Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg

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

Version du 19 décembre 2012

Préface

C'est quoi, l'algèbre ? Dans l'histoire on comprend par l'algèbre l'étude des équations. Au cours des 2000 ans de cette étude, les gens se sont aperçus que certaines structures revenaient très souvent, et en plus dans des contextes tout à fait différents ! Depuis, les algébristes s'occupent aussi de l'étude et du dévelopement de ces structures, ainsi que, évidemment, de leurs applications dans d'autres domaines en sciences, ingénierie et mathématiques. Le cours d'algèbre 1 sera dédié 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 allons approfondir la théorie des anneaux et nous allons traiter quelques compléments au cours d'algèbre linéaire. En algèbre 3 le cours culminera en 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

Voici quelques références :
- Lelong-Ferrand, Arnaudiès. *Cours de mathématiques, Tome 1, Algèbre*. Dunod. Ce livre est très complet et très détailé. 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.

1 Premiers mots du langage mathématique

Le langage mathématique est différent du langage du quotidien par
– sa précision : tout terme a une définition précise ;
– son formalisme : souvent on utilise des symboles et des formules.

L'implication $\Rightarrow$

Nous introduisons le symbole $\Rightarrow$ pour les *implications*. Il se lit comme : « implique », « alors », « en conséquence », « donc », « est suffisant pour » etc.

(1) S'il pleut, la rue est mouillée.
(2) Il suffit qu'il pleuve pour que la rue soit mouillée.
(3) Je réussis l'examen. Donc je reçois les points ECTS.
(4) Si on a $x = 1$, alors $2x = 2$.
(5) Si on a $x = 1$, alors $x^2 = 1$.

Nous formalisons ces phrases maintenant ; nous nous intéressons seulement à la relation entre les deux parties de la phrases (il nous est égal s'il pleut actuellement ou non ; on s'intéresse uniquement aux implications) :

(1) Il pleut. $\Rightarrow$ La rue est mouillée.
(2) Il pleut. $\Rightarrow$ La rue est mouillée.
(3) Je réussis l'examen. $\Rightarrow$ Je reçois mes points ECTS.
(4) $x = 1 \ \Rightarrow \ 2x = 2$
(5) $x = 1 \ \Rightarrow \ x^2 = 1$

Parfois il est utile de formaliser encore un peu plus. On appelle une phrase comme « Il pleut. » ou « $x = 2$ » une assertion. Une assertion est vraie ou fausse.[1]
Si A et B sont des assertions, l'implication $\Rightarrow$ est une assertion de la forme

$$A \Rightarrow B,$$

qui signifie : si A est vraie, alors B est vraie. Elle ne dit pas (! !) que A est vraie !

L'implication $\Leftarrow$

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

(1) La rue est mouillée s'il pleut.
(2) Pour que la rue soit mouillée, il suffit qu'il pleuve.
(3) Je reçois les points ECTS si je réussis l'examen.
(4) On a $2x = 2$, si $x = 1$.
(5) On a $x^2 = 1$, si $x = 1$.

[1] Il y a des subtilités avec cette phrase que nous n'évoquerons pas car vous ne les rencontrerez dans aucun cours de vos études, sauf si vous suivez un cours de logique mathématique.

La formalisation est ainsi :

(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) $x^2 = 1 \Leftarrow x = 1$

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. Elle ne dit pas (! !) que B est vraie !

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) $x^2 = 1 \Leftrightarrow (x = 1 \text{ ou } x = -1)$

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.

Faites bien attention lequel des symboles $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ utiliser.

C'est une grande source d'erreur au début.

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.
Introduisons maintenant le formalisme (facile !) des tables de vérité (v= vraie, f = fausse) :

A	B	A et B	Explication
v	v	v	Si A est vraie et B est vraie, alors (A et B) est vraie.
v	f	f	Si A est vraie et B est fausse, alors (A et B) est fausse.
f	v	f	Si A est fausse et B est vraie, alors (A et B) est fausse.
f	f	f	Si A est fausse et B est fausse, alors (A et 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 et B est vraie (en particulier, si les deux sont vraies, alors « A ou B » est vraie).
Voici, la table de vérité qui exprime ce fait :

A	B	A ou 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 ou 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.

L'existence $\exists$

Voici quelques exemples d'assertions vraies :

(1) Il y a un étudiant dans cette salle.
(2) Il existe un $x \in \mathbb{Q}$ tel que $2x = 2$.
(3) Il existe un et un seul $x \in \mathbb{Q}$ tel que $2x = 2$.
(4) Il existe un $x \in \mathbb{Q}$ tel que $x^2 = 1$.
(5) Il existe un et un seul $x \in \mathbb{Q}$ 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 encore 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 $x > 0$.

On remplace souvent le « t.q. » par deux points « : ».

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 $x \in \mathbb{Q}$ on a $x^2 \geq 0$.
(3) Pour tout $n \in \mathbb{N}$ on a $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

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

La négation (symbole : $\neg$)

Si A est une assertion, nous écrivons « (non A) » pour sa négation. La table de vérité de la négation est triviale :

A	non 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 $x \leq 0$

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

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

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 et B	non (A et B)	non A	non B	(non A) ou (non 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

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

La contraposée

Soient A et B deux assertions. Alors, l'assertion ($A \Rightarrow B$) est vraie, si et seulement si (non $A \Leftarrow$ non B) est vraie. On appelle l'assertion (non $A \Leftarrow$ non 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 $x \leq 0$) $\Leftrightarrow x \neq 1$

La table de vérité de l'implication

On voudrait mentionner 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 pourquoi on fait 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. »
Remarquons que la table de vérité de ($A \Rightarrow B$) est la même que celle de l'assertion ((non A) ou B). Démontrez comme exercice que la table de vérité de l'assertion $(A \Rightarrow B)$ est aussi la même que celle de la contraposée ((non A) $\Leftarrow$ (non B)).

2 Ensembles et fonctions

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 objet sont égaux ou distincts.

On peut décrire des exemples 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.

[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.

Nous allons aussi utiliser les ensembles suivants que vous connaissez déjà de l'école, mais qui seront introduits de manière précise dans ce cours (bientôt) et en Analyse.
– $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, les *nombres naturels*.
– $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, les *nombres entiers*.
– $\mathbb{Q}$, les *nombres rationnels*.
– $\mathbb{R}$, les *nombres réels*.

On peut aussi définir des ensembles par des propriétés. Par exemple :
– $\mathcal{X} = \{ \underbrace{xy}_{\text{éléments}} \mid \underbrace{x \in \mathcal{Z}, y \in \mathcal{Z}}_{\text{propriétés}} \} = \{00, 01, 02, 03, \ldots, 99\}$.
– $\mathcal{E} = \{P \mid P$ est étudiant(e) de ce cours $\}$, l'ensemble des étudiants de ce cours.
– $\mathcal{L} = \{P \mid P$ est un/une Luxembourgeois(e) $\}$, l'ensemble de tous les Luxembourgeois.
– $\mathcal{B} = \{abc \mid a \in A, b \in B, c \in C\}$, l'ensemble de tous les mots en trois lettres.
– $\mathcal{G} = \{n \mid n \in \mathbb{N}, n$ 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 2.1. *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*

$$A \cup B := \{a \mid a \in A \text{ ou } a \in B\}$$

la réunion de A et B.
– *On appelle l'ensemble*

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

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 2.2. *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 $x \in A \cap (B \cup C)$.
$\Rightarrow x \in A$ et $x \in (B \cup C)$
$\Rightarrow x \in A$ et ($x \in B$ ou $x \in C$)
$\Rightarrow$ ($x \in A$ et $x \in B$) ou ($x \in A$ et $x \in C$)
$\Rightarrow x \in A \cap B$ ou $x \in A \cap C$

$\Rightarrow x \in (A \cap B) \cup (A \cap C)$
Nous avons démontré (1).
(2) Soit $x \in (A \cap B) \cup (A \cap C)$
$\Rightarrow x \in A \cap B$ ou $x \in A \cap C$
$\Rightarrow$ ($x \in A$ et $x \in B$) ou ($x \in A$ et $x \in C$)
$\Rightarrow x \in A$ et ($x \in B$ ou $x \in C$)
$\Rightarrow x \in A \cap (B \cup C)$.
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 $x \in A \cup (B \cap C)$
$\Rightarrow x \in A$ ou $x \in (B \cap C)$
$\Rightarrow x \in A$ ou ($x \in B$ et $x \in C$)
$\Rightarrow$ ($x \in A$ ou $x \in B$) et ($x \in A$ ou $x \in C$)
$\Rightarrow x \in A \cup B$ et $x \in A \cup C$
$\Rightarrow x \in (A \cup B) \cap (A \cup C)$
Nous avons démontré (1).
(2) Soit $x \in (A \cup B) \cap (A \cup C)$
$\Rightarrow x \in A \cup B$ et $x \in A \cup C$
$\Rightarrow$ ($x \in A$ ou $x \in B$) et ($x \in A$ ou $x \in C$)
$\Rightarrow x \in A$ ou ($x \in B$ et $x \in C$)
$\Rightarrow x \in A$ ou $x \in (B \cap C)$
$\Rightarrow x \in A \cup (B \cap C)$
Nous avons démontré (2), et donc (b). □

Lemme 2.3. *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 : $x \in A$ et $x \notin A$. 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 : $x \in A$ ou $x \notin A$. 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 :

$$x \in E \setminus (E \setminus A) \Leftrightarrow x \notin E \setminus A \Leftrightarrow \text{non}(x \in E \setminus A) \Leftrightarrow \text{non}(x \notin A) \Leftrightarrow x \in A.$$

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 :

$$x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow \text{non}(x \in A \cup B) \Leftrightarrow \text{non}(x \in A \text{ ou } x \in B)$$

$$\Leftrightarrow \text{non}(x \in A) \text{ et non}(x \in B) \Leftrightarrow x \in \overline{A} \text{ et } x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B}.$$

Ceci prouve l'égalité des deux ensembles.

