MIN17101 – Compléments de mathématiques discrètes
Algèbre et Arithmétique

Jules Baudrin [1], d'après le polycopié de Yann Rotella

Version du 11/09/26

Résumé

Ce polycopié est le support de 3 séances d'1h30 de cours de mathématiques (et des 2/3 séances de TD associées). Il est destiné aux étudiant.e.s en Master 1 d'informatique à l'UVSQ. Il aborde les définitions des structures fondamentales en algèbre (groupe, anneau, corps) et leurs propriétés, mais également les rudiments d'arithmétique nécessaire à tout étudiant en informatique. L'objectif de ce cours de compléments est double : apprendre et/ou revoir des propriétés fondamentales, mais aussi (ou surtout) raisonner et faire preuve de rigueur dans la démonstration d'énoncés mathématiques faisant intervenir peu d'hypothèses. *Les pré-requis sont peu nombreux* : un.e étudiant.e ayant suivi un cours de mathématiques de licence depuis son lycée est tout à fait en mesure de comprendre et réussir dans cette UE. Dit autrement, même si vous êtes fâché.e.s avec les maths, vous pouvez briller dans ce cours !

M1 informatique UVSQ Paris-Saclay 2026 – 2027

1. Toutes les remarques (contenu, typos, imprécisions) sont les bienvenues à jules.baudrin@uvsq.fr.

Table des matières

1 Introduction

Faire de l'exemple la règle. En algèbre, on étudie les propriétés de certaines opérations que l'on peut vouloir faire sur les éléments d'un ensemble donné, à l'instar de la multiplication et de l'addition que vous manipulez depuis quasi toujours. Ces opérations se comportent différemment mais possèdent parfois des propriétés très semblables. À titre d'exemple, on peut par exemple remarquer que l'addition des entiers $a + 0 = a$ est très proche de la multiplication de réels non nuls $a \times 1 = a$ (si l'on est prêt à regarder du même angle le rôle de 0 pour l'addition $+$ et le rôle de 1 pour la multiplication $\times$). Le but de l'algèbre est précisément de partir d'exemples aux propriétés communes, pour construire une définition plus générale faisant des exemples initiaux des cas particuliers. Une fois une telle définition établie, il est alors possible d'étudier *d'un même angle* des structures qui étaient vues comme différentes, mais également de découvrir et classifier tous les objets tombant sous cette nouvelle définition plus générale.

Objectifs du cours. Le but de ce cours est de vous initier à un tel point de vue en étudiant de manière plus constructive les opérations (lois) sur un ensemble. Nous identifierons donc certaines propriétés partagées par les ensembles munis de telles opérations.

Le contenu de ce cours sera immédiatement utile et mobilisable en cryptographie, mais également de manière générale en informatique (et dans d'autres sciences). Plus important peut-être encore que les applications « dans la vraie vie », l'intérêt réside dans une compréhension *profonde* des règles et des structures mathématiques que nous verrons.

Ce cours sert également de remise à niveau et de rappels sur le raisonnement mathématique et la rédaction rigoureuse de preuves simples. Si le côté « abstrait » des définitions peut paraître d'abord déroutant, il faut garder à l'esprit qu'elles sont dépourvues de toutes les propriétés *particulières* que pouvaient avoir nos exemples initiaux, ce qui facilite très souvent la démonstration des propriétés *générales*. Autrement dit, il faut connaître, comprendre et accepter les définitions que nous verrons, et (presque) rien d'autre ne sera nécessaire dans les raisonnements que nous verrons. L'intérêt du cours ne réside donc pas uniquement dans son contenu (les théorèmes) : le formalisme, la rigueur de rédaction et de démonstration sont des compétences attendues dans un master d'informatique, peu importe la nature des sujets étudiés.

2 Lois de composition

Dans cette section, nous estimons connu les définitions d'ensemble et fonctions. Nous abordons en effet les propriétés de fonctions particulières.

