H$. En tout nous avons $H \subseteq \langle M \rangle \subseteq H$, donc $H = \langle M \rangle$. Nous avons donc vérifié la définition et concluons que $\langle M \rangle$ est engendré par M. □

Si G est cyclique, il est engendré par un seul élément g et tout élément s'écrit comme g^n pour un $n \in \mathbb{Z}$ (noter que le n n'est pas unique en général). Nous allons généraliser ceci à un ensemble de générateurs quelconque. Attention, la description explicite du groupe engendré est peut-être différente de celle qu'on pourrait attendre (sans avoir regardé les détails).

Proposition 16.13. *Soit $(G, \star, e)$ un groupe, $M \subseteq G$ un sous-ensemble et $\langle M \rangle$ le sous-groupe de G engendré par M. Alors*

$$\langle M \rangle = \{x_1^{\epsilon_1} \star x_2^{\epsilon_2} \star \cdots \star x_n^{\epsilon_n} \mid n \in \mathbb{N}, x_i \in M, \epsilon_i \in \{-1, 1\}\}.$$

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.

Démonstration. Soit H l'ensemble à droite de l'égalité dans l'assertion. Il est clair que $M \subseteq H$ et $H \subseteq \langle M \rangle$, parce que $\langle M \rangle$ est un groupe.
Nous montrons par le lemme 16.4 que H est un sous-groupe de G : 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 H. 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 H. Donc, H est un sous-groupe de G.
Alors, H fait partie des groupes dont $\langle M \rangle$ est l'intersection. En conséquence $\langle M \rangle \subseteq H$. En tout nous avons $H \subseteq \langle M \rangle \subseteq H$, donc $H = \langle M \rangle$. Nous avons donc vérifié la définition et concluons que $\langle M \rangle$ est engendré par M. □

Homomorphismes

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 16.14. – *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 16.15. *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 16.16. – $c : \mathbb{Z} \to \mathbb{Z}$*, 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 14.6.*
– *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 16.17. *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 16.18. *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 $\{m \mid n \text{ divise } m\}$*, l'ensemble des multiples de* n.

Définition-Lemme 16.19. *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 16.20 (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 16.4 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 16.4 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 16.21. *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) Soient $g_1, g_2 \in G$*. Les assertions suivantes sont équivalentes :*

(i) $\varphi(g_1) = \varphi(g_2)$.

(ii) $g_1 \star g_2^{-1} \in \ker(\varphi)$.

(iii) Il existe $k \in \ker(\varphi)$ *tel que* $g_1 = k \star g_2$.

(c) 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 (c).
(b) « (i) $\Rightarrow$ (ii) » : Soient $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$. On a

$$\epsilon = \varphi(g_1) \circ \varphi(g_1)^{-1} = \varphi(g_1) \circ \varphi(g_2)^{-1} = \varphi(g_1 \star g_2^{-1}).$$

Donc, $g_1 \star g_2^{-1} \in \ker(\varphi)$.
« (ii) $\Rightarrow$ (iii) » : Prendre $k := g_1 \star g_2^{-1}$.
« (iii) $\Rightarrow$ (i) » : Soit $k \in \ker(\varphi)$ tel que $g_1 = k \star g_2$. Alors :

$$\varphi(g_1) = \varphi(k \star g_2) = \varphi(k) \circ \varphi(g_2) = \epsilon \circ \varphi(g_2) = \varphi(g_2).$$

(c) est une conséquence directe de (b). □

Définition 16.22. *Un homomorphisme de groupes qui est bijectif est appelé un* isomorphisme.
Parfois on appelle un homomorphisme injectif un monomorphisme *et un homomorphisme surjectif un* epimorphisme. *(Nous n'allons pas utiliser ces deux derniers termes.)*

Lemme 16.23. *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 16.24. *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 16.25 (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. □

Chapitre III

Objets de base de l'algèbre linéaire abstraite

17 Espaces vectoriels

Dans votre cours d'algèbre linéaire vous avez déjà beaucoup travaillé avec des espaces vectoriels, peut-être sans les nommer ainsi. 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 17.1. *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) $\forall\, a, b \in K, \forall v \in V : (a \cdot_K b) \cdot_V v = (a \cdot_K b) \cdot_V v$,

(SM4) $\forall\, v \in V : 1_K \cdot_V v = v$.

Notation 17.2. *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 17.3. *(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 habituelle de $\mathbb{C}$ (on regarde donc le nombre réel x comme un nombre complexe).

Notation 17.4 (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 17.5. *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. □

Pour la plupart du temps, on n'écrira pas les indices, mais seulement $f + g$, $f \cdot g$, etc.

Exemple 17.6. *(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 17.7. *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). □

18 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 18.1. *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 18.2.
– *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 $W = \{\binom{a}{0} \mid a \in \mathbb{R}\} \subseteq V$. Alors, W est un sous-espace de V.*
– *Soient $V = \mathbb{R}^3$ et $W = \left\{ \begin{pmatrix} a \\ b \\ 2b \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq V$. Alors, W est un sous-espace de V.*

Lemme 18.3. *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) ⇒ (ii) » : Pour voir que $(W, +, 0)$ est un sous-groupe de $(V, +, 0)$ on utilise le lemme 16.4 : 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) ⇒ (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 18.4. *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 18.5. *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 18.6. *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 16.9).*

Définition-Lemme 18.7. *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 16.12. □

Définition 18.8. *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 18.9. *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 16.13.)

(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 18.10. *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 $I = \{1, \ldots, n\}$, 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 18.11. *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) ⇒ (ii) » : L'existence de tels $w_i \in W_i$ provient de la proposition 18.9 (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 $W_i \cap \sum_{j\in I\setminus\{i\}} W_j = 0$. □

19 Bases et dimension

Bases

Définition 19.1. *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 19.2. *Soit K un corps et $d \in \mathbb{N}_{>0}$. On pose* $e_1 = \begin{pmatrix} 1\\0\\0\\\vdots\\0\end{pmatrix}, e_2 = \begin{pmatrix} 0\\1\\0\\\vdots\\0\end{pmatrix}, \dots, e_d = \begin{pmatrix} 0\\0\\0\\\vdots\\1\end{pmatrix}$ *et* $E = \{e_1, e_2, \dots, e_d\}$. *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 19.3. *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 $e \notin E$, 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 $a_i = -1$:

$$0 = \sum_{i=1}^{n} a_i e_i.$$

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) ⇒ (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) ⇒ (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 19.4. *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 19.3. □

Dans le cours Algèbre 2 nous allons démontrer à l'aide du lemme de Zorn que tout espace vectoriel possède une base.

Exemple 19.5. *(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 19.6. *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

$$0 = b(\sum_{i=1}^{n} a_i e_i \in V) + \sum_{i=1, i\neq j}^{n} b_i e_i = b a_j e_j + \sum_{i=1, i\neq j}^{n} (a_i + b_i) e_i.$$

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 19.7 (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. Cela nous permet d'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 19.6 nous permet de changer e_j en w_r. Cela finit la preuve. □

Corollaire 19.8. *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 19.7 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'ils ont la même cardinalité. □

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 19.9. *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 19.10. *(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 19.11. *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 $C = \{w_1, \ldots, w_r\}$ une K-base de W. Comme C est K-linéairement indépendant, la proposition 19.7 implique $r \leq n$. 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 19.12 (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 19.7.)*
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 19.4 nous permet de choisir une K-base B parmi les éléments de E. Par la proposition 19.7 nous échangeons des éléments de B par $e_1, \ldots, e_r$ en gardant une K-base. □

La proposition 19.12 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 19.11 (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.

20 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 20.1. *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 une tilda : $\varphi : V \xrightarrow{\sim} W$. S'il existe un isomorphisme $V \to W$ on écrit souvent simplement $V \cong W$.*

Remarque 20.2. *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 20.3. *(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 20.4. *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 20.5. *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 vraie pour toute application, donc en particulier pour les applications K-linéaires.
(d) Cela est vraie pour tout homomorphisme de groupes, donc par la remarque 20.2 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 20.3 (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 20.6. *Soient K un corps, V un K-espace vectoriel et $S = \{v_1, \dots, v_n\}$ une K-base de V. Nous rappelons que l'on a $v = \sum_{i=1}^{n} b_i v_i$ avec des uniques $b_1, \dots, b_n \in K$; 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 20.7. *(a) Soient K un corps, $n \in \mathbb{N}$ et $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$. Donc $E = \{e_1, e_2, \dots, e_n\}$ 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 $v = \binom{3}{2} \in V$. Alors, $v = 3 \cdot \binom{1}{1} + \binom{1}{-1}$, donc $v_S = \binom{3}{1}$.