(e) On a, d'après (b) et (d) :

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

□

Applications et fonctions

Définition 2.4. *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 sexe$(P) =$ homme si la personne P de l'ensemble $\mathcal{L}$ de tous les Luxembourgeois est un homme, et sexe$(P) =$ 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

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

est surjective mais pas injective.
L'application

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

est injective mais pas surjective.
L'application

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

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 2.5. *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 :

$$\begin{array}{rcl} y \in f(A \cup B) & \Leftrightarrow & \exists x \in A \cup B, y = f(x) \Leftrightarrow \exists x \in E \text{ tel que } x \in A \cup B \text{ et } y = f(x) \\ & \Leftrightarrow & \exists x \in E \text{ tel que } (x \in A \text{ ou } x \in B) \text{ et } y = f(x) \\ & \Leftrightarrow & \exists x \in E \text{ tel que } (x \in A \text{ et } y = f(x)) \text{ ou } (x \in B \text{ et } y = f(x)) \\ & \Leftrightarrow & (\exists x \in A, y = f(x)) \text{ ou } (\exists x \in B, y = f(x)) \\ & \Leftrightarrow & y \in f(A) \text{ ou } y \in f(B) \\ & \Leftrightarrow & y \in f(A) \cup f(B). \end{array}$$

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 :

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

Ceci prouve l'égalité des deux ensembles.

(d) Soit x dans E ; on a :

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

Ceci prouve l'égalité des deux ensembles.

□

Définition 2.6. *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 2.7 (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 2.8. *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 $f(a) = b$.*

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 2.7) implique :

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

On utilisant $g \circ f = \mathrm{id}_A$ nos 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 2.9. *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 2.10. *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 2.8. 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 2.9 donnent que f est surjective. La relation $g \circ f = \mathrm{id}_A$, l'injectivité de id_A et la partie (b) du lemme 2.9 donnent que f est injective. Ainsi, on obtient que f est bijective. □

3 Relations et nombres naturels

3.1 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 3.1. *Soit E un ensemble ; on appelle* relation binaire sur E *toute partie R de l'ensemble $E \times E$.*

Vocabulaire 3.2. *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 3.3. *Une relation binaire R sur un ensemble E est dite :*
- réflexive *si pour tout x dans E on a xRx ;*
- symétrique *si pour tout (x, y) dans $E \times E$ on a $(xRy \Rightarrow yRx)$;*
- antisymétrique *si pour tout (x, y) dans $E \times E$ on a $((xRy$ et $yRx) \Rightarrow x = y)$;*
- transitive *si pour tout (x, y, z) dans $E \times E \times E$ on a $((xRy$ et $yRz) \Rightarrow xRz)$;*
- totale *si pour tout (x, y) dans $E \times E$ on a $(xRy$ ou $yRx)$.*

Exemples 3.4.
- *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.*
- *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 dernières.

3.2 Relations d'équivalence

3.2.1 Définition et premiers exemples

Définition 3.5. *Soit E un ensemble ; on appelle* relation d'équivalence sur E *une relation binaire sur E qui est réflexive, symétrique et transitive.*

Exemples 3.6.

1. *L'égalité sur un ensemble est une relation d'équivalence.*
2. *Sur l'ensemble des droites affines du plan, le parallélisme est une relation d'équivalence.*
3. *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.

3.2.2 Classes d'équivalence et ensemble quotient

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

Définitions 3.7.
1. *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 $\bar{x}$.*
2. *Soit ω une classe d'équivalence de E ; tout élément x dans ω est appelé un* représentant *de ω.*
3. *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 3.8.
1. *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) !*
2. *Soient x et y dans E ; alors on a : $xRy \Leftrightarrow \bar{x} = \bar{y}$.*

Exemples 3.9.
1. *Pour l'égalité sur un ensemble E, on a : $\bar{x} = \{x\}$.*
2. *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 :*
$$\bar{x} = \{y \in E : f(y) = f(x)\} = f^{-1}(\{f(x)\}).$$
C'est « l'image réciproque de l'image de x ».

Proposition 3.10. *(a) Les classes d'équivalence de E sont toutes non vide 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) Soit $\overline{x}$ et $\overline{y}$ deux classes d'équivalence. Si $\overline{x} \cap \overline{y} \neq \emptyset$, alors $\overline{x} = \overline{y}$.

(e) 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) 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 $\overline{x} = \overline{y}$.
(e) et une conséquence directe de (a)–(d) : 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 (d) : deux classes d'équivalences sont soit les mêmes, soit disjointes. □

Proposition 3.11. *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. □

3.2.3 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 3.12. *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 3.13. *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*.

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

Démonstration.

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

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

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

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

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

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

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

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

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

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

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

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

□

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

3.3 Relations d'ordre

Définition 3.14. *Soit E un ensemble ; on appelle* relation d'ordre sur E *une relation binaire sur E qui est réflexive, transitive et antisymétrique.*

Exemples 3.15.

1. *L'égalité est une relation d'ordre.*

2. *Sur l'ensemble des parties d'un ensemble, l'inclusion est une relation d'ordre (en générale non totale).*
3. *Le « plus petit ou égal à $\leq$ » sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ est une relation d'ordre (totale). (Attention : $<$ ne définit pas de relation d'ordre ; la réflexivité n'est pas satisfaite.)*

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

Définition 3.16.
– *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 3.17. *Le plus grand et plus petit élément d'un ensemble ordonné n'existent pas toujours, mais lorsqu'ils existent ils sont uniques.*

Définition 3.18. *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 3.19. *Une partie qui possède un majorant (respectivement un minorant) est dite* majorée *(respectivement* minorée*).*

3.4 Les entiers naturels $\mathbb{N}$

On admettra qu'on peut, à partir de la notion d'ensemble, construire l'ensemble des entiers naturels $\mathbb{N}$ avec ses propriétés usuelles : addition (et multiplication), relation d'ordre. On admettra également que l'ensemble construit $\mathbb{N}$ possède la propriété d'être *bien ordonné*, qui s'exprime dans la proposition suivante.

Proposition 3.20 ($\mathbb{N}$ est bien ordonné)**.** *Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.*

Cette propriété a pour conséquence le *principe de récurrence*, utilisé de manière intensive pour des démonstrations dans tous les domaines des mathématiques.

Proposition 3.21 (Principe de récurrence)**.** *Soit $A(n)$ une assertion dépendant de n dans $\mathbb{N}$. Alors :*

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

Démonstration. 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. □

On utilise le principe de récurrence pour des démonstrations de la manière suivante :

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.

Notation 3.22. *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.*

Exemple 3.23. *(a) (« Petit Gauß » :) Nous voulons démontrer l'assertion*

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

pour tout $n \in \mathbb{N}_{>0}$.

Initialisation : *Pour $n=1$ on a $1=\frac{1(1+1)}{2}$, 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.*

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

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

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

(b) (« La somme des premiers nombres impairs » :) Nous voulons démontrer l'assertion

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

pour tout $n \in \mathbb{N}_{>0}$.

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 $\sum_{i=1}^{n}(2i-1)=n^2$.*

Le principe de récurrence a plusieurs variantes.

Proposition 3.24 (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 :*

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

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

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

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*

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

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*

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

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

Proposition 3.25. *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 3.26 (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.

3.5 Le cardinal d'un ensemble

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

Définition 3.27. *Soit E un ensemble. Le nombre d'éléments $\#E$ de E est aussi appelé la* cardinalité *(ou : le cardinal) de E. Une autre notation c'est $|E|$.*
Si E, F sont des ensembles et $f : E \to F$ est une application bijective, alors, on dit que E et F ont le même cardinal *(même si les ensembles sont infinis).*
Les ensembles qui ont le même cardinal que $\mathbb{N}$ sont appelés dénombrables.

Exemple 3.28. – $|\emptyset| = 0$ *(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).*

On va maintenant regarder les ensembles finis de plus près.

Proposition 3.29. *Pour tout $n \in \mathbb{N}$ on note $E_n := \{1, 2, \ldots, n\}$, en particulier, $E_0 = \emptyset$. C'est un ensemble de cardinal n.*
Soit E un ensemble fini de cardinal n. Alors il existe une bijection $E_n \to E$.

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

$$A(n) : \text{ pour tout ensemble } E \text{ de cardinal } n \text{ il existe une bijection } E_n \to E$$

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

Initialisation : Pour $n = 0$ on a $E_0 = \emptyset$ et $E = \emptyset$, donc $A(0)$ est vraie.

Hérédité : « $A(n) \Rightarrow A(n+1)$ » : Supposons donc que pour $n \in \mathbb{N}$ l'assertion $A(n)$ est vraie. Soit E un ensemble de cardinal $n+1$ et soit $e \in E$. L'ensemble $E' := E \setminus \{e\}$ est de cardinal n, donc, il existe une bijection

$$f' : E_n \to E'.$$

On définit l'application

$$f : E_{n+1} \to E, \quad m \mapsto \begin{cases} f'(m) & \text{si } m \leq n, \\ e & \text{si } m = n+1. \end{cases}$$

Elle est bijective, donc $A(n+1)$ est vraie.

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

□

Proposition 3.30. *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.*

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

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

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

Initialisation : Pour $n = 0$ on a $E_0 = \emptyset$ et $E_{k+1} \neq \emptyset$, donc $A(0)$ est vraie car il n'y a 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

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

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+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.

□

Corollaire 3.31. *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 la proposition 3.29 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. La (contraposée de la) proposition 3.30 donne alors $n = m$. □

Proposition 3.32. *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 3.33. *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 $|E \sqcup F| = |E| + |F|$.

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

(d) $\mathcal{F}(E, F)$ est 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 $|\mathcal{S}(E)| = |E|!$ (la notation $n!$ avec $n \in \mathbb{N}$ est la « factorielle de n » qui est definie comme $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$).