2.1 Définitions

Informellement une loi sur un ensemble E, c'est une opération qui permet de transformer deux éléments de E en un autre élément de E. On rappelle que le produit cartésien

de deux ensembles E, F, que l'on note $E \times F$, n'est rien d'autre que l'ensemble formé des paires d'éléments (x, y) où $x \in E$ et $y \in F$.

Définition 2.1 (Loi de composition)**.** Soit E un ensemble. Une *loi de composition* (ou seulement *loi*) sur E est une fonction de $E \times E$ vers E.

En d'autres termes, une loi de composition est une *opération binaire* sur un ensemble. D'après la définition, on peut tout à fait noter une loi sur E comme $f : E \times E \to E$ puisque c'est une fonction. Pourtant, il est beaucoup plus courant d'utiliser un symbole ($*$, $\times$, $\circ$, $+$) plutôt qu'une lettre. De plus, plutôt que d'utiliser la notation *préfixe* utilisée pour les fonctions, nous utilisation la *notation infixe*. Ainsi l'addition de deux entiers naturels a, b par la loi $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ n'est en général pas notée $+(a, b)$, mais plutôt $a + b$ comme vous l'avez toujours fait.

Attention 2.2. Dans la suite de ce polycopié, le symbole $\star$ est utilisé pour désigner une loi quelconque.

Au tableau en revanche, on utilise $\circ$ plus simple à dessiner, mais qui peut être confondu avec la composition de fonctions.

Remarque 2.3. Lorsqu'on s'apprête à utiliser une loi de composition, il convient de *toujours* vérifier que la loi est bien définie, c'est à dire que *toutes* les images appartiennent bien au bon ensemble.

Il faut également garder en tête qu'une loi de composition ne compose pas seulement des nombres, elle peut composer des objets plus compliqués.

Exercice 1. ✍ Donner plusieurs exemples de loi définies sur des ensembles E où $E \neq \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

✍ La division sur $\mathbb{R}$ est-elle une loi ?

À partir d'une loi sur un ensemble E, on peut vouloir *restreindre la loi* à seulement un sous-ensemble $F \subset E$. Ceci n'est néanmoins pas toujours possible. Il faut pour cela que F soit un sous-ensemble *stable*.

Définition 2.4 (Sous-ensemble stable pour un loi)**.** Soit E un ensemble muni de la loi $\star$, et F un sous-ensemble de E. On dit que F est *stable* pour la loi $\star$ si F vérifie :

$$\forall (x, y) \in F \times F, \quad x \star y \in F.$$

Proposition 2.5 (Loi induite)**.** *Soit E un ensemble muni de la loi $\star_E$, et F un sous-ensemble stable pour la loi $\star_E$. Alors F peut être munie de la loi $\star_F : F \times F \to F$ définie par :*

$$\forall (x, y) \in F \times F, \quad x \star_F y \stackrel{\text{def}}{=} x \star_E y\,.$$

Exercice 2. Malgré les apparences, la loi $\star_E$ et la loi $\star_F$ ne sont pas les mêmes lois.

✍ Quelles sont les différences entre $\star_E$ et $\star_F$?

✍ Quel est le problème si F n'est pas stable pour la loi $\star_E$?

En pratique, on ne fait cependant pas apparaître l'ensemble dans la notation de la loi : on utilise $\star$ pour désigner à la fois $\star_F$ et $\star_E$. Il conviendra donc de faire attention.

Exercice 3. ✍ Pourquoi cet abus de notation n'est-il généralement pas problématique ?

✍ Donner des exemples de parties stables pour la multiplication et de l'addition dans $\mathbb{R}$.

✍ Construire une loi de composition sur $E = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ telle qu'il n'y ait pas de partie stable non-triviale.

	♣	♢	♡	♠
♣				
♢				
♡				
♠				

2.2 Propriétés des lois de composition

La définition de loi permet de mettre sur pied d'égalité les opérations d'addition, multiplication, composition de fonctions, multiplications matricielles, *etc.* On peut donc s'intéresser aux propriétés qui sont partagées ou non par ses différentes lois.