Proposition 20.8. *Soient K un corps et V un K-espace vectoriel de dimension finie n avec K-base $S = \{v_1, \dots, v_n\}$.*
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 20.9. *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 :

$$M_{T,S}(\varphi) \circ (v_i)_S = M_{T,S}(\varphi) := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \circ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,i} \\ a_{2,i} \\ \vdots \\ a_{m,i} \end{pmatrix} = (\varphi(v_i))_T,$$

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

$$M_{T,S}(\varphi) \circ (\sum_{i=1}^{n} b_i v_i)_S = \sum_{i=1}^{n} b_i \cdot \big(M_{T,S}(\varphi) \circ (v_i)_S\big)$$
$$= \sum_{i=1}^{n} b_i \cdot (\varphi(v_i))_T = (\sum_{i=1}^{n} b_i \cdot \varphi(v_i))_T = (\varphi(\sum_{i=1}^{n} b_i \cdot v_i))_T = (\varphi(v))_T.$$

Cela montre le théorème. □

Exemple 20.10. *$\mathbb{C}$ 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 20.11. *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 20.12. *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 et 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 20.13. *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 $C_{S_1,S_2} \circ C_{S_2,S_1}$ est l'identité. Le même raisonnement marche avec les rôles de S_1 et S_2 inversés. □

Proposition 20.14. *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 20.15. *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 mot : le produit matriciel correspond à la composition d'applications.

Démonstration. $M_{U,T}(\psi) \circ M_{T,S}(\varphi) \circ v_S = M_{U,T}(\psi) \circ (\varphi(v))_T = (\psi(\phi(v)))_U = M_{U,T}(\psi \circ \varphi) \circ v_S$. □

Chapitre IV

Débuts de la théorie des groupes

21 Sous-groupes normaux et quotients de groupes

Nous connaissons déjà la construction d'un groupe quotient : $\mathbb{Z}/n\mathbb{Z}$ est le quotient du groupe $(\mathbb{Z}, +, 0)$ par le sous-groupe (normal – voir plus bas) $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.
Avant tout, un avertissement : on peut construire un groupe quotient seulement pour les sous-groupes qui seront appelés normaux (ou distingués). Nous commençons quand-même dans le cadre général et ne spécialisons aux sous-groupes normaux qu'au dernier moment car la construction générale nous mène par exemple au théorème important de Lagrange.
À 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 21.1. *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 9.16). □

Exemple 21.2. *$\mathbb{Z}/n\mathbb{Z}$ 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 14.5 nous avons défini la relation d'équivalence

$$xR_n y \Leftrightarrow x \equiv y \pmod{n}.$$

Nous avons

$$x \equiv y \pmod{n} \Leftrightarrow x - y \in n\mathbb{Z}.$$

Donc la relation d'équivalence définie dans 14.5 est la même que celle de 21.1.

Définition-Lemme 21.3. *Soit G un groupe et $H \leq G$ un sous-groupe.*

(a) De la même manière que dans la définition-lemme 21.1 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 21.4. *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 21.5. *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 21.6 (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 21.4.
Plus précisement, on va distinguer les cas $\#G = \infty$ et $\#G < \infty$. Si $\#G = \infty$, il suit de la rénunion 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 fini. La formule est maintenant claire. □

Corollaire 21.7. *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 21.6 $\#G = (G : H) \cdot \#H$ car l'indice est entier. □

Exemple 21.8. *(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.

Définition 21.9. *Soit G un groupe et $H \leq G$ un sous-groupe. On appelle H un* sous-groupe normal *ou* distingué *si $gH = Hg$ pour tout $g \in G$. Notation : $H \trianglelefteq G$.*
Dans ce cas il est donc inutile de faire la distinction entre classes à gauche et classes à droite, et nous parlerons seulement de classes suivant H.

Exemple 21.10. *Soit G un groupe abélien. Tout sous-groupe $H \leq G$ est normal.*
Raison : La commutativité implique directement $gH = Hg$.

Lemme 21.11. *Soit G un groupe et $H \leq G$ un sous-groupe. Les assertions suivantes sont équivalentes :*

(i) $H \trianglelefteq G$

(ii) $\forall\, g \in G : gHg^{-1} = H$

(iii) $\forall\, g \in G : gHg^{-1} \subseteq H$

(iv) $\forall\, g \in G\, \forall\, h \in H : ghg^{-1} \in H$.

Démonstration. Toutes les implications sont triviales sauf « (iv) ⇒ (i) ».
Donc nous supposons $gHg^{-1} \subseteq H$, ce qui implique $gH \subseteq Hg$ (multiplication par g à droite). Maintenant, on prend l'inverse des deux côtés de $gHg^{-1} \subseteq H$ et on obtient $g^{-1}Hg \subseteq H$, alors $Hg \subseteq gH$ (multiplication par g à gauche). Ayant vu $gH \subseteq Hg$ et $Hg \subseteq gH$, on conclut $gH = Hg$. □

Proposition 21.12. *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.

(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. □

Exemple 21.13. *Soit $n \in \mathbb{N}$. Le groupe alterné A_n (voir la définition-lemme 16.19) est un sous-groupe normal du groupe symétrique S_n.*
Raison : Il est le noyau de l'homomorphisme de groupe $S_n \to \{+1, -1\}$ appelé signature.

Proposition 21.14. *Soit $(G, \cdot, 1)$ un groupe et $N \trianglelefteq G$ un sous-groupe normal.*

(a) Soient $g_1N = g_2N, h_1N = h_2N \in G/N$ des classes de G suivant N. Alors, $(g_1h_1)N = (g_2h_2)N$.

(b) (a) permet de définir l'application

$$\star : G/N \times G/N \to G/N, \quad (gN, hN) \mapsto gN \star hN := (gh)N.$$

(c) $(G/N, \star, N)$ est un groupe, appelé quotient de G par N.

(d) 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) On a $g_1^{-1}g_2 =: n_1 \in N$ et $h_1^{-1}h_2 =: n_2 \in N$ et $h_1^{-1}n_1h_1 = n_3 \in N$. Donc

$$(g_1h_1)^{-1}(g_2h_2) = h_1^{-1}(g_1^{-1}g_2)h_2 = h_1^{-1}n_1h_2 = (h_1^{-1}n_1h_1)h_1^{-1}h_2 = n_3n_2 \in N.$$

(b) En effet, (a) montre que la définition ne dépend pas du choix des représentants.
(c)

Associativité $(g_1N \star g_2N) \star g_3N = (g_1g_2)N \star g_3N = ((g_1g_2)g_3)N = (g_1(g_2g_3))N = g_1N \star (g_2g_3)N = g_1N \star (g_2N \star g_3N)$ pour tout $g_1N, g_2N, g_3N \in G/N$.

Existence du neutre $gN \star N = (g1)N = gN$ pour tout $gN \in G/N$.

Existence d'inverse $gN \star g^{-1}N = (gg^{-1})N = N$ pour tout $gN \in G/N$.

(d)

Surjectivité Clair.

Homomorphisme $\pi(gh) = (gh)N = gN \star hN = \pi(g) \star \pi(h)$ pour tout $g, h \in G$.

Noyau $\pi(g) = gN = N$ si et seulement si $g \in N$.

□

Exemple 21.15. *$(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ est le quotient de $(\mathbb{Z}, +, 0)$ par le sous-groupe normal $(n\mathbb{Z}, +, 0)$.*

Théorème 21.16 (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 9.19.)

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 $\overline{\varphi}(gN) = \varphi(g) = 0$, 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 21.17. *(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.

22 Ordres

Soient G un groupe et $g \in G$. Rappelons la définition de g^n pour tout $n \in \mathbb{Z}$ (voir la définition 16.6 :

$$g^n = \begin{cases} 1 & \text{si } n = 0, \\ \underbrace{g \cdot g \cdot \ldots \cdot g}_{n\text{-fois}} & \text{si } n > 0, \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{|n|\text{-fois}} & \text{si } n < 0. \end{cases}$$

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 22.1. *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 22.2.