4 Groupes

Le monoïde $(\mathbb{N}, +, 0)$

Les propriétés suivantes des nombres naturels sont bien connues :

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 4.1. *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 4.2. *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 4.3.

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

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

Rappelons que nous avons déjà démontré *l'associativité de la composition d'applications* dans le lemme 2.7. 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 2.10. 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 4.4. *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 4.5. *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 4.6. *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 4.7. *Soit $m \in M$. 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 :

$$\begin{pmatrix} m & f(m) & f^2(m) & f^3(m) & \dots & f^{-1}(m) \end{pmatrix}$$

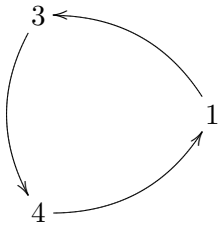
Exemple 4.8. *(a)* $M = \{1, 2, 3, 4, 5, 6\}$.

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

Le cycle qui contient 1 *est* $\begin{pmatrix} 1 & 3 & 4 \end{pmatrix}$. *C'est évidemment aussi le cycle qui contient* 3 *et* 4. *Encore une fois la signification de ce cycle est :*

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

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



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

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

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

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

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

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

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

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

(d) L'inverse de $(1\ \ 6\ \ 3\ \ 5)\ (2\ \ 4) \in S_6$ *est* $(1\ \ 5\ \ 3\ \ 6)\ (2\ \ 4)$.

Il est clair que l'écriture en cycles à supports disjoints est unique, sauf qu'on a le droit d'écrire les cycles dans une autre ordre et de commencer tout cycle par n'importe quel élément du cycle ; c'est-à-dire, on a par exemples les égalités :

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

Définition 4.9. *Un élément* $\tau \in S_n$ *est appelé* transposition *s'il existe* $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$ *tels que* $\tau = (i\ \ j)$.

Proposition 4.10. *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 $(a_1\ \ a_2\ \ a_3 \ldots a_r)$ s'écrit comme un produit de transpositions. C'est le cas car :

$$(a_1\ \ a_2\ \ a_3 \ldots a_r) = (a_r\ \ a_1) \circ (a_{r-1}\ \ a_1) \circ \cdots \circ (a_3\ \ a_1) \circ (a_2\ \ a_1).$$

□

5 Les entiers relatifs

Construction de $\mathbb{Z}$

Comme avant nous supposons les nombres naturels donnés avec toutes leurs propriétés bien connues (qui vont être rappelées).
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.
Une propriété bien connue des nombres naturels est que pour tous $a, b \in \mathbb{N}$ tels que $a \geq b$ il existe $d \in \mathbb{N}$ tel que $a = b + d$. Réciproquement si $a, b, d \in \mathbb{N}$ avec $a = b + d$, alors $a \geq b$.
La construction est basée sur la relation d'équivalence suivante.

Lemme 5.1. *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 la « propriété bien connue » ci-dessus. □

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 ». Bien que la multiplication ne soit pas difficile, on ne la regardera que dans la prochaine section. On s'occupe d'abord de l'addition.

Proposition 5.2. *Soit $\mathcal{Z}$ l'ensemble quotient de $\mathbb{N}$ par la relation d'équivalence définie dans le lemme 5.1.*

(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 5.3. *Pour tout* $\overline{a - b} = \overline{(a, b)} \in \mathcal{Z} \setminus i(\mathbb{N})$ *on a* $-\overline{a - b} = \overline{(b, a)} \in i(\mathbb{N})$ *et* $\overline{(a, b)} = \overline{(0, b - a)}$.

Démonstration. On a $a < b$, donc $\overline{(b, a)} \in \mathcal{Z}$. Le reste est clair. □

La multiplication des entiers relatifs

D'abord nous rappelons la multiplication des nombres naturels : La multiplication est une application

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a \cdot b = ab$$

qui satisfait :

Associativité Pour tous $a, b, c \in \mathbb{N}$ on a $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Élément neutre Pour tout $a \in \mathbb{N}$ on a $1 \cdot a = a \cdot 1 = a$.

Commutativité Pour tous $a, b \in \mathbb{N}$ on a $a \cdot b = b \cdot a$.

Distributivité Pour tous $a, b, c \in \mathbb{N}$ on a $(a + b) \cdot c = a \cdot c + b \cdot c$.

Donc $(\mathbb{N}, \cdot, 1)$ est un monoïde commutatif.
Une autre propriété très importante et bien connue des nombres naturels est la *règle de simplification* : pour tous $a, b, c \in \mathbb{N}$ tels que $a + c = b + c$ on a $a = b$.
Nous allons maintenant définir une multiplication sur notre « modèle » des entiers relatifs.

Proposition 5.4. *(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. □

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 $n \in \mathbb{N}$).

Anneaux

Définition 5.5. *Soient A un ensemble, $0_A, 1_A \in A$ deux éléments (pas nécéssairement 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 : $a + bc = a + (b \cdot c)$.

Lemme 5.6. *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 $0 = 0 \cdot a$. De la même façon : $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, donc $0 = a \cdot 0$. □

Exemple 5.7. *D'autres exemples d'anneaux sont :*
– *$(\mathbb{Q}, +, \cdot, 0, 1)$ est un anneau commutatif. Nous allons l'introduire formellement un peu plus tard.*
– *$(\mathbb{R}, +, \cdot, 0, 1)$ est un anneau commutatif. Il est connu des cours d'analyse et d'algèbre linéaire.*
– *$(\mathrm{Mat}_{2\times 2}(\mathbb{R}), +, \circ, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ est un anneau non-commutatif où $\circ$ note le produit matriciel.*

Définition-Lemme 5.8. *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 définissante de $A^\times$. □

Proposition 5.9. $\mathbb{Z}^\times = \{-1, 1\}$.

Démonstration. Il est une propriété bien connue de $\mathbb{N}$ que les seuls $a, b \in \mathbb{N}$ tels que $ab = 1$ sont $a = b = 1$. Si nous avons maintenant $a, b \in \mathbb{Z}$ avec $ab = 1$.
Si $a = \overline{(a, 0)} \in \mathbb{N}$ et $-b = \overline{(0, b)} \notin \mathbb{N}$, alors $\overline{(a, 0)} \cdot \overline{(0, b)} = \overline{(0, ab)} \notin \mathbb{N}$, donc ce cas est exclu.
Il reste à traiter le cas $\overline{(0, a)} \cdot \overline{(0, b)} = \overline{(ab, 0)} = \overline{(1, 0)}$, donc $a = b = 1$. □

Nous allons définir $\mathbb{Q}$ plus bas. Mais, 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

La propriété suivante des nombres naturels est bien connue : Pour tous $a, b \in \mathbb{N}$ tels que $ab = 0$, on a $a = 0$ ou $b = 0$.
Cette propriété reste valable pour $\mathbb{Z}$:

Proposition 5.10. *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 propriété de $\mathbb{N}$. 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 5.11. *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 5.12. *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 $ba = ca$. □

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 1. Effectivement, $3^{2012} =$

$$92889044588673769408930657158348637826253549738504402109446757688468292001008951330455686103135599435113269636691014193561324481293011619114370779797484532844502242818739756218769948728814713733963048450580139262655738290648436056477488586554569394630906606107459853399507260212571559105799059148489675525945234943427703047493820250646683714819140966942766998561791969345116849723253912785288621046469910341198346673143018586329173778550226801467817639806221514414791302508418812863657825701961769122152840214259983193500947245033100050601698088857156756341067790795022020127174479331881592685162237056834921409126356155082885916841461312766183596807125158846708980789530152015431456264939875716416229796717748349156426924910549996452947118501200024544027832540741788367702817371614709127269653373187151370781963928984799983669255770751058745723969318940086177579962471483395066809484748509853042208511416935201254255727222974802772253602512607193550634457144 1$$

– (voyez le cours)

La divisibilité dans $\mathbb{Z}$

Définition 5.13. *Soit $a, b \in \mathbb{Z}$. On dit que b* divise *a s'il existe $q \in \mathbb{Z}$ tel que $a = bq$. Notation : $b \mid a$. $p \in \mathbb{N} \setminus \{0, 1\}$ est appelé* nombre premier *si les seuls diviseurs positifs de p sont 1 et p. Notation pour l'ensemble des nombres premiers : $\mathbb{P} := \{p \mid p \in \mathbb{N}, p \text{ nombre premier }\}$.*

Lemme 5.14. *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 $rq = 1$, et donc $r = \pm 1$ et $q = r$ par la proposition 5.9, donc 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 $a \mid (b - c)$.

□

Proposition 5.15 (Euclide)**.** *L'ensemble des nombres premiers $\mathbb{P}$ est infini.*

Démonstration. Supposons le contraire : $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$. Nous allons obtenir une contradiction qui nous dit que cette supposition est fausse.
L'astuce est de considérer

$$q := 1 + p_1 \cdot p_2 \cdot \ldots \cdot p_n > 1$$

et de démontrer que le plus petit diviseur de q qui est strictement plus grand que 1 est un nombre premier qui n'est pas dans la liste.
Plus formellement : $M := \{m \in \mathbb{N}_{>1} \mid m \mid q\}$ est un sous-ensemble de $\mathbb{N}$ qui n'est pas vide (car $q \in M$ comme $q \mid q$). Donc, comme $\mathbb{N}$ est bien ordonné, il existe un plus petit élément $s \in M$. Soit $t \in \mathbb{N}_{>1}$ un diviseur de s. Alors, par le lemme 5.14 (a) on a $t \mid q$, donc $t \in M$. Comme $t \leq s$, il en suit que $t = s$, donc s est un nombre premier, donc il existe $1 \leq i \leq n$ tel que $s = p_i$.
Nous avons encore par le lemme 5.14 que

$$p_i \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n.$$

Comme $p_i = s \mid q$, le lemme 5.14 (b) donne :

$$p_i \mid (q - p_1 \cdot p_2 \cdot \ldots \cdot p_n),$$

donc $p_i \mid 1$, ce qui implique $p_i \leq 1$. La contradiction désirée. □

Dès qu'on saura que tout nombre naturel ≥ 2 s'écrit de façon unique (à l'ordre près) comme un produit de nombres premiers, la preuve pourra être abrégée : on peut prendre n'importe quel nombre premier p qui divise q (son existence sera garantie car q s'écrit comme produit de nombres premiers) ; alors $p = p_i$ pour un $1 \leq i \leq n$ et on obtiendra la même contradiction.