Définition 2.6 (Commutativité)**.** Soit $\star$ une loi sur un ensemble E. On dit que la loi $\star$ est *commutative* si :

$$\forall (x, y) \in E \times E, \quad x \star y = y \star x.$$

Définition 2.7 (Associativité)**.** Soit $\star$ une loi sur un ensemble E. On dit que la loi $\star$ est *associative* si :

$$\forall (x, y, z) \in E, \quad (x \star y) \star z = x \star (y \star z).$$

Exercice 4. ✍ Il y a une erreur dans la définition de l'associativité, trouvez-la et corrigez-la.

✍ Donner des exemples de lois associatives et commutatives, associatives et non commutatives, non associatives et commutatives, non associatives et non commutatives.

Remarque 2.8. — Même si la loi n'est pas commutative, il se peut que *certains* éléments $x_0, y_0 \in E$ vérifient, $x_0 \star y_0 = y_0 \star x_0$. On dit alors que x_0 et y_0 commutent pour la loi $\star$.

— Si une loi est associative, une expression de type $a \star u \star v \star b$ et correctement définie sans parenthèse, *c.-à-d. l'ordre de calcul* n'importe pas.

— Si la loi est associative *et* commutative, alors nous pouvons réordonner les éléments et écrire, par exemple $x \star y \star x \star y \star z \star x = x^3 \star y^2 \star z$, à condition de définir $x^n := x \star x \ldots \star x$ pour tout $n \in \mathbb{N}$ et tout $x \in E$. Une telle expression peut être définie par induction.

Exercice 5. ✍ Quel est le problème avec « pour tout $n \in \mathbb{N}$ » dans la remarque juste au dessus ?

✍ La notation x^n est dite « multiplicative ». Quelle serait d'après vous la notation « additive » ?

Vous connaissez également des propriétés qui portent sur des couples de lois.

Définition 2.9 (Distributivité)**.** Soit E un ensemble muni de **deux** lois notées $\bullet$ et $\star$. On dit que la loi $\star$ est *distributive* par rapport à la loi $\bullet$ si pour tout x, y, z dans E :

$$x \star (y \bullet z) = (x \star y) \bullet (x \star z) \quad \text{et} \quad (x \bullet y) \star z = (x \star z) \bullet (y \star z)\,.$$

Pour la première de ces équations on parle de distributivité à gauche, et de distributivité à droite pour la deuxième.

Exercice 6. ✍ Donner des couples de lois qui sont distributives l'une par rapport à l'autre.

✍ Donner des couples de lois qui sont distributives l'une par rapport à l'autre et vice-versa.

✍ Si $\star$ est commutative, comment pouvons-nous réécrire la définition ?

Attention 2.10. N'importe quelle manipulation algébrique comme échanger deux termes, retirer des parenthèses, distribuer ou factoriser des termes sont des manipulations qui *nécessitent d'être justifiées*, en prouvant (ou en mentionnant une hypothèse de

l'exercice) que la loi est commutative, associative ou distributive. Les seules exceptions (et encore...) sont les opérations comme l'addition ou la multiplication dans $\mathbb{Z}$ ou $\mathbb{R}$ car ces propriétés sont considérées comme connues.

2.3 Élément neutre et inversibilité

Nous avons pour le moment présenté les propriétés des lois qui portent sur tous les éléments sans distinction (*c.f.* les symboles « pour tout » dans les définitions de la section précédente). Il existe cependant des éléments avec des propriétés particulières.

Définition 2.11 (Élément neutre)**.** Soit E un ensemble muni d'une loi $\star$. Soit e un élément de E. On dit que e est un *élément neutre* pour la loi $\star$ s'il vérifie la propriété :

$$\forall x \in E, \quad a \star e = e \star a = a\,.$$

Proposition 2.12 (Unicité de l'élément neutre)**.** *Soit $(E, \star)$ un ensemble muni d'une loi. Alors E possède au plus un élément neutre pour $\star$. Autrement dit, soit E ne possède pas d'élément neutre pour $\star$, soit E possède* un unique *élément neutre pour $\star$.*