– *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 :*

$$\mathrm{ord}\big((1)\big) = 1,\ \ \mathrm{ord}\big((1\ 2)\big) = 2,\ \ \mathrm{ord}\big((1\ 3)\big) = 2,$$
$$\mathrm{ord}\big((2\ 3)\big) = 2,\ \ \mathrm{ord}\big((1\ 2\ 3)\big) = 3,\ \ \mathrm{ord}\big((1\ 3\ 2)\big) = 3.$$

– *Les ordres des éléments de $(\mathbb{Z}/6\mathbb{Z}, +, \overline{0})$ sont les suivants :*

$$\mathrm{ord}(\overline{0}) = 1,\ \ \mathrm{ord}(\overline{1}) = 6,\ \ \mathrm{ord}(\overline{2}) = 3,\ \ \mathrm{ord}(\overline{3}) = 2,\ \ \mathrm{ord}(\overline{4}) = 3,\ \ \mathrm{ord}(\overline{5}) = 6.$$

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 22.3. *Soient G un groupe et $g \in G$.*

(a) On suppose $n = \mathrm{ord}(g) < \infty$. Soit $m \in \mathbb{Z}$ tel que $n \mid m$. Alors, $g^m = 1$.

(b) Soit $m \in \mathbb{N}$ tel que $m < \mathrm{ord}(g)$. Alors, les éléments $1, g, g^2, \ldots, g^m$ sont deux à deux distincts.

Démonstration.
(a) On a $m = nq$ avec $q \in \mathbb{Z}$. Alors, $g^m = g^{nq} = (g^n)^q = 1^q = 1$.
(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 $0 < b - a \leq m < \mathrm{ord}(g)$. □

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 22.4. *Soient G un groupe et $g \in G$. Alors,*

$$\mathrm{ord}(g) = \#\langle g \rangle.$$

En mots : l'ordre du sous-groupe engendré par g est égal à l'ordre de g.

Démonstration. Supposons d'abord que $\mathrm{ord}(g)$ est infini. Alors pour tout $m \in \mathbb{N}$ les éléments $1, g, g^2, \ldots, g^m$ sont distincts par le lemme 22.3 (b), donc $\langle g \rangle$ est un groupe de cardinal infini.
Supposons maintenant $\mathrm{ord}(g) = n < \infty$. Alors les n éléments $1, g, g^2, \ldots, g^{n-1} \in \langle g \rangle$ sont distincts, encore par le lemme 22.3 (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 22.5. *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 21.7 du théorème de Lagrange et la proposition 22.4 on a $\mathrm{ord}(g) = \#\langle g\rangle \mid \#G$. □

Corollaire 22.6 (« 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 22.5 et du lemme 22.3 (a). □

Notons la caractérisation suivante des groupes cycliques finis. Soit G un groupe de cardinal n. Alors, G est cyclique si et seulement s'il existe $g \in G$ tel que $\mathrm{ord}(g) = n$. Cela sera utilisé beaucoup dans ce qui suit.

Corollaire 22.7. *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 22.5) et $\mathrm{ord}(g) \neq 1$, alors $\mathrm{ord}(g) = p$, donc $\langle g\rangle = G$, et G est cyclique. □

Corollaire 22.8. *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 22.9. *Soient G un groupe et $g \in G$. Considérons l'homomorphisme de groupes*

$$\varphi : \mathbb{Z} \to G, \quad m \mapsto g^m.$$

(a) L'image de φ est $\langle g\rangle$.

(b) Soit $m \in \mathbb{Z}$. Alors, $m \in \ker(\varphi) \Leftrightarrow g^m = 1$.

(c) $\mathrm{ord}(g) = \infty \Leftrightarrow \ker(\varphi) = \{0\} \Leftrightarrow \varphi$ est injectif.

(d) Soit $m \in \mathbb{Z}$ tel que $g^m = 1$. Alors, $\mathrm{ord}(g) \mid m$.

(e) Soit $\mathrm{ord}(g) = n < \infty$. Alors, $\ker(\varphi) = n\mathbb{Z}$.

(f) Soit $\mathrm{ord}(g) = n < \infty$. Alors, l'application

$$\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G, \quad \overline{m} \mapsto g^m$$

provenant du 1er théorème d'isomorphisme 21.16 est un homomorphisme de groupes injectif d'image $\langle g\rangle$.

Démonstration. (a) Cela est évident à cause de la déscription $\langle g\rangle = \{g^m \mid m \in \mathbb{Z}\}$.
(b) C'est la définition du noyau appliqué à notre cas.
(c) La deuxième équivalence provient de la proposition 16.21.
« $\Leftarrow$ » : Supposons que $\ker(\varphi) \neq \{0\}$. Donc il existe $m \in \mathbb{N}_{>0} \cap \ker(\varphi)$ tel que $g^m = 1$. Alors, $\mathrm{ord}(g) \leq m < \infty$.
« $\Rightarrow$ » : Supposons que φ est injectif. Alors, φ est un isomorphisme $\mathbb{Z} \to \langle g\rangle$, donc en particulier une bijection. Donc $\langle g\rangle$ est infini, donc $\mathrm{ord}(g) = \infty$ par la proposition 22.4.
(d) Soit $m \in \mathbb{Z}$ tel que $g^m = 1$. Soit $n = \mathrm{ord}(g) \leq |m| < \infty$. Par la division euclidienne nous avons $m = n \cdot q + r$ avec $0 \leq r < n$. On a $1 = g^m = g^{n\cdot q} g^r = (g^n)^q g^r = 1^q g^r = 1g^r = g^r$. Comme $0 \leq r < n$ par la définition de l'ordre la seule possibilité qui reste est $r = 0$, donc $\mathrm{ord}(g) \mid m$.
(e) Le lemme 22.3 (a) nous donne l'inclusion $n\mathbb{Z} \subseteq \ker(\varphi)$. L'autre inclusion est le contenu de (d)
(f) Par (e), on a $\ker(\varphi) = \mathrm{ord}(g)\mathbb{Z}$. Donc, l'assertion suit directement du théorème d'isomorphisme 21.16. □

Corollaire 22.10 (Classification des groupes cycliques)**.** *Soit G un groupe cyclique.*

(a) Si $n = \#G$ est fini, alors G est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$.
(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) Comme $\mathrm{ord}(g) = \#G = n$, l'assertion est le contenu de la proposition 22.9 (f).
(b) L'homomorphisme $\varphi : \mathbb{Z} \to G$ de la proposition 22.9 est injectif par (c) et surjectif par (a). □

Corollaire 22.11. *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 $\mathrm{ord}(g^i) < \infty$. L'ordre de g^i est le plus petit $q \in \mathbb{N}_{\geq 1}$ tel que $(g^i)^q = g^{iq} = 1$. Donc $q = \frac{m}{i}$ où $m \in \mathbb{N}_{\geq 1}$ est minimal tel que
– $g^m = 1$ ($\Leftrightarrow \mathrm{ord}(g) \mid m$ par la proposition 22.9) et
– $i \mid m$.
Alors $m = \mathrm{ppcm}(i, \mathrm{ord}(g))$ et $\mathrm{ord}(g^i) = \frac{m}{i} = \frac{\mathrm{ppcm}(i,\mathrm{ord}(g))}{i} = \frac{\mathrm{ppcm}(i,\mathrm{ord}(g))\cdot \mathrm{pgcd}(i,\mathrm{ord}(g))}{i\cdot \mathrm{pgcd}(i,\mathrm{ord}(g))} = \frac{i\cdot \mathrm{ord}(g)}{i\cdot \mathrm{pgcd}(i,\mathrm{ord}(g))} = \frac{\mathrm{ord}(g)}{\mathrm{pgcd}(i,\mathrm{ord}(g))}$. □

Définition-Lemme 22.12. *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 22.13. *Soient G un groupe abélien fini et $H_1, H_2 \leq H$ 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 22.8), alors, l'application $\phi : H_1 \times H_2 \to G$ donné par $(h_1, h_2) \mapsto h_1 h_2$ est un homomorphisme de groupes injectif.*

Démonstration. **Homomorphisme** On calcule

$$\phi((h_1, h_2)(h_1', h_2')) = \phi((h_1 h_1', h_2 h_2')) = h_1 h_1' h_2 h_2' \overset{\text{abélien}}{=} h_1 h_2 h_1' h_2' = \phi((h_1, h_2))\phi((h_1', h_2')).$$

Injectivité $\phi((h_1, h_2)) = h_1 h_2 = 1$, donc $h_1 = h_2^{-1} \in H_1 \cap H_2 = \{1\}$, donc $h_1 = h_2 = 1$.

□

Exemple 22.14. *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 22.7, 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 22.13 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 23.16 que nous n'avons pas encore démontré, donc il faut faire un peu plus de travail maintenant).
  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 22.13 (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 21.7. 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 $b^2 \in bH$. La deuxième possibilité est impossible (sinon b serait dans H). Donc $b^2 \in H$. Donc $\mathrm{ord}(b^2)$ est 1 ou 3 (par le corollaire 22.11). 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.