Division euclidienne

Proposition 5.16 (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 5.17. *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 5.18. *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) ⇒ (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) ⇒ (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 5.19. *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 résiduels

Lemme 5.20. *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 $n \mid (x_1x_2 - y_1y_2)$, 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 5.21. *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 5.20 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 5.22. *(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 commun diviseur

Définition 5.23. *Soient* $d \in \mathbb{N}$ *et* $x, y \in \mathbb{Z}$*. On appelle* d *le* 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* $((e \mid x \text{ et } e \mid y) \Rightarrow e \mid d)$.

Proposition 5.24. *Soient* $x, y \in \mathbb{Z}$*.*

1. *Un plus grand commun diviseur de* x *et* y *existe et il est unique.*
2. 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 clair : Si $d, e \in \mathbb{N}$ sont des plus grands communs diviseurs tous les deux, alors $d \mid e$ et $e \mid d$, 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 5.25. $r_0 = 99$ *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

$$r_n = a r_1 + b r_0,$$

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 5.26. *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 5.27. *Soient* $m \in \mathbb{N}$ *et* $x, y \in \mathbb{Z}$*. On appelle* m *le* plus petit commun multiple de x, y *(notation :* $m = \mathrm{ppcm}(x, y)$*) si*
– $x \mid m$ *et* $y \mid m$ *et*
– *pour tout* $n \in \mathbb{N}$ *on a* $((x \mid n \text{ et } y \mid n) \Rightarrow m \mid n)$.

Proposition 5.28. *Soient* $x, y \in \mathbb{Z}$.

1. *Un plus petit commun multiple de* x *et* y *existe et il est unique.*
2. *On a l'identité* $xy = \mathrm{signe}(xy) \cdot \mathrm{ppcm}(x, y) \cdot \mathrm{pgcd}(x, y)$.

Démonstration. Exercice. □

Corps finis

Lemme 5.29. *Soit* $n \in \mathbb{N}_{>1}$*. Soit* $x \in \mathbb{Z}$ *tel que* $\mathrm{pgcd}(x, n) = 1 = ax + bn$ *avec* $a, b \in \mathbb{Z}$ *(l'identité de Bézout).*
Alors, la classe $\overline{a}$ *est un inverse multiplicatif de la classe* $\overline{x}$ *dans l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$.

Démonstration. Nous avons $1 = ax + bn \equiv ax \pmod{n}$, donc $\overline{1} = \overline{ax} = \overline{a} \cdot \overline{x}$. □

Corollaire 5.30. *Soit* $n \in \mathbb{N}_{>1}$*. Alors, le groupe d'unités de l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ *est*

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

Démonstration. Dans le lemme 5.29 nous avons vu que toutes les classes $\overline{x}$ pour $x \in \mathbb{Z}$ tel que $\mathrm{pgcd}(x, n) = 1$ sont des unités.
Si $x = py$ et $n = pm$ avec $1 < p < n$, alors nous avons $\overline{m} \neq \overline{0}$ et

$$\overline{xm} = \overline{ypm} = \overline{ypm} = \overline{y}\overline{0} = \overline{0},$$

donc $\overline{x}$ ne peut pas être une unité, car s'il l'était : $\overline{1} = \overline{yx}$, alors

$$\overline{m} = \overline{1}\overline{m} = \overline{yxm} = \overline{y}\overline{0} = \overline{0},$$

une contradiction. □

Définition 5.31. *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*

– $0 \neq 1$.

Corollaire 5.32. *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) $\Rightarrow$ (ii) » : Supposons que n n'est pas un nombre premier, donc $n = ab$ avec $1 < a, b < n$. Alors par le corollaire 5.30 $\overline{a} \neq \overline{0}$ n'est pas une unité de $\mathbb{Z}/n\mathbb{Z}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.
« (ii) $\Rightarrow$ (i) » : Si n est un nombre premier, tous les $a \in \mathbb{Z}$ tels que $1 \leq a \leq n-1$ satisfont $\mathrm{pgcd}(a, n) = 1$, donc toutes les classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ sont inversibles. Donc, la seule classe qui n'est pas inversible est $\overline{0}$ et $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Unique factorisation en nombres premiers

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.

Lemme 5.33. *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 5.34. *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 5.33. 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 5.33 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 5.35. *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 5.14 (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 5.36 (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 5.35 il existe un nombre premier p qui divise m. Comme p est un produit de nombres premiers (le produit avec le seul facteur p), on a $p \notin M$, donc $p < m$, donc $2 \leq \frac{m}{p} < m$, donc $\frac{m}{p} \notin M$. Donc $\frac{m}{p}$ est un produit d'éléments premiers, donc $m = p\frac{m}{p}$ l'est aussi. Donc $m \notin M$. Contradiction. Donc M est vide.
(b) Nous démontrons le résultat par récurrence pour $n \geq 1$. Pour $n = 1$ le résultat est clair. Supposons que nous avons déjà démontré le résultat pour tout nombre naturel positif strictement plus petit que n. Montrons-le pour n.
Nous avons donc

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

Comme $p_1 \mid n$, il suit du corollaire 5.34 qu'il existe un $j \in \{1, \ldots, s\}$ tel que $p_1 \mid q_j$. Comme q_j et p_1 sont des nombres premiers, on a $p_1 = q_j$. En conséquence, nous obtenons

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

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

6 Les nombres rationnels

Les 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 6.1. *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 $ax = ax$.

Symmétrie 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 5.12 on obtient $az = cx$, donc $(a, x) \sim (c, z)$.

□

Proposition 6.2. *Soit $\mathbb{Q}$ l'ensemble quotient du lemme 6.1.*

(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 $\mathbb{Z}$

Nous admettons l'ordre naturel $\leq$ sur $\mathbb{N}$ (par exemple $7 \leq 8$) (en fait, nous l'avons déjà utilisé). Il satisfait les propriétés suivantes :
– $\forall\, n, m, p \in \mathbb{N}:\ \big(n \leq m \ \Rightarrow\ n + p \leq m + p\big)$,
– $\forall\, n, m, p \in \mathbb{N}:\ \big(n \leq m \ \Rightarrow\ n \cdot p \leq m \cdot p\big)$.
Nous allons étendre l'ordre naturel d'abord à $\mathbb{Z}$ puis à $\mathbb{Q}$ 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 6.3. *(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 $i : \mathbb{N} \to \mathcal{Z},\ \ n \mapsto \overline{n-0}$ 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 6.4. *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 $yz = \overline{dn-cn} \leq \overline{bn-an} = xz$. □

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

Définition-Lemme 6.5. *(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. Exercice. □

À partir de maintenant nous allons écrire $\leq$ au lieu de $\preccurlyeq$.

Lemme 6.6. *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. Exercice. □

La valeur absolue de $\mathbb{Q}$

Définition 6.7. *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 6.8. *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 » ; voir les exercices pour une valeur propre qui n'est pas archimédienne).

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 6.9 (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 contruits à partir des nombres rationnels :
En 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.

7 Introduction aux groupes

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 7.1. *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 7.2. – *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 7.3. *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 7.4 (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 7.5. *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 7.6. *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 7.7. – *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 7.8. *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 7.9. *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 7.10. *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 7.4 : $g^n \star (g^m)^{-1} = g^{n-m} \in H$. 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 7.11. *Soient $(G, \star, e)$ un groupe, I un ensemble « d'indices » (par exemple $I = \{1, 2, \ldots, n\}$) 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 7.4 H est un sous-groupe de G.

□

Définition-Lemme 7.12. *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 7.11 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 7.13. *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 7.4 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

Exemple 7.14. – *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 ses 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 7.15. *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 7.16.
- *$c : \mathbb{Z} \to \mathbb{Z}$, 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 5.20.
- *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 7.17. *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 7.18. *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 $\{m \mid n$ divise $m\}$, l'ensemble des multiples de n.

Définition-Lemme 7.19. *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 7.20 (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 7.4 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 7.4 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 7.21. *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) Les assertions suivantes sont équivalentes :

(i) φ est injectif.

(ii) $\ker(\varphi) = \{e\}$.

(c) 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 $g_1 = k \star g_2$.

Démonstration. (a) C'est par définition ! On le mentionne ici uniquement à cause de la similarité avec (b).
(b) est une conséquence directe de (c).
(c) « (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 :

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

□

Définition 7.22. *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 7.23. *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 7.24. *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 7.25 (Cayley)**.** *Soit $(G, \star, e)$ un groupe fini. Soit $S(G) := \{\sigma : G \to G \mid$ 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. □

8 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 en 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 8.1. *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. □

Exemple 8.2. *$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes à gauche du groupe $\mathbb{Z}$ (pour l'addition) suivant le sous-groupe $n\mathbb{Z}$.*

Définition-Lemme 8.3. *Soit G un groupe et $H \leq G$ un sous-groupe.*

(a) De la même manière que dans la définition-lemme 8.1 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
– $G = \bigsqcup_{Hg \in H\backslash G} Hg$,
– $Hg_1 \cap Hg_2 = \begin{cases} \emptyset & \text{si } g_1g_2^{-1} \notin H, \\ Hg_1 & \text{si } g_1g_2^{-1} \in H. \end{cases}$

(b) L'application

$$\phi : G/H \to H\backslash G, \quad gH \mapsto Hg^{-1}$$

est bijective.