Démonstration. Par l'absurde, supposons que $(E, \star)$ possède au moins deux éléments neutres. Soit $e_1 \neq e_2$ deux éléments neutres distincts. Alors d'une part puisque e_1 est neutre, on a $e_1 \star e_2 = e_2$ (composer par e_1 ne change pas la valeur). D'autre part, puisque e_2 est neutre on a $e_1 \star e_2 = e_1$. On en déduit donc que $e_1 = e_2$, ce qui contredit l'hypothèse initiale $e_1 \neq e_2$. Cela prouve donc que E possède au plus un élément neutre. □

Exercice 7. ✍ Donner des couples $(E, \star)$ pour lesquels il existe un élément neutre.

✍ Donner des couples $(E, \star)$ pour lesquels il n'y a pas d'élément neutre.

Définition 2.13 (Élément inversible)**.** Soit $(E, \star)$ un ensemble muni d'une loi qui possède un élément neutre e (relativement à la loi $\star$). Soit x un élément de E. On dit que x est *inversible* pour la loi $\star$ s'il vérifie la propriété :

$$\exists y \in E, \quad x \star y = y \star x = e\,.$$

On appelle un tel élément y (s'il existe) un *inverse* de x.

Proposition 2.14 (Unicité de l'inverse)**.** *Soit $(E, \star)$ un ensemble muni d'une loi qui possède un élément neutre e (relativement à la loi $\star$). On suppose de plus que $\star$ est associative. Alors tout élément $x \in E$ possède au plus un inverse (pour $\star$). Autrement dit, soit x ne possède pas d'inverse, soit x possède un inverse et cet inverse est unique.*

Démonstration. Par l'absurde, soit $x \in E$ et supposons que x possède au moins deux inverses $y_1 \neq y_2$ distincts. Alors,

$$y_1 = y_1 \star e = y_1 \star (x \star y_2) = (y_1 \star x) \star y_2 = e \star y_2 = y_2 \,.$$

On en déduit donc que $y_1 = y_2$ ce qui contredit l'hypothèse initiale $y_1 \neq y_2$. Cela prouve donc que x possède au plus un élément neutre. □

Exercice 8. ✍ Dans la preuve ci-dessus, justifier toutes les égalités de l'équation.

✍ Donner la notation d'un inverse en notation additive et multiplicative.

✍ Donner un exemple de couples $(E, \star)$ où aucun élément n'admet un inverse.

✍ Donner un exemple de couples $(E, \star)$ où certains éléments admettent un inverse et d'autres n'admettent pas d'inverse.

✍ Construire une loi de composition sur $E = \{\clubsuit, \diamondsuit, \heartsuit\}$ admettant $\clubsuit$ comme élément neutre et telle que $\diamondsuit$ admette deux inverses. Vérifier que la loi construite n'est pas associative.

	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\clubsuit$			
$\diamondsuit$			
$\heartsuit$			

Proposition 2.15 (L'inverse de l'inverse)**.** *Soit $(E, \star)$ un ensemble muni d'une loi qui possède un élément neutre e (relativement à la loi $\star$). Soit $x \in E$ et $y \in E$ un inverse de x. Alors x est un inverse de y.*

Démonstration. En exercice. □

3 Groupes

Jusqu'à maintenant, les propriétés des lois ont été étudiées séparément. Cependant comme vu avec les précédents exemples, il n'est pas rare qu'un couple $(E, \star)$ vérifient plusieurs propriétés différentes. Toutes les combinaisons de propriétés (ou presque) forme ce que l'on appelle une *structure algébrique*, c'est-à-dire une sorte de modèle ou de prototype d'ensemble avec des propriétés précises. Ces structures sont en pratique très nombreuses.

Dans notre cas, nous allons dans un premier temps considérer l'une des structures les plus simples qui apparaît presque partout en mathématiques : les *groupes*. Plus tard, nous définirons également les structures d'*anneau* et de *corps*, qui sont des groupes avec d'autres propriétés supplémentaires.

3.1 Définitions

Définition 