23 Compléments

Cette section ne sera pas examinée. On ne donne pas toutes les démonstrations pour raison de manque de temps. Regardez-la quand-même car son contenu pourra être utilisé dans des cours à venir.

Définition 23.1. *Soit $(G, \star, e)$ un groupe. Le* centre de *G est défini comme*

$$\mathcal{Z}(G) := \{g \in G \mid \forall\, h \in G :\ g \star h = h \star g\}.$$

Lemme 23.2. *Soit $(G, \star, e)$ un groupe. Alors le centre $\mathcal{Z}(G)$ est un sous-groupe normal de G.*

Démonstration. Exercice sur la feuille 9 ($\mathcal{Z}(G)$ est un sous-groupe). La normalité est facile. □

Groupes de matrices

Définition 23.3. *Soient K un corps et $n \in \mathbb{N}_{\geq 1}$. On pose*

$$\mathrm{GL}_n(K) = \{M \in \mathrm{Mat}_{n\times n}(K) \mid \exists N \in \mathrm{Mat}_{n\times n}(K) : M \circ N = \mathrm{id}_n\}$$

et $\mathrm{id}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$.
Le groupe linéaire général *est* $(\mathrm{GL}_n(K), \circ, \mathrm{id}_n)$.

Proposition 23.4. *Le déterminant* det *(défini comme en algèbre linéaire) a les propriétés suivantes :*

(a) Une matrice $M \in \mathrm{Mat}_{n\times n}(K)$ est inversible si et seulement si $\det(M) \neq 0$. On a alors

$$\mathrm{GL}_n(K) = \{M \in \mathrm{Mat}_{n\times n}(K) \mid \det(M) \neq 0\}.$$

(b) On rappelle $K^\times = K \setminus \{0\}$. L'application

$$\det : (\mathrm{GL}_n(K), \circ, \mathrm{id}_n) \to (K^\times, \cdot, 1), \quad M \mapsto \det(M)$$

est un homomorphisme de groupes.

(c) Le noyau de $\det$ *est égal à*

$$\mathrm{SL}_n(K) = \{M \in \mathrm{Mat}_{n\times n}(K) \mid \det(M) = 1\}.$$

On appelle $(\mathrm{SL}_n(K), \circ, \mathrm{id}_n)$ *le* groupe spécial linéaire.

Démonstration. Algèbre linéaire. □

Proposition 23.5. *Soient K un corps et $n \in \mathbb{N}_{\geq 1}$. Alors, le centre de* $\mathrm{GL}_n(K)$ *est égal à*

$$\left\{ \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x \end{pmatrix} \mid x \in K^\times \right\}.$$

La classification des groupes abéliens

Corollaire 23.6. *Soit G un groupe cyclique.*

(a) Si $H \leq G$ est un sous-groupe (automatiquement normal car G est abélien), alors le quotient G/H est aussi cyclique.

(b) Tout sous-groupe H de G est aussi cyclique.

Démonstration. Par le corollaire 22.10 nous pouvons supposer $G = \mathbb{Z}$ ou $G = \mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}_{\geq 1}$. Ces cas sont un exercice. □

Lemme 23.7. *Soient G un groupe abélien fini et $g, h \in G$.*

(a) Si $\mathrm{pgcd}(\mathrm{ord}(g), \mathrm{ord}(h)) = 1$, *alors* $\mathrm{ord}(gh) = \mathrm{ord}(g)\,\mathrm{ord}(h)$.

(b) Il existe $i, j \in \mathbb{N}$ tels que $\mathrm{ord}(g^i h^j) = \mathrm{ppcm}(\mathrm{ord}(g), \mathrm{ord}(h))$.

Démonstration. (a) Soit $m := \mathrm{ord}(gh)$. Donc $g^m h^m = 1$ et par $\langle g\rangle \cap \langle h\rangle = \{1\}$ (à cause du corollaire 22.8), on a $g^m = h^m = 1$ Par la proposition 22.9, il en suit que $\mathrm{ord}(g) \mid m$ et $\mathrm{ord}(h) \mid m$, donc $\mathrm{ord}(g)\,\mathrm{ord}(h) \mid m$ (utilisant encore une fois $\mathrm{pgcd}(\mathrm{ord}(g), \mathrm{ord}(h)) = 1$). Il est clair que $(gh)^{\mathrm{ord}(g)\,\mathrm{ord}(h)} = 1$.
(b) Soient

$$\mathrm{ord}(g) = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} \text{ et } \mathrm{ord}(h) = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

les factorisations en nombres premiers (c'est-à-dire, les $p_1, \ldots, p_k$ sont des nombres premiers distincts), où on les trie de la façon que $m_1 \geq n_1, \ldots, m_s \geq n_s$ et $m_{s+1} < n_s, \ldots, m_k < n_k$. Soient

$$g' := g^{p_{s+1}^{m_{s+1}} \cdot \ldots \cdot p_k^{m_k}} \text{ et } h' := h^{p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}}.$$

Par le corollaire 22.11 nous avons

$$\mathrm{ord}(g') = p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \text{ et } \mathrm{ord}(h') = p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k}.$$

Donc, (a) implique que l'ordre de $g'h'$ est

$$p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \cdot p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k} = \mathrm{ppcm}(\mathrm{ord}(g), \mathrm{ord}(h)).$$

□

Définition 23.8. *Soit G un groupe. On considère l'ensemble $M := \{n \in \mathbb{N}_{>0} \mid \forall\, g \in G : g^n = 1\}$. Si $M \neq \emptyset$, alors, on définit* l'exposant du groupe *G comme le plus petit élément dans M. Si $M = \emptyset$, on dit que l'exposant du groupe G est infini. Notation :* $\exp(G)$.

Proposition 23.9. *Soit G un groupe abélien fini.*

(a) Il existe $g \in G$ tel que $\operatorname{ord}(g) = \exp(g)$.

(b) $\exp(g) \mid \#G$.

(c) $\exp(G) = \operatorname{ppcm}(\operatorname{ord}(g) \mid g \in G)$.

(d) G est cyclique $\Leftrightarrow \exp(G) = \#G$.

Démonstration. Soit $n := \operatorname{ppcm}(\operatorname{ord}(g) \mid g \in G)$. Il est clair que $g^n = 1$ pour tout $g \in G$, donc $\exp(G) \leq n$. Le lemme 23.7 (b) montre qu'il existe $g \in G$ tel que $\operatorname{ord}(g) = n$. En conséquence $n \leq \exp(G)$. Toutes les assertions sont maintenant claires. □

Sans démonstration on énonce la classification des groupes abéliens de type fini. La preuve n'est pas très difficile, mais nous n'avons malheureusement plus de temps.

Théorème 23.10 (Classification des groupes abéliens de type fini)**.** *Soit G un groupe abélien de type fini (c'est-à-dire que G peut être engendré par un nombre fini d'éléments). Alors, il existe des uniques $r, s \in \mathbb{N}$ et des uniques $d_1, d_2, \ldots, d_s \in \mathbb{N}_{\geq 2}$ tels que*
– $d_1 \mid d_2 \mid \cdots \mid d_s$ *et*
– $G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$.

Exemple 23.11. *On obtient du théorème 23.10 qu'à isomorphisme près il n'existe que deux groupes abéliens de cardinal* 12*, en l'occurence $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Actions de groupes

Définition 23.12. *Soient E un ensemble et G un groupe.*

(a) 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*
– $\forall x \in E : 1.x = x$.

(b) Soit $x \in E$. L'ensemble $E_x = \{g.x \mid g \in G\}$ s'appelle l'orbite de *x (en anglais : orbit, en allemand : Bahn).*

(c) 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'est un sous-groupe de G.*

(d) L'application

$$\pi : G \to S_E = \{f : E \to E \text{ bijection}\}, \quad g \mapsto \pi_g = (x \mapsto g.x)$$

est un homomorphisme de groupes (S_E est le groupe symétrique). S'il est injectif, on dit que l'opération de G sur E est fidèle *(faithful, treu).*

(e) S'il existe $x \in E$ tel que $E_x = E$, on dit que l'opération de G sur E est transitive.

Exemple 23.13. *Soit G un groupe. G opère sur lui-même par conjugaison :*

$$G \times G \to G, \quad (g,h) \mapsto ghg^{-1}.$$

La proposition la plus importante pour les actions de groupes est la suivante.

Proposition 23.14. *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

$$\forall (x,y) \in E^2,\ x \sim_G y \iff \exists g \in G, y = g \cdot x$$

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.

(b) Pour $x \in E$ on a $\#E_x = (G : G_x)$ (le cardinal de l'orbite est l'indice du stabilisateur).