Démonstration. C'est clair ! (Notez pour (b) que $Hg^{-1} = (gH)^{-1}$ parce que $H^{-1} = H$.) □

Lemme 8.4. *Soient G un groupe et $H \leq G$ un sous-groupe. Pour tout $g_1, g_2 \in G$ l'application*

$$g_1H \longrightarrow g_2H, \quad g_1h \mapsto (g_2g_1^{-1})g_1h = g_2h$$

est bijective. Donc $\#H = \#gH$ pour tout $g \in G$ (les deux peuvent être infinis).

Démonstration. La surjectivité est évidente. Regardons donc l'injectivité : $g_2h_1 = g_2h_2$ implique $g_2^{-1}g_2h_1 = g_2^{-1}g_2g_2h_2$, donc $h_1 = h_2$. □

Définition 8.5. *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 8.6 (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 8.4. □

Définition 8.7. *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 8.8. *Soit G un groupe abélien. Tout sous-groupe $H \leq G$ est normal.*
Raison : La commutativité implique directement $gH = Hg$.

Lemme 8.9. *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 8.10. *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 8.11. *Soit $n \in \mathbb{N}$. Le groupe alterné A_n 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 8.12. *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 8.13. *$(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ est le quotient de $(\mathbb{Z}, +, 0)$ par le sous-groupe normal $(n\mathbb{Z}, +, 0)$.*

Proposition 8.14. *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 ψ 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 7.20. 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 7.20 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 8.10. □

Théorème 8.15 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soit $\varphi : G \to H$ un homomorphisme de groupe. 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.

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 $\overline{\varphi}(gN) = \varphi(g) = h$.

□

Remarque 8.16. *L'application $\overline{\varphi}$ est la même que dans le théorème 3.13.*

9 Ordres

Définition-Lemme 9.1. *Soient G un groupe et $g \in G$. Considérons l'homomorphisme de groupes $\phi : \mathbb{Z} \to G$ donné par $n \mapsto g^n$ (voir la définition 7.6 pour la signification de g^n).*

(a) Si G est fini, alors $\ker(\phi) \cap \mathbb{N}_{>0} \neq \emptyset$.

(b) Si $\ker(\phi) \cap \mathbb{N}_{>0} \neq \emptyset$, *alors* l'ordre de g *est défini comme le plus petit élément de* $\ker(\phi) \cap \mathbb{N}_{>0}$. *Sinon on dit que l'ordre de G est infini. Notation :* $\mathrm{ord}(g)$.

(c) Si $\mathrm{ord}(g)$ *est fini, alors pour tout* $m \in \ker(\phi)$ *on a* $\mathrm{ord}(g) \mid m$.

(d) Si $\mathrm{ord}(g)$ *est fini, alors on a* $\mathrm{ord}(g) = \#\langle g \rangle$.

(e) Si $\mathrm{ord}(g)$ *est fini, alors* $\overline{\phi} : \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z} \to G$, *donné par* $n + \mathrm{ord}(g)\mathbb{Z} \mapsto g^n$, *est un homomorphisme injectif de groupes, et son image est* $\langle g \rangle$.

(f) $\mathrm{ord}(g) = 1$ *si et seulement si* $g = 1$.

Démonstration. (a) Comme G est fini, il existe $a, b \in \mathbb{N}$ tels que $a > b$ et $g^a = g^b$. Donc, $g^{a-b}g^b = g^b$, donc $g^{a-b} = 1$.
(c) Soit $m \in \mathbb{Z}$ tel que $g^m = 1$. Par la division euclidienne nous avons $m = \mathrm{ord}(g) \cdot q + r$ avec $0 \leq r < \mathrm{ord}(g)$. On a $1 = g^m = g^{\mathrm{ord}(g)\cdot q}g^r = (g^{\mathrm{ord}(g)})^q g^r = 1^q g^r = 1g^r = g^r$. Comme $0 \leq r < \mathrm{ord}(g)$ par la définition de l'ordre la seule possibilité qui reste est $r = 0$, donc $\mathrm{ord}(g) \mid m$.
(d) Soit $n = \mathrm{ord}(g)$. Les éléments $1, g, g^2, \ldots, g^{n-1}$ de $\langle g \rangle$ sont distincts (sinon avec le même argument qu'en (a) on obtiendrait une contradiction). Ils forment déjà un sous-groupe de G car les produits et les inverses y appartiennent ; pour les inverses : $(g^a)^{-1} = g^{n-a}$ pour $1 \leq a \leq n-1$.
(e) Par (c) $\ker(\phi)$ est le sous-groupe $\mathrm{ord}(g)\mathbb{Z}$ de $\mathbb{Z}$. Donc, l'assertion suit directement du théorème d'isomorphisme 8.15.
(f) Il est clair que $\mathrm{ord}(1) = 1$. Soit $\mathrm{ord}(g) = 1$, alors $\#\langle g \rangle = 1$, donc $g = 1$. □

Corollaire 9.2. *Soit G un groupe cyclique.*

(a) Si $n := \#G$ est fini, alors G est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$.

(b) Si G n'est pas fini, alors G est isomorphe au groupe $(\mathbb{Z}, +, 0)$.

Démonstration. (a) Soit g un générateur de G, donc $\mathrm{ord}(g) = \#G = n$. Donc, il suffit d'utiliser la définition-lemme 9.1 (e).
(b) L'homomorphisme $\phi : \mathbb{Z} \to G$ de la définition-lemme 9.1 (donné par $n \mapsto g^n$) est injectif et surjectif. □

Corollaire 9.3. *Soient G un groupe fini et $g \in G$. Alors* $\mathrm{ord}(g) \mid \#G$.

Démonstration. Par le théorème de Lagrange 8.6 et la définition-lemme 9.1 on a $\mathrm{ord}(g) = \#\langle g\rangle \mid \#G$. □

Corollaire 9.4 (« 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. Soit $n = \mathrm{ord}(g)$. Comme $n \mid \#G$ on a $\#G = nm$ pour un $m \in \mathbb{N}$. Donc, $g^{\#G} = g^{nm} = (g^n)^m = 1^m = 1$. □

Corollaire 9.5. *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 et $\mathrm{ord}(g) \neq 1$, alors $\mathrm{ord}(g) = p$, donc $\langle g\rangle = G$, et G est cyclique. □

Corollaire 9.6. *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. Exercice. □

Corollaire 9.7. *Soit 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. On cherche $m \in \mathbb{N}_{>0}$ minimal tel que
– $g^m = 1$ ($\Leftrightarrow \mathrm{ord}(g) \mid m$) et
– $i \mid m$.
Donc $m = \mathrm{ppcm}(i, \mathrm{ord}(g))$, alors $\mathrm{ord}(g^i) = \frac{m}{i} = \frac{\mathrm{ppcm}(i,\mathrm{ord}(g))}{i} = \frac{\mathrm{ppcm}(i,\mathrm{ord}(g))\cdot\mathrm{pgcd}(i,\mathrm{ord}(g))}{i\cdot\mathrm{pgcd}(i,\mathrm{ord}(g))} = \frac{i\cdot\mathrm{ord}(g)}{i\cdot\mathrm{pgcd}(i,\mathrm{ord}(g))} = \frac{\mathrm{ord}(g)}{\mathrm{pgcd}(i,\mathrm{ord}(g))}$. □

Définition-Lemme 9.8. *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 9.9. *Soient G un groupe abélien fini et $H_1, H_2 \leq H$ deux sous-groupes de G.*

(a) Si $H_1 \cap H_2 = \{1\}$, alors, l'application $\phi : H_1 \times H_2 \to G$ donné par $(h_1, h_2) \mapsto h_1h_2$ est un homomorphisme de groupes injectif.

(b) Si $\operatorname{pgcd}(\#H_1, \#H_2) = 1$*, alors* $H_1 \cap H_2 = \{1\}$.

Démonstration. (a)

Homomorphisme On calcule $\phi((h_1, h_2)(h_1', h_2')) = \phi((h_1h_1', h_2h_2')) = h_1h_1'h_2h_2' = h_1h_2h_1'h_2' = \phi((h_1, h_2))\phi((h_1', h_2'))$.

Injectivité $\phi((h_1, h_2)) = h_1h_2 = 1$, donc $h_1 = h_2^{-1} \in H_1 \cap H_2 = \{1\}$, donc $h_1 = h_2 = 1$.

(b) Soit $g \in H_1 \cap H_2$. Donc $\operatorname{ord}(g) \mid \#H_1$ et $\operatorname{ord}(g) \mid \#H_2$, donc $\operatorname{ord}(g) = 1$, donc $H_1 \cap H_2 = \{1\}$. □

Lemme 9.10. *Soient* G *un groupe abélien fini et* $g, h \in G$.

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

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

Démonstration. (a) Soit $m := \operatorname{ord}(gh)$. Donc $g^mh^m = 1$ et par $\langle g\rangle \cap \langle h\rangle = \{1\}$ (à cause du lemme 9.9 (b)), on a $g^m = h^m = 1$ Par la définition-lemme 9.1 (c), il en suit que $\operatorname{ord}(g) \mid m$ et $\operatorname{ord}(h) \mid m$, donc $\operatorname{ord}(g)\operatorname{ord}(h) \mid m$ (utilisant encore une fois $\operatorname{pgcd}(\operatorname{ord}(g), \operatorname{ord}(h)) = 1$). Il est clair que $(gh)^{\operatorname{ord}(g)\operatorname{ord}(h)} = 1$.
(b) Soient

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

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 9.7 nous avons

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

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

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

□

Définition 9.11. *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 9.12. *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 $n := \mathrm{ppcm}(\mathrm{ord}(g) \mid g \in G)$. Il est clair que $g^n = 1$ pour tout $g \in G$, donc $\exp(G) \leq n$. Le lemme 9.10 (b) montre qu'il existe $g \in G$ tel que $\mathrm{ord}(g) = n$. En conséquence $n \leq \exp(G)$. Toutes les assertions sont maintenant claires. □

Exemple 9.13. *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, 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 (cycliques et non-cycliques). On va démontrer qu'il n'y en a pas plus ; donc tout groupe d'ordre 4 est abélien.*
  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 $c = ba$. Donc G est abélien. Par le lemme 9.9 (a) nous obtenons $\langle a \rangle \times \langle b \rangle$ 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 : abélien et 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 $\mathbb{Z}/6\mathbb{Z}$).
  Soit $g \in G$ différent de l'élément neutre. Comme l'ordre de g est un diviseur de 6 et strictement plus petit que 6 (sinon le groupe serait cyclique engendré par g), on a $\mathrm{ord}(g) = 2$ ou $\mathrm{ord}(g) = 3$.
  On veut démontrer qu'il existe $a, b \in G$ tels que $\mathrm{ord}(a) = 3$ et $\mathrm{ord}(b) = 2$.
  Si tout élément non-neutre de G était d'ordre 2, G serait abélien par l'exercice 5 de la feuille 5.
  En choisissant $b_1 \neq b_2$ d'ordre 2, le lemme 9.9 (a) nous donne une injection $\phi : \langle b_1 \rangle \times \langle b_2 \rangle \to G$. L'image de ϕ serait un sous-groupe d'ordre 4, mais $4 \nmid 6$, c'est une contradiction avec le théorème de Lagrange 8.6.
  Soit donc a un élément 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 dernière possibilité est immédiatement vu être impossible. Donc $b^2 \in H$. Donc $\mathrm{ord}(b^2)$ est 1 ou 3. Le dernier cas menerait à $\mathrm{ord}(b) = 6$ qui est exclu. Donc $\mathrm{ord}(b) = 2$.
  Notons que $ab \neq 1, a, a^2, b$. Aussi $a^2 b \neq 1, a, a^2, b, ab$. Donc $G = \{1, a, a^2, b, ab, a^2 b\}$. Si $ba = ab$, alors G serait abélien et dans ce cas $\mathrm{ord}(ab) = 6$ et le groupe serait cyclique ce que nous supposons ne pas être le cas. La seule autre possiblité est $ba = a^2 b$.
  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 $\phi(A^2 B) = a^2 b$. C'est clairement une bijection. Que c'est un homomorphisme est une conséquence de $\mathrm{ord}(A) = 3$, $\mathrm{ord}(B) = 2$ et $BA = A^2 B$ qui est facilement vérifié.

10 Compléments

Lemme 10.1. *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 sur la feuille 13. □

Proposition 10.2 (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 8.15) 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 10.1 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 8.15. □

Proposition 10.3 (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 8.15) 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 8.15. □

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 10.4 (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 10.5. *On obtient du théorème 10.4 qu'à isomorphisme près il n'existe que deux groupes abéliens de cardinal* 12*, en l'occurence* $\mathbb{Z}/12\mathbb{Z}$ *et* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Exercices en cours : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David 17/09/2012

1. Lesquels des symboles « $\Rightarrow$ », « $\Leftarrow$ », « $\Leftrightarrow$ » peuvent être écrit dans les lacunes de sorte que les assertions suivantes soient vraies ?

   Soient x, y des nombres réels.

   (1) $3x = 6$ _____ $x = 2$

   (2) $3x = 6$ _____ $x = 2$ ou $x = 1$

   (3) $3x = 6$ _____ $x = 2$ ou $x > 0$

   (4) $3x = 6$ _____ $x \neq 3$

   (5) $x^2 = 4$ _____ $x = 2$

   (6) $x - y = 0$ et $x + y = 6$ _____ $x = 3$ et $y = 3$

   (7) $y = 2x$ et $3x = 2y - x$ _____ $x = 1, y = 2$

2. Faites la négation des phrases suivantes :

   (a) Tous les étudiants de ce cours sont luxembourgeois.

   _____

   (b) Adrien parle français ou allemand.

   _____

   (c) Adrien parle français et allemand.

   _____

   (d) Deux cotés de ce triangle ont la même longeur.

   _____

3. (a) Remplissez la table de vérité :

A	B	A ou B	non (A ou B)	non A	non B	(non A) et (non B)
v	v			f	f	
v	f			f	v	
f	v			v	f	
f	f			v	v	

   (b) On définit le « ou exclusif » (XOR) par la table de vérité :

A	B	A XOR B
v	v	f
v	f	v
f	v	v
f	f	f

   Exprimez XOR en utilisant seulement « et », « ou » et « non ».

4. Il y a trois suspects dans une enquête pour meurtre : Adrien (A), Berta (B), Christian (C). L'enquête a déjà établi les faits suivants :

   (1) Au moins une des trois personnes A,B,C est coupable.

   (2) A n'est pas coupable si B et C ne sont pas tous les deux coupables.

   (3) Si C est coupable ou si A n'est pas coupable, alors B ne peut pas être coupable.

   Trouvez pour chaque personne si elle est coupable ou non.

5. Considérez la 'preuve' suivante qui démontre $1 = 0$:

$$
\begin{array}{ll}
2x = 2 & \mid \text{additionner } (2x-4) \\
\Rightarrow 4x - 4 = 2x - 2 & \mid \text{simplifier} \\
\Rightarrow 4(x-1) = 2(x-1) & \mid \text{diviser par } (x-1) \\
\Rightarrow 4 = 2 & \mid \text{soustraire } 2 \\
\Rightarrow 2 = 0 & \mid \text{diviser par } 2 \\
\Rightarrow 1 = 0 &
\end{array}
$$

   Qu'est-ce que vous en pensez ? Pourquoi ?

Exercices : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 1

17/09/2012

Les exercices sont à rendre le 24/09/2012 au début du cours.

Vos solutions aux exercices vont être notées A (bien), B (moins bien), C (insuffisant). La note que vous obtenez pour vos exercices ainsi que pour vos résultats aux devoirs surveillés comptent pour la note finale du cours : une moyenne de A compte 2 points sur 20 et 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 une 13 dans l'examen, la note finale sera 14.

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.

   Lesquelles des assertions suivantes sont correctes ? Justifiez (de façon concise !) vos réponses !

   (a) Il existe de jeunes cochons dans la ferme.

   (b) Il existe de vieux cochons dans la ferme.

   (c) Tous les cochons qui ne sont pas voraces sont jeunes.

   (d) Il y a de jeunes cochons malades.

   (e) Tous les jeunes cochons sont malades.

2. Faites la négation des assertions suivantes :

   (1) Tous les nombres parfaits sont pairs.

   Rem. : Vous n'avez pas besoin de connaître la définition d'un nombre parfait pour écrire la négation. En fait, il n'est pas connu si cette assertion est vraie ou fausse.

   (2) $\forall\, \epsilon > 0\ \exists\, \delta > 0\ \forall\, x : (|x - x_0| \leq \delta \Rightarrow |f(x) - f(x_0)| \leq \epsilon)$

   Rem. : Dans votre cours d'Analyse 1 vous allez apprendre que ceci est la définition de la continuité de la fonction f au point x_0.

3. Soient A, B des ensembles. Démontrez :

   (a) $A \subseteq B \ \Leftrightarrow\ A = A \cap B \ \Leftrightarrow\ B = A \cup B$.

   (b) $A \cap B = \emptyset \ \Leftrightarrow\ A \setminus B = A$.

À propos. Pour illustrer qu'une assertion fausse comme $0 = 1$ implique tout, on dit qu'Einstein a donné l'exemple suivant : « Si $0 = 1$, alors $1 = 2$. L'ensemble dont les éléments sont le pape et moi a deux éléments. Mais, puisque $1 = 2$, cet ensemble n'a qu'un élément, ce qui implique que je suis le pape. »

Exercices : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 2

24/09/2012

Les exercices sont à rendre le 01/10/2012 au début du cours.

Les exercices 1 et 4 sont à rédiger et à rendre. Les exercices 2 et 3 sont supplémentaires.

1. Soient E un ensemble et A, B, C et D des parties (ou sous-ensembles) de E.

   (a) Démontrer :

   $$((A \subseteq C) \text{ et } (B \subseteq D) \text{ et } (C \cap D = \emptyset) \text{ et } (A \cup B = C \cup D)) \Rightarrow ((A = C) \text{ et } (B = D)).$$

   (b) Démontrer : $A \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B} \cap C) = A \cup B \cup C$.

2. **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 ?

3. Soient E, F et G des ensembles.

   (a) Soit f une application injective de F dans G ; démontrer :

   $$\forall (g, h) \in \mathcal{F}(E, F), (f \circ g = f \circ h \Longrightarrow g = h).$$

   (b) Soit f une application surjective de E dans F ; démontrer :

   $$\forall (g, h) \in \mathcal{F}(F, G), (g \circ f = h \circ f \Longrightarrow g = h).$$

4. **Fonctions caractéristiques**

   Soit E un ensemble ; on rappelle qu'on note $\mathcal{P}(E)$ l'ensemble des parties de E et $\mathcal{F}(E, \{0, 1\})$ l'ensemble des fonctions de E dans l'ensemble $\{0, 1\}$.

   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 $f(x) \times g(x)$;

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

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

   (c) Quelle est la fonction caractéristique du sous-ensemble $A \setminus B = A \cap \overline{B}$?

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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 3

01/10/2012

Ces exercices qui ne sont pas à rendre et celles des feuilles précédentes vous préparent au devoir surveillé du 11/10/2012.

1. Soient E, F, G des ensembles et $f : E \to F$ et $g : F \to G$ des applications. Démontrez que si f et g sont injectives, alors $g \circ f$ est injective.
2. Soit E l'ensemble des nombres premiers différents de 2. On définit sur E une relation binaire R par :

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

   (a) 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.