(c) Soit I l'ensemble des orbites de l'action. Dans toute orbite on choisit un représentant x_i. Alors, on a l'égalité :

$$\#E = \sum_{i \in I} (G : G_{x_i}).$$

Les théorèmes de Sylow

Définition 23.15. *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 $\#H = p^r$.*

Voici le théorème principal sur les sous-groupe de Sylow.

Théorème 23.16. *Soient G un groupe fini et p un nombre premier.*

(a) Si $p \mid \#G$, alors G possède un p-groupe de Sylow.

(b) Tous les p-groupes de Sylow de G sont conjugués, c'est-à-dire, si H_1 et H_2 sont deux p-groupes de Sylow, alors il existe $g \in G$ tel que $gH_1g^{-1} = H_2$.

(c) Soit $U \leq G$ un sous-groupe de cardinal p^k. Alors, il existe un p-groupe de Sylow $H \leq G$ tel que $U \leq H$.

(d) Soit s_p le nombre des p-groupes de Sylow de G. Alors, $s_p \equiv 1 \mod p$.

Plus sur les quotients de groupes

Proposition 23.17. *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 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 $\pi^{-1}(H)$ est en effet un sous-groupe par la proposition 16.20. En plus $\pi^{-1}(H) \supseteq \pi^{-1}(\{1\}) = \ker(\pi) = N$.
– Surjectivité : Soit $U \leq G$ un sous-groupe tel que $N \subseteq U$. Par la proposition 16.20 nous avons $H := \pi(U)$ est un sous-groupe de G/N.
On a : $\Phi(H) = \pi^{-1}(\pi(U)) = U$, donc la surjectivité.
On vérifie la dernière 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 $xu^{-1} \in \ker(\pi) = N \subseteq U$, donc $xu^{-1} = v \in U$, donc $x = uv \in U$.
« $\supseteq$ » : Soit $u \in U$, donc $\pi(u) \in \pi(U)$, donc $u \in \pi^{-1}(\pi(U))$.
– Injectivité : Soient $H_1, H_2 \in G/N$ des sous-groupes tels que $\Phi(H_1) = \Phi(H_2)$. Alors, $\pi^{-1}(H_1) = \pi^{-1}(H_2)$, et donc $H_1 = \pi(\pi^{-1}(H_1)) = \pi(\pi^{-1}(H_2)) = H_2$, montrant l'injectivité.
On vérifie encore l'égalité $H = \pi(\pi^{-1}(H))$ pour tout sous-groupe $H \leq G/N$.
« $\subseteq$ » : 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 $g \in \pi^{-1}(H)$.
(b) est clair.
(c) Proposition 21.12. □

Lemme 23.18. *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 23.19 (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 21.16) 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 23.18 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 21.16. □

Proposition 23.20 (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 21.16) 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 21.16. □

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 1

18/09/2013

Les exercices sont à rendre le 23/09/2013 au début du cours.

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.** *La somme de deux entiers relatifs impairs est* _____.
   Compléter et écrire une démonstration.
2. **Proposition.** *Soit n un entier impair. Alors $n^2 - 1$ est divisible par 8.*
   Écrire une démonstration.
3. **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.
4. (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)

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 2

23/09/2013

Les exercices sont à rendre le 30/09/2013 au début du cours.

---

1. 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 $y = 2$

2. Résoudre dans $\mathbb{Q}$ l'équation $2x(x+1)^2 = x^3 + 4x^2 + 2x + 8$. Utiliser « $\Rightarrow$ », « $\Leftarrow$ » et/ou « $\Leftrightarrow$ » !

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. 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.

5. Écrire la négation des phrases suivantes.

   (a) Adrien parle français et allemand.

   (b) Ce triangle a deux côtés de même longueur.

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. »

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 3

30/09/2013

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé du 03/10/2013.

---

1. 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.

2. Soient A, B et C des assertions. Écrire des tables de vérité pour démontrer :

   (a) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$;

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

3. Soient A, B et C des assertions. Utiliser le théorème 3.1 pour vérifier les assertions suivantes.

   (a) $\neg\big(\neg A \wedge (B \vee A)\big) = A \vee \neg B$;

   (b) $\neg\big((A \vee B) \wedge (B \wedge A)\big) = \neg A \vee \neg B$;

   (c) $\neg\big(A \wedge (\neg(B \vee C))\big) \wedge (A \vee B) = B \vee (A \wedge C)$.

4. Une assertion qui est toujours vraie s'appelle une *tautologie*. Soient A, B et C des assertions ; démontrer que les assertions suivantes sont des tautologies :

   (a) $A \Rightarrow (A \vee B)$;

   (b) $\big(A \wedge (A \Rightarrow B)\big) \Rightarrow B$;

   (c) $\big((A \Rightarrow B) \wedge \neg B\big) \Rightarrow \neg A$;

   (d) $\big((A \Rightarrow B) \wedge (B \Rightarrow C)\big) \Rightarrow (A \Rightarrow C)$.

5. 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) $\exists\, y \in \mathbb{Z} : \forall\, x \in \mathbb{N} : x \geq y$.

Tourner la page, svp.

6. 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.
   (c) (Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction et $x_0 \in \mathbb{R}$. (Cette partie n'est pas à nier))
   $\forall\, \epsilon > 0 : \exists\, \delta > 0 : \forall\, x \in \mathbb{R} : \big(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon\,\big)$.
   Dans votre cours d'Analyse 1 vous verrez que ceci est la définition de la continuité de la fonction f au point x_0.
7. 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.
8. Écrire les expressions suivantes sans utiliser les symboles $\sum$ et $\prod$.

   (a) $\displaystyle\sum_{i=-4}^{-6} i^2$; (b) $\displaystyle\prod_{k=0}^{n} x^{k-2}$; (c) $\displaystyle\prod_{m=1}^{n} m^2$; (d) $\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{m} 1$.

9. 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) $a_1 + 2a_2 + 3a_3 + 3a_1^2 + 6a_2^2 + 9a_3^2 + 9a_1^3 + 18a_2^3 + 27a_3^3 + 27a_1^4 + 54a_2^4 + 81a_3^4$.
10. 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) $\sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j = \sum_{k=0}^{n}\sum_{\ell=0}^{k} a_\ell b_{k-\ell} + \sum_{k=0}^{n}\sum_{\ell=0}^{k} a_{k-\ell} b_\ell$.

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`)

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 4

07/10/2013

Les exercices sont à rendre le 14/10/2013 au début du cours.

1. (a) Démontrer par récurrence :

$$\forall\, n \in \mathbb{N}_{>0} : 1 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

   (b) Soient n dans $\mathbb{N}_{\geq 2}$ et $a_1, \ldots, a_n$ des nombres rationnels (ou réels, ou entiers... cela ne change rien pour l'exercice). Démontrer par récurrence :

$$\sum_{i=2}^{n} (a_i - a_{i-1}) = a_n - a_1.$$

   (c) Soit n dans $\mathbb{N}$. Démontrer, par récurrence finie, que pour tout entier k entre 0 et n on a :

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \prod_{i=1}^{k} \frac{n+1-i}{i}.$$

   (d) Que pensez-vous de la démonstration suivante ?

   Assertion : Soit C un cours avec n participants. Alors tous les participants sont du même sexe.

   Démonstration par récurrence. Si $n = 1$, l'assertion est trivialement vraie. Soit maintenant C un cours avec $n + 1$ participants. Nous attendons jusqu'à ce qu'un des participants, appelons-le A, quitte le cours pour un instant. Par hypothèse de récurrence les n participants restants sont du même sexe s. Après le retour de A, nous faisons sortir un autre participant B pour un instant. Encore par hypothèse de récurrence, les n participants restants sont du même sexe, qui doit encore être s. Donc A, B et les autres participants sont tous du même sexe. □

2. (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) $A \cup B = E \iff E \setminus A \subseteq B \iff E \setminus B \subseteq A$.

Tourner la page, s.v.p.

3. (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 bijective. 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 injectives, alors $g \circ f$ est injective.

   (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.

À propos (Paradoxe de Russell). On ne peut pas faire n'importe quoi avec les ensembles. Par exemple, 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.

Pour lever ce paradoxe, les mathématiciens ont introduit la notion de *catégorie*, mais ceci est une autre histoire.

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 5

14/10/2013

Les exercices sont à rendre le 21/10/2013 au début du cours.

1. (a) Soient E, F des ensembles, $f : E \to F$ une application surjective et $C \subseteq F$ un sous-ensemble. Démontrer : $f(f^{-1}(C)) = C$.
   L'inclusion $f(f^{-1}(C)) \subseteq C$ a déjà été démontrée en cours, il est inutile de la redémontrer.