   (b) La relation R est-elle une relation d'équivalence ?

3. 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 ?
4. Soit E un ensemble.

   (1) Soient A et B des sous-ensembles de E ; démontrer :

   (a) $A \cap B = \emptyset \iff B \subseteq E \setminus A \iff A \subseteq E \setminus B$;

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

   (2) Soient E, F des ensembles. Par $\mathcal{P}(E)$ et $\mathcal{P}(F)$ on note l'ensemble de toutes les parties de E ou de F respectivement. Donnez soit une preuve soit un contre-exemple à chacune des deux assertions suivantes :

   (a) $\mathcal{P}(E \cap F) = \mathcal{P}(E) \cap \mathcal{P}(F)$.

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

   (3) Soient E un ensemble et $\mathcal{P}(E)$ l'ensemble de toutes les parties de E. Démontrez qu'il n'existe pas d'application surjective $f : E \to \mathcal{P}(E)$.

   Astuce : Pour une telle application f donnée considérer l'ensemble $Y := \{x \mid x \in E, x \notin f(x)\} \in \mathcal{P}(E)$. Est-ce que Y peut être dans l'image de f ?

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.

Pour être plus précis, il faudrait dire que l'hôtel peut toujours accueillir un ensemble *dénombrable* de clients. Par contre, si tous les nombres réels arrivent et chacun veut une chambre, l'hôtel ne suffira pas car l'ensemble des nombres réels n'est pas dénombrable (par l'argument de la diagonale de Cantor).

(Adapté et corrigé de : `http://fr.wikipedia.org/wiki/Hôtel_de_Hilbert`)

Exercices : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 4

08/10/2012

Les exercices sont à rendre le 15/10/2012 au début du cours.

Les exercices 1, 2 et 3 sont à rédiger et à rendre. Les exercices 4, 5, 6 et 7 sont supplémentaires.

1. Démontrer par récurrence :

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

2. Soit E un ensemble à n éléments.
   (a) L'objectif de cette question est de démontrer : $\#\mathcal{P}(E) = 2^n$.
      i. Vérifier le résultat pour n égal à 0, 1, 2 et 3.
      ii. On suppose n supérieur ou égal à 1. On fixe un élément x dans E et on note $\mathcal{P}_x$ l'ensemble des parties de E qui contiennent x, $\mathcal{Q}_x$ l'ensemble des parties de E qui ne contiennent pas x.
      Démontrer $\mathcal{P}(E) = \mathcal{P}_x \sqcup \mathcal{Q}_x$, puis que $\mathcal{P}_x$ et $\mathcal{Q}_x$ ont même cardinal, égal à celui de $\mathcal{P}(E \setminus \{x\})$.
      Indication : donner une bijection entre $\mathcal{P}_x$ et $\mathcal{P}(E \setminus \{x\})$ et une bijection entre $\mathcal{Q}_x$ et $\mathcal{P}(E \setminus \{x\})$.
      iii. Démontrer par récurrence sur n qu'on a $\#\mathcal{P}(E) = 2^n$.
      iv. En utilisant la première question de l'exercice de la feuille 2 sur les fonctions caractéristiques, retrouver le résultat voulu.
   (b) Soient E et F deux ensembles finis de même cardinal n.
   Démontrer par récurrence que l'ensemble des injections de E dans F est de cardinal $n!$, où $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ s'appelle « n factorielle » ou « factorielle (de) n ».
   En déduire que l'ensemble des bijections de E dans lui-même est de cardinal $n!$.
3. (a) Trouvez une application injective et non bijective $f : \mathbb{N} \to \mathbb{N}$.
   (b) Trouvez une application surjective et non bijective $f : \mathbb{N} \to \mathbb{N}$.
   Indication : regarder le cours...
4. Choisir une des variantes du principe de récurrence (autre que le « Changement d'initialisation ») et la démontrer.
5. Que pensez-vous de la preuve suivante ?
   Assertion : Soit C un cours avec n participants. Alors tous les participant sont du même sexe.
   Preuve 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. □
6. Trouver une bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

7. Soient E, F des ensembles finis. Démontrer :
   (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.

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 : `http ://fr.wikipedia.org/wiki/Argument_de_la_diagonale_de_Cantor`)

Exercices : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 5

15/10/2012

Les exercices sont à rendre le 22/10/2012 au début du cours.

Les exercices 2, 3 et 5 sont à rédiger et à rendre. Les exercices 1 et 4 sont supplémentaires.

1. Soit S_4 le groupe symétrique en 4 lettres. Faites la liste de ses éléments. Utilisez 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 $(G, *, e)$ un groupe. On note l'inverse de $a \in G$ par a^{-1}
   (a) Supposons que $(a * b)^{-1} = a^{-1} * b^{-1}$ pour tout $a, b \in G$. Montrer que G est un groupe abélien.
   (b) Supposons que $a^2 * b^2 = (a * b)^2$ pour tout $a, b \in G$. Montrer que G est un groupe abélien.
   (c) Supposons que $a^2 = e$ pour tout $a \in G$ Montrer que G est un groupe abélien.
   Indication : Vous pouvez utiliser (b).
   (d) Montrer 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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 6

22/10/2012

Les exercices sont à rendre le 05/11/2012 au début du cours.
Feuille pour deux semaines.

Les exercices 1, 4, 5 et 6 sont à rédiger et à rendre. Les exercices 2 et 3 sont supplémentaires.

1. Soit n dans $\mathbb{N}_{\geq 1}$; on se place dans le groupe symétrique S_n.
   (a) Démontrer que 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) Démontrer que 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.

2. Cet exercice est une version abstraite de la définition de $\mathbb{Z}$ du cours : il s'agit de construire un groupe (commutatif) à partir d'un monoïde **commutatif** et **régulier**.

   Soit $(M, *, e)$ un monoïde commutatif. On suppose de plus que M est **régulier**, c'est-à-dire qu'il vérifie :
   $$\forall (a,b,c) \in M^3, (a * c = b * c \Longrightarrow a = b)\,.$$
   Démontrer :
   (a) La relation binaire $\sim$ définie sur $M \times M$ par
   $$(a,b) \sim (c,d) \quad \Longleftrightarrow \quad a * d = b * c$$
   est une relation d'équivalence. On note G l'ensemble quotient de M par la relation d'équivalence.
   (b) L'application
   $$\otimes : G \times G \to G, \quad \overline{(a,b)} \otimes \overline{(c,d)} := \overline{(a * c, b * d)}$$
   est bien définie.
   (c) $(G, \otimes, e)$ est un groupe abélien et l'inverse de $\overline{(a,b)}$ est $\overline{(b,a)}$.
   (d) L'application
   $$i : M \to G, \quad n \mapsto \overline{(n,e)}$$
   est injective et satisfait $i(a * b) = i(a) \otimes i(b)$ pour tous $a, b \in M$.

3. Soit $\mathcal{Z}$ l'ensemble quotient de $\mathbb{N}$ par la relation d'équivalence définie en cours. Il a été démontré que 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
   $$\overline{a - b} \;\cdot_{\mathcal{Z}}\; \overline{c - d} = \overline{(ac + bd) - (ad + bc)}.$$
   Posons $1_{\mathcal{Z}} := \overline{(1,0)} = \overline{1 - 0}$. Démontrer :
   (a) $(\mathcal{Z}, \cdot_{\mathcal{Z}}, 1_{\mathcal{Z}})$ est un monoïde abélien.

(b) 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 $a, b, c, d, e, f \in \mathbb{N}$.

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

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

(a) Démontrer que R_n est une relation d'équivalence sur $\mathbb{Z}$.

On l'appelle la « congruence modulo n ». Lorsque a et b sont en relation pour R_n, on note $a \equiv b \mod n$ et on dit que « a et b sont congrus modulo n ».

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

5. Soit $n \in \mathbb{N}$ qui s'écrit dans le système décimal comme $n = c_r c_{r-1} \dots c_1 c_0$ (avec $c_i \in \{0, 1, \dots, 9\}$). Utiliser le calcul de congruence 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.

6. Écrire les tables d'addition et de multiplication de l'anneau $\mathbb{Z}/6\mathbb{Z}$.

À propos.

Charles a un méchant prof qui dit : Au cours d'une des 6 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 été écrite pendant les 5 premières heures, alors, forcément, elle sera écrite la 6ème heure ; ça ne sera pas une surprise ! Alors, forcément, l'interrogation doit être écrite pendant une des 5 premières heures.

Si l'interrogation n'a pas été écrite pendant les 4 premières heures, alors, forcément, elle sera écrite la 5ème heure ; ça ne sera pas une surprise ! Alors, forcément, l'interrogation doit être écrite pendant une des 4 premières heures.

Continuant ainsi, l'interrogation doit forcément être écrite 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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 7

05/11/2012

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé du 15/11/2012.

---

1. Calculer le plus grand commun diviseur de 384 et 90 ainsi que l'identité de Bézout. Utiliser la méthode des matrices.
2. (a) Démontrer que l'anneau résiduel $\mathbb{Z}/51\mathbb{Z}$ n'est pas un anneau intègre.
   (b) Calculer l'inverse de la classe $\overline{16}$ dans $\mathbb{Z}/51\mathbb{Z}$.
3. Soient $x, y \in \mathbb{N}$. Démontrer :
   (a) Un plus petit commun multiple de x et y existe et il est unique.
   (b) On a l'identité $xy = \mathrm{ppcm}(x, y) \cdot \mathrm{pgcd}(x, y)$.
4. Soit $b \in \mathbb{N}_{\geq 2}$. Pour $r_0, r_1, \ldots, r_n \in \{0, \ldots, b-1\}$ on pose
$$m = \sum_{i=0}^{n} r_i b^i = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n.$$
   On utilise aussi la notation $(r_n r_{n-1} \ldots r_1 r_0)_b$ pour m et on dit que r_i est le i-ième chiffre du *développement b-adique de m*.
   Exemple : Pour $b = 10$, le développement 10-adique de 125 n'est rien d'autre que $(125)_{10}$.
   (a) Calculer les chiffres du développement 2-adique de 125.
   (b) Calculer les chiffres du développement 7-adique de 125.
   (c) Démontrer que tout $m \in \mathbb{N}$ possède un développement b-adique.
   Indication : Division euclidienne par b.
   (d) Démontrer que les chiffres dans le développement b-adique d'un $m \in \mathbb{N}$ sont uniques.
5. Soit $n \in \mathbb{N}$. Nous définissons
$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} := \overline{x + y}$$
   et
$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} := \overline{x \cdot y}.$$
   Démontrer : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un anneau commutatif.
   Indication : Utiliser un lemme 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.