   (b) Dans cette partie, vous allez voir que les inclusions dans 1(a), 1(d) et 2(a) du lemme 8.2 du cours ne sont pas des égalités en général.

   (i) Écrire explicitement des ensembles E, F, une application $f : E \to F$ et un sous-ensemble $A \subseteq E$ tels que $A \neq f^{-1}(f(A))$.

   (ii) Écrire explicitement des ensembles E, F, une application $f : E \to F$ et des sous-ensembles $A \subseteq E$, $B \subseteq E$ tels que $f(A \cap B) \neq f(A) \cap f(B)$.

   (iii) Écrire explicitement des ensembles E, F, une application $f : E \to F$ et un sous-ensemble $C \subseteq F$ tels que $f(f^{-1}(C)) \neq C$.

   (c) Soient E et F des ensembles. On note $\mathcal{P}(E)$ (respectivement $\mathcal{P}(F)$) l'ensemble de toutes les parties de E (respectivement de F). Donner soit une démonstration soit un contrexemple à chacune des deux assertions suivantes :

   (i) $\mathcal{P}(E \cap F) = \mathcal{P}(E) \cap \mathcal{P}(F)$;

   (ii) $\mathcal{P}(E \cup F) = \mathcal{P}(E) \cup \mathcal{P}(F)$.

2. (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 :

   $$\forall (x, y) \in E \times E,\ xRy \iff \frac{x+y}{2} \in E.$$

   (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 ?

   (c) **Exercice très important**
   Soit n un entier naturel ; on définit sur $\mathbb{Z}$ une relation binaire R_n par :

   $$\forall\, (a, b) \in \mathbb{Z}^2,\ aR_nb \iff n|(a-b).$$

   (1) 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.

   (2) Donner la classe d'équivalence d'un entier relatif pour la relation R_0. Même question pour R_1.

3. **Fonctions caractéristiques**

Soient E et F des ensembles ; on note $\mathcal{P}(E)$ l'ensemble des parties de E et $\mathcal{F}(E,F)$ l'ensemble des fonctions de E dans F.

Soit A une partie de E ; on définit un élément f_A de $\mathcal{F}(E,\{0,1\})$, appelé la *fonction caractéristique* de A, par : $f_A(x)=1$ si $x\in A$ et $f_A(x)=0$ si $x\notin A$.

(a) Démontrer que l'application F de $\mathcal{P}(E)$ dans $\mathcal{F}(E,\{0,1\})$ qui à une partie A de E associe sa fonction caractéristique f_A est bijective.

(b) Pour f et g dans $\mathcal{F}(E,\mathbb{R})$, on note :
- $f+g$ l'application de E dans $\mathbb{R}$ qui envoie tout élément x de E sur $f(x)+g(x)$;
- $f-g$ l'application de E dans $\mathbb{R}$ qui envoie tout élément x de E sur $f(x)-g(x)$;
- $f\times g$ ou $f\cdot g$ l'application de E dans $\mathbb{R}$ qui envoie tout élément x de E sur $f(x)\cdot g(x)$.

On note de plus $\mathbf{1}$ la fonction constante égale à 1 sur E.

Soient A et B des parties de E ; démontrer que les applications $\mathbf{1}-f_A$, $f_A\cdot f_B$ et $f_A+f_B-f_A\cdot f_B$ sont des fonctions caractéristiques de sous-ensembles de E qu'on déterminera.

(c) Écrire la fonction caractéristique du sous-ensemble $A\setminus B$ en fonction de celle de A et celle de B.

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 sixème 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 ?

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 6

21/10/2013

Les exercices sont à rendre le 28/10/2013 au début du cours.

1. (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 $\mathbb{N}$.
2. Soient E et F des ensembles finis. Démontrer les assertions suivantes. *Indication : dans certains cas, on pourra raisonner par récurrence.*
   (a) $\#E \leq \#F \iff$ il existe une injection de E dans F.
   (b) $\#F \leq \#E \iff$ il existe une surjection de E dans F.
   (c) On suppose $\#E = \#F$ et on considère une fonction f de E dans F ; alors :
   f est bijective $\iff$ f est injective $\iff$ f est surjective.
3. 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 : $(m + n) + \ell = m + (n + \ell)$.
   (c) *(Principe de descente infinie de Fermat)* Démontrer qu'il n'existe pas de suite d'entiers naturels strictement décroissante.
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.

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.

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 7

28/10/2013

Les exercices sont à rendre le 04/11/2013 au début du cours.

1. Soit S_4 le groupe symétrique en 4 lettres. Dresser la liste de ses éléments. Utiliser l'écriture en cycles.
2. Faites les calculs suivants dans le groupe S_{10} :
   (a) $\big(1\ \ 3\big)\ \big(2\ \ 7\ \ 4\ \ 10\ \ 9\big) \circ \big(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10\big) = ?$
   (b) $\big(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10\big) \circ \big(1\ \ 3\big)\ \big(2\ \ 7\ \ 4\ \ 10\ \ 9\big) = ?$
   (c) $\big(1\ \ 2\big)\ \big(3\ \ 4\big)\ \big(5\ \ 6\big)\ \big(7\ \ 8\big)\ \big(9\ \ 10\big) \circ \big(1\ \ 10\big)\ \big(2\ \ 3\big)\ \big(4\ \ 5\big)\ \big(6\ \ 7\big)\ \big(8\ \ 9\big) = ?$
3. Trouvez les inverses dans le groupe S_{10} des éléments suivants :
   (a) $\big(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10\big)$,
   (b) $\big(1\ \ 3\big)\ \big(2\ \ 7\ \ 4\ \ 10\ \ 9\big)$,
   (c) $\big(1\ \ 2\big)\ \big(3\ \ 4\big)\ \big(5\ \ 6\big)\ \big(7\ \ 8\big)\ \big(9\ \ 10\big)$.
4. 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 :

$$\tau\sigma\tau^{-1} = \big(\tau(a_{1,1})\ \ \tau(a_{1,2})\ \ \ldots\ \ \tau(a_{1,m_1})\big)\ \big(\tau(a_{2,1})\ \ \tau(a_{2,2})\ \ \ldots\ \ \tau(a_{2,m_2})\big) \ldots \big(\tau(a_{r,1})\ \ \tau(a_{r,2})\ \ \ldots\ \ \tau(a_{r,m_r})\big).$$

5. Soit n dans $\mathbb{N}_{\geq 1}$; on se place dans le groupe symétrique S_n. Démontrer :
   (a) Toute transposition de S_n s'écrit comme produit de transpositions de la forme $(i\ \ i+1)$ (i pouvant prendre toutes les valeurs entre 1 et $n-1$).
   (b) S_n peut être engendré par $\big(1\ \ 2\big)$ et $\big(1\ \ 2\ \ 3\ \ \ldots\ \ n-1\ \ n\big)$, c'est-à-dire que tout élément de S_n s'écrit comme un produit de ces deux éléments.
6. Soit $(A, +, \cdot, 0, 1)$ un corps. Démontrer que A est un anneau intègre.

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`)

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 8

04/11/2013

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé du 07/11/2013.

---

1. 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 :
   (a) n est divisible par 3 (ou 9) si et seulement si la somme $\sum_{i=0}^{r} c_i$ l'est ;
   (b) n est divisible par 11 si et seulement si la somme $\sum_{i=0}^{r} (-1)^i c_i$ l'est.
2. Donner et démontrer une règle facile pour le calcul, en fonction de n, des deux derniers chiffres de 7^n (utiliser les congruences modulo 100).
   Indication : $7^2 = 49$, $7^3 = 343$, $7^4 = 2401$.
3. Calculer le plus grand diviseur commun de 385 et 84, ainsi qu'une relation de Bézout.
4. Écrire les tables d'addition et de multiplication de l'anneau $\mathbb{Z}/6\mathbb{Z}$.
5. (a) Trouver un diviseur de zéro différent de $\bar{0}$ dans l'anneau quotient $\mathbb{Z}/51\mathbb{Z}$. *Cela démontre, entre autres, que $\mathbb{Z}/51\mathbb{Z}$ n'est pas un anneau intègre.*
   (b) Calculer l'inverse de la classe $\overline{16}$ dans $\mathbb{Z}/51\mathbb{Z}$.
6. 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 !).*

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")

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 9

11/11/2013

Les exercices sont à rendre le 18/11/2013 au début du cours.

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 est de sgn est noté A_n et appelé le *groupe alterné*.
   Dresser la liste de tous les éléments du groupe A_4.
3. Soit $(G, \star, e)$ un groupe. 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 de G.
4. Soit $n \in \mathbb{N}$. Nous définissons

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ \ (\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$$

   et

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ \ (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}.$$

   Démontrer : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un anneau commutatif.
   Indication : Utiliser le lemme 14.6 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.

Tourner la page, s.v.p.

5. 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 plusieures possibilités pour démontrer (a). Par exemple :
- *Si pour l'existence dans 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.*

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)

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

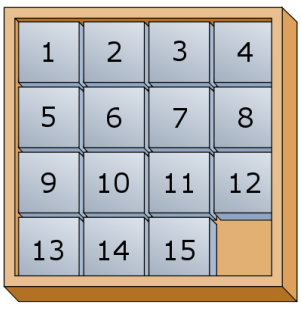
Feuille 10

18/11/2013

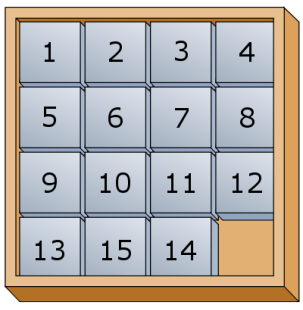
Les exercices sont à rendre le 25/11/2013 au début du cours.

1. Soit $(G, \star, e)$ un groupe. Soient H_1 et H_2 deux sous-groupes de G. Démontrer l'équivalence des deux assertions suivantes :
   (i) $H_1 \cup H_2$ est un sous-groupe de G.
   (ii) $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.
2. Soit $(G, \star, e)$ un groupe.
   (a) 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.
   (b) 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.
   (c) Démontrer que l'application
   $$\begin{array}{rccc} \varphi : & G & \to & \mathrm{Aut}(G) \\ & h & \mapsto & \sigma_h \end{array}$$
   est un morphisme de groupes.
   (d) 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 de $\mathrm{Aut}(G)$.
3. 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.

Tourner la page, svp.

(b) Démontrer qu'il est impossible d'obtenir la position finale (ci-dessus) à partir de la position initiale. *Indication : utiliser S_{15}, le signe d'une permutation et (a).*

4. Soient $(K, +_K, \cdot_K, 0_K, 1_K)$ un corps commutatif et 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 de E dans K dont toutes les valeurs sont 0 par $0_{\mathcal{F}}$ (concrètement : $0_{\mathcal{F}} : E \to K$ est 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 multiplication scalaire

$$\cdot_{\mathcal{F}} : K \times \mathcal{F}(E, K) \to \mathcal{F}(E, K), \quad (x, f) \mapsto x \cdot_{\mathcal{F}} f \text{ où } \forall e \in E : (x \cdot_{\mathcal{F}} f)(e) := x \cdot_K (f(e)).$$

Démontrer que $(\mathcal{F}(E, K), +_{\mathcal{F}}, \cdot_{\mathcal{F}}, 0_{\mathcal{F}})$ est un K-espace vectoriel.

5. Soit V l'espace vectoriel $\mathcal{F}(\mathbb{R}, \mathbb{R})$ (voir l'exercice précédent pour cette notation). Lesquels des sous-ensembles suivants sont des sous-espaces vectoriels de V ? Justifier la réponse.
   (a) $\{f \in V \mid f(1) = 0\}$,
   (b) $\{f \in V \mid f(0) = 1\}$,
   (c) $\{f \in V \mid f$ ne possède qu'un nombre fini de zéros$\}$,
   (d) $\{f \in V \mid f$ possède un nombre infini de zéros$\}$,
   (e) $\{f \in V \mid f(x) = 0$ pour tout $x \in \mathbb{R}$ sauf un nombre fini$\}$,
   (f) $\{f \in V \mid$ la suite $(f(k))_{k=1}^{\infty}$ tend vers $0\}$,
   (g) $\{f \in V \mid f$ est croissante$\}$,
   (h) $\{f \in V \mid$ l'application $g \in V$ définie par $\forall x \in \mathbb{R}, g(x) := f(x) - f(x-1)$ appartient à $U\}$, où $U \leq V$ est un sous-espace vectoriel donné.

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 !"

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 11

25/11/2013

Les exercices sont à rendre le 02/12/2013 au début du cours.

---

1. Soit $V = (\mathbb{F}_2)^4$, le $\mathbb{F}_2$-espace vectoriel standard de dimension 4 (ici, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ est le corps de cardinalité 2).
   (a) Dresser la liste de tous les éléments de V.
   (b) Trouver une base du sous-espace de V engendré par $\begin{pmatrix}\overline{1}\\ \overline{1}\\ \overline{0}\\ \overline{0}\end{pmatrix}, \begin{pmatrix}\overline{0}\\ \overline{1}\\ \overline{1}\\ \overline{0}\end{pmatrix}, \begin{pmatrix}\overline{0}\\ \overline{0}\\ \overline{1}\\ \overline{1}\end{pmatrix}, \begin{pmatrix}\overline{1}\\ \overline{0}\\ \overline{0}\\ \overline{1}\end{pmatrix}$. Justifier votre réponse.
2. Soit p un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps de cardinal p. Soit $d \in \mathbb{N}_{>0}$.
   Quelle est la cardinalité du $\mathbb{F}_p$-espace vectoriel standard de dimension d ? Démontrer votre réponse.
3. Soit $V = \mathcal{F}(\mathbb{N}, \mathbb{R})$ le $\mathbb{R}$-espace vectoriel de toutes les applications $\mathbb{N} \to \mathbb{R}$ (voir la feuille 10). Soit
   $$F := \{f \in V \mid f(n+2) = f(n+1) + f(n) \text{ pour tout } n \in \mathbb{N}\}.$$
   (a) Démontrer que F est un sous-espace vectoriel de V.
   (b) Démontrer que la dimension de F est 2 en exhibant une $\mathbb{R}$-base.
   (c) (Exercice supplémentaire.) Trouver $x, y \in \mathbb{R}$ tels que $f(n) := x^n$, $g(n) := y^n$ définissent des éléments de F qui sont $\mathbb{R}$-linéairement indépendants.
   (d) (Exercice supplémentaire.) Utiliser la partie précédente pour démontrer une formule qui exprime $f(n)$ en termes de $f(0)$, $f(1)$ et n, pour tout $f \in F$.
   Les éléments de F sont connus sous le nom de *suites de Fibonacci*.
4. Soient K un corps et V un K-espace vectoriel. Soient $e_1, e_2, \ldots, e_n \in V$ des éléments non nuls. Pour $i = 1, \ldots, n$ on pose $W_i = \langle e_i \rangle$, le sous-espace engendré par e_i (donc, $W_i = \{a \cdot e_i \mid a \in K\}$).
   Démontrer que les assertions suivantes sont équivalentes :
   (i) $e_1, \ldots, e_n$ est une K-base de V.
   (ii) $V = \bigoplus_{i=1}^n W_i$.

Tourner la page, svp.

5. Lesquelles des applications suivantes sont K-linéaires ? Justifier votre réponse.
   (a) $K = \mathbb{R}$, $\varphi : \mathbb{R} \to \mathbb{R}^2, x \mapsto \left(\begin{smallmatrix} x \\ x+2 \end{smallmatrix}\right)$;
   (b) $K = \mathbb{R}$, $\varphi : \mathbb{R} \to \mathbb{R}^2, x \mapsto \left(\begin{smallmatrix} x \\ x \cdot 2 \end{smallmatrix}\right)$;
   (c) $K = \mathbb{Q}$, $\varphi : \mathbb{Q}^2 \to \mathbb{Q}^2, \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} -y \\ x \end{smallmatrix}\right)$;
   (d) $K = \mathbb{R}$, $\varphi : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$;
   (e) $K = \mathbb{F}_2$, $\varphi : \mathbb{F}_2 \to \mathbb{F}_2, x \mapsto x^2$;
   (f) $K = \mathbb{R}$, $\varphi : \{(a_n)_{n\in\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}}$ est une suite réelle convergente$\} \to \mathbb{R}, (a_n)_{n\in\mathbb{N}} \mapsto \lim_{n\to\infty} a_n$;
   (g) $K = \mathbb{R}$, $\varphi : \mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$ où $\overline{z}$ est le conjugué complexe de z, c'est-à-dire, si $z = x + iy$ avec $x, y \in \mathbb{R}$, alors $\overline{z} = x - iy$;
   (h) $K = \mathbb{C}$, $\varphi : \mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$.

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 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.

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 12

02/12/2013

Les exercices sont à rendre le 09/12/2013 au début du cours.