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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 8

12/11/2012

Les exercices sont à rendre le 19/11/2012 au début du cours.

Les exercices 1, 3, et 4 sont à rédiger et à rendre. L'exercice 2 est supplémentaire.

1. (a) Calculer le dernier chiffre de 11^n pour tout $n \in \mathbb{N}$ en utilisant les congruences modulo 10.

   (b) Donner et démontrer une règle facile pour le calcul des deux derniers chiffres de 7^n en utilisant les congruences modulo 100.

   Indication : $7^2 = 49$, $7^3 = 343$, $7^4 = 2401$.

2. Nous savons 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 $p_1, \ldots, p_r$ des nombres premiers et $a = p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}$ ainsi que $a = p_1^{f_1} \cdot \cdots \cdot p_r^{f_r}$ avec $e_i, f_i \geq 0$ pour $i = 1, \ldots, r$.

   Exprimer la décomposition de $\mathrm{pgcd}(a, b)$ et $\mathrm{ppcm}(a, b)$ en facteurs premiers. Démontrer la réponse.

3. Soit $\mathbb{Q}$ l'ensemble quotient du cours. Démontrer :

   (a) Les deux applications
   $$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$
   et
   $$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$
   sont bien définies, c'est-à-dire, leurs définitions ne dépendent pas des choix des représentant (a, x) et (b, y) des classes $\frac{a}{x}$ et $\frac{b}{y}$.

   Le cas de $+$ a déjà été traité en cours.

   (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 $\iota(n \cdot m) = \iota(n) \cdot \iota(m)$.

4. Dans ce jeu, pris du livre « Gödel, Escher, Bach » de Hofstadter, nous produisons des chaînes des symboles M, I, U selon quatre règles :

   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-ce possible d'obtenir la chaîne MU en commençant par la chaîne MI en utilisant les règles ci-dessus ?

Indication : Les quatres règles conservent la propriété suivante : le nombre de fois que I apparaît dans la chaîne n'est pas congru à 0 mod 3.

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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 9

19/11/2012

Les exercices sont à rendre le 26/11/2012 au début du cours.

Les exercices 2, 3, 4 et 5 sont à rédiger et à rendre. L'exercice 1 est supplémentaire.

1. Soient X un ensemble non vide et e un élément dans X, fixé. On définit une application $\star$ de $X \times X$ dans X par : $\forall (x, y) \in X \times X, x \star y = e$.
   (a) L'opération $\star$ est-elle associative ?
   (b) L'opération $\star$ est-elle commutative ?
   (c) A-t-on $\forall x \in X, x \star x = e$?
   (d) On suppose dans cette question que $(X, \star)$ est un groupe (donc on suppose que l'élément neutre existe, sans le préciser encore).
      (1) Démontrer que l'élément neutre du groupe $(X, \star)$ est e.
      (2) Démontrer que $X = \{e\}$ (c'est-à-dire, $\forall x \in X, x = e$).
2. Faites la liste complète de tous les sous-groupes de S_3. Lesquels sont cycliques ? Donner un générateur pour tout sous-groupe cyclique.
3. 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) $((\mathbb{Z}/10\mathbb{Z})^\times, \cdot, \overline{1})$
4. 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.
5. Soient $(G, \star, e)$ un groupe et H_1, 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 $H_2 \subseteq H_1$.

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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 10

26/11/2012

Les exercices sont à rendre le 03/12/2012 au début du cours.

Tous les exercices sont à rendre.

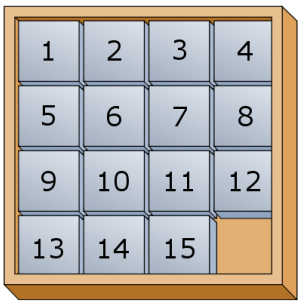
1. Soit $(G, \star, e)$ un groupe. Pour $h \in G$ on définit
$$\sigma_h : G \to G, \quad g \mapsto h \star g \star h^{-1}.$$
   (a) Montrer que pour tout $h \in G$ l'application σ_h est un morphisme de groupes.
   (b) Montrer que σ_h est bijectif en donnant un inverse.

2. 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.

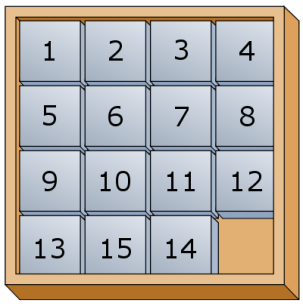
3. Le noyau est de sgn est noté A_n et appelé le *groupe alterné*.
   Faire la liste de tous les éléments du groupe A_4.

4. Vous connaissez certainement le jeu représenté dans l'image. Un coup consiste en le déplacement du trou d'une case à droite, à gauche, en haut ou en bas.

Position initiale



Position finale



   (a) Supposons qu'au début le trou est en bas à droite comme dans l'image.
   Démontrer : Si après n coups le trou se trouve aussi en bas à droite, alors n est pair.
   Indication : Il peut aider de colorer le tableau comme un jeu d'échec.
   (b) Montrer 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).

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 gauffres sont bonnes. Les frites sont bonnes.
Comment les gauffres aux frites doivent être bonnes !"

Exercices : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 11

03/12/2012

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé du 13/12/2012.

---

1. 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.
2. Soit $(G, \star, e)$ un groupe. Pour $h \in G$ on définit
   $$\sigma_h : G \to G, \quad g \mapsto h \star g \star h^{-1}.$$
   Un résultat de la feuille 10 dit que pour tout $h \in G$ l'application σ_h est un automorphisme de G (c'est-à-dire un isomorphisme de $(G, \star, e)$ dans $(G, \star, e)$).
   (a) Démontrer que l'application
   $$\begin{array}{rccc} \varphi : & G & \to & \mathrm{Aut}(G) \\ & h & \mapsto & \sigma_h \end{array}$$
   est un morphisme de groupes.
   (b) Un automorphisme $\sigma : G \to G$ est appelé *intérieur* s'il existe $h \in G$ tel que pour tout $g \in G$ 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. Montrer que tout groupe de cardinal 7 est cyclique.
4. Soient G un groupe et $H \lneq G$ un sous-groupe. Soit $C = G \setminus H$ le complément de H dans G. Démontrer : $\langle C \rangle = G$.
5. Soit $n \in \mathbb{N}_{\geq 1}$. Faites la liste de tous les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$.
6. Soit G un groupe fini et $H_1 \leq G$, $H_2 \leq G$ des sous-groupes de G tels que $H_1 \subseteq H_2$. Démontrer :
   $$(G : H_1) = (G : H_2) \cdot (H_2 : H_1).$$

À propos.

Le théorème de Lagrange affirme notamment : pour un groupe fini G d'ordre n, pour tout sous-groupe H de G d'ordre d, d est un diviseur de n. La « réciproque » du théorème de Lagrange n'est pas toujours vraie : pour un groupe fini G d'ordre n et d un diviseur de n, il n'existe pas toujours de sous-groupe de G d'ordre d. Par exemple : le groupe A_4 (d'ordre 12) n'a pas de sous-groupe d'ordre 6 ; le groupe A_5 (d'ordre 60) n'a pas de sous-groupe d'ordre 15. Vous pouvez essayer de le démontrer !

Exercices : Algèbre 1

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 12

10/12/2012

Les exercices sont à rendre le 17/12/2012 au début du cours.

Tous les exercices sont à rédiger et à rendre.

1. On continue l'exercice 2(b) de la feuille 11. Démontrer :
   (a) Le noyau de l'application $\varphi : G \to \mathrm{Aut}(G)$ est le centre $\mathcal{Z}(G)$ (voir la feuille 9).
   (b) $\mathcal{Z}(G)$ est un sous-groupe normal de G.
   (c) $G/\mathcal{Z}(G)$ est isomorphe à $\mathrm{Inn}(G)$ (c'est-à-dire qu'il existe un isomorphisme de groupes entre ces deux groupes).
2. Soit H un sous-groupe de $(\mathbb{Z}, +, 0)$. Démontrer qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.
   Indication : Regarder l'ensemble $H \cap \mathbb{N}_{>0}$, considérer son plus petit élément (s'il existe) et utiliser la division euclidienne.
3. 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. L'une est la suivante : 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.
4. (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.

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 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 13

17/12/2012

Ces exercices qui ne sont pas à rendre vous aident à mieux comprendre les sous-groupes normaux.

1. Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal.
   Démontrer que $H \cap N$ est un sous-groupe normal de H.
2. Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal.
   Soit $HN := \{hn \mid h \in H, n \in N\}$ et $NH := \{nh \mid n \in N, h \in H\}$.
   Démontrer : $HN = NH$ et HN est un sous-groupe de G.
3. Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal.
   Soit $HN := \{hn \mid h \in H, n \in N\}$, comme dans l'exercice précédent.
   (a) Démontrer : N est un sous-groupe normal de HN.
   (b) On suppose en plus que H est aussi un sous-groupe normal de G.
   Démontrer : HN est un sous-groupe normal de G.

À propos : Le paradoxe de Monty Hall

Vous êtes le 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. 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 ?