1. Soient K un corps, V un espace vectoriel et $W_1 \leq V$, $W_2 \leq V$ des sous-espaces de dimension finie. Soient $S_1 = \{v_1, \ldots, v_r\}$ une K-base de W_1 et $S_2 = \{w_1, \ldots, w_s\}$ une K-base de W_2. On écrit $W_1 + W_2 = \sum_{i=1}^{2} W_i$ pour la somme de W_1 et W_2.
   (a) Démontrer que $\{v_1, \ldots, v_r, w_1, \ldots, w_s\}$ engendre $W_1 + W_2$ en tant que K-espace vectoriel.
   (b) Conclure : $\dim_K(W_1 + W_2) \leq \dim_K(W_1) + \dim_K(W_2)$.
   (c) On suppose maintenant que la somme est directe : $W_1 + W_2 = W_1 \oplus W_2$.
   Démontrer que $\{v_1, \ldots, v_r, w_1, \ldots, w_s\}$ est une K-base de $W_1 \oplus W_2$.
   (d) On suppose maintenant que la somme $W_1 + W_2$ n'est pas directe.
   Démontrer que $\{v_1, \ldots, v_r, w_1, \ldots, w_s\}$ n'est pas une K-base de $W_1 + W_2$.
   (e) Conclure que les assertions suivantes sont équivalentes :
      (i) la somme $W_1 + W_2$ est directe ;
      (ii) $\dim_K(W_1 + W_2) = \dim_K(W_1) + \dim_K(W_2)$.

2. (a) Soient K un corps, V, W des K-espaces vectoriels et $S = \{v_1, \ldots, v_n\}$ des vecteurs de V.
      (1) On suppose dans cette question que S engendre V. Soient $\phi : V \to W$ et $\psi : V \to W$ deux applications K-linéaires telles que $\phi(v_i) = \psi(v_i)$ pout tout $i \in \{1, \ldots, n\}$.
      Démontrer : $\phi(v) = \psi(v)$ pour tout $v \in V$.
      Cela signifie que toute application K-linéaire est uniquement determinée par les images des éléments d'une famille génératrice.
      (2) On suppose dans cette question que S est une K-base de V. Soient $w_1, \ldots, w_n$ des éléments de W (pas nécessairement une base !).
      Démontrer qu'il existe une application K-linéaire $\phi : V \to W$ telle que $\phi(v_i) = w_i$ pout tout $i \in \{1, \ldots, n\}$.
      Indication : utiliser que tout élément $v \in V$ s'écrit de façon unique comme $v = \sum_{i=1}^{n} a_i v_i$.
   (b) Soient $v_1 = \binom{2}{0}, v_2 = \binom{1}{1} \in \mathbb{R}^2$. On écrit $S = \{e_1, e_2\}$ avec $e_1 = \binom{1}{0}$ et $e_2 = \binom{0}{1}$ pour la base canonique de $\mathbb{R}^2$. Soit $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ l'unique application $\mathbb{R}$-linéaire telle que $\varphi(v_1) = \binom{0}{1}$ et $\varphi(v_2) = \binom{5}{2}$.
      (1) Démontrer que $T = \{v_1, v_2\}$ est une $\mathbb{R}$-base de $\mathbb{R}^2$.
      (2) Écrire (pas de calcul à faire !) la matrice $M_{S,T}(\varphi)$.
      (3) Écrire (pas de calcul à faire !) la matrice de changement de bases $C_{S,T}$.
      (4) Calculer la matrice $C_{T,S}$.
      (5) Calculer la matrice $M_{S,S}(\varphi)$.
      (6) Vérifier que la matrice $M = M_{S,S}(\varphi)$ satisfait $M \circ v_1 = \binom{0}{1}$ et $M \circ v_2 = \binom{5}{2}$.

Tourner la page, svp.

3. Soient $(G, \star, e)$ un groupe et $H \leq G$ un sous-groupe. Démontrer :
   La relation définie par
   $$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1^{-1} \star g_2 \in H$$
   est une relation d'équivalence.
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.

À propos : Le problème de Syracuse

On prend un nombre entier positif. S'il est pair on le divise par 2, sinon on le multiplie par 3 et on lui ajoute 1. On répète ensuite cette opération avec le nouveau nombre obtenu. Est-il vrai qu'on obtiendra toujours le nombre 1 après un certain nombre d'étapes ?

Cette conjecture a un énoncé très simple mais se révèle être incroyablement compliquée. Paul Erdős a dit à propos de cette conjecture : « Les mathématiques ne sont pas encore prêtes pour de tels problèmes. » Il a offert d'ailleurs $500 à celui qui prouverait ou réfuterait cette conjecture.

Exercices : Algèbre 1

Semestre d'hiver 2013/2014

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David, Dr. Santiago Molina

Feuille 13

09/12/2013

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé du 12/12/2013.

---

1. (a) Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ des groupes. On définit l'application :

$$\cdot : (G \times H) \quad \times \quad (G \times H) \to G \times H, \quad (g_1, h_1) \cdot (g_2, h_2) := (g_1 \star g_2, h_1 \circ h_2).$$

   Démontrer que $(G \times H, \cdot, (e, \epsilon))$ est un groupe.

   (b) Démontrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 4 qui n'est pas cyclique.

   (c) Démontrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est un groupe d'ordre 6 qui est cyclique.

2. (a) Calculer l'ordre de tout élément de $(\mathbb{Z}/8\mathbb{Z}, +, \overline{0})$.

   (b) On rappelle que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot, \overline{1})$ est le groupe des unités de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$. Calculer l'ordre de tout élément de $((\mathbb{Z}/8\mathbb{Z})^\times, \cdot, \overline{1})$.

3. Soit $n \in \mathbb{N}_{>1}$. On considère le groupe symétrique S_n.

   (a) Soient r un entier entre 2 et n et c dans S_n un cycle de longueur r. Calculer l'ordre de c.

   (b) Soient $c_1, \ldots, c_k$ dans S_n des cycles à supports disjoints, de longueurs respectives $r_1, \ldots, r_k$ (toutes comprises entre 2 et n) ; on note σ l'élément $c_1 c_2 \cdots c_k$. Calculer l'ordre de c en fonction de $r_1, \ldots, r_k$.

   (c) Soit r un nombre premier tel que $n/2 < r \leq n$. Démontrer que tout élément de S_n d'ordre r est un cycle de longueur r.

4. Dans cet exercice on démontre que S_5 ne possède pas de sous-groupe de cardinal 15 (bien que $15 \mid 120$ et $\#S_5 = 120$). *Ceci montre donc que la réciproque du théorème de Lagrange est fausse.* On raisonne par l'absurde : soit $H \leq S_5$ un sous-groupe de cardinal 15.

   (a) Combien d'éléments d'ordre 5 possède S_5 ? Combien d'éléments d'ordre 3 possède S_5 ?

   (b) En utilisant l'exercice précédent, démontrer que tout élément dans $H \setminus \{\mathrm{id}\}$ est soit un 3-cycle, soit un 5-cycle.

   (c) En déduire que H est la réunion de tous les 5-cycles, tous les 3-cycles et de l'identité.

   (d) Trouver explicitement un élément d'ordre 2 dans H.

   (e) En déduire une contradiction.

Tourner la page, svp.

5. Soit G un groupe.
   (a) Démontrer : si G est cyclique et $H \leq G$ est un sous-groupe (automatiquement normal car G est abélien), alors le quotient G/H est aussi cyclique.
   (b) Démontrer : si G est cyclique, alors tout sous-groupe H de G est aussi cyclique.
   Indication : il y a plusieurs manières de démontrer cette assertion. Utiliser par exemple : soient $a, b \in \mathbb{Z}$ et $d = \mathrm{pgcd}(a, b)$; si $g^a, g^b \in H$, alors $g^d \in H$.
   (c) Trouver un exemple d'un groupe G non cyclique et d'un sous-groupe normal $H \lhd G$ tels que H et G/H sont cycliques.

À propos : Le paradoxe de Monty Hall

Vous êtes candidat à un jeu télévisé et le présentateur vous propose de choisir votre prix. On vous place devant trois portes fermées. Derrière l'une de ces portes se trouve un cadeau merveilleux (la démonstration de l'hypothèse de Riemann par exemple) mais les deux autres portes ne cachent rien d'intéressant... Vous choisissez une porte (sans l'ouvrir). Une fois cela fait le présentateur ouvre une porte non intéressante parmi les deux portes restantes (exercice : une telle porte existe !). On vous propose maintenant de changer votre choix, quelle est la stratégie optimale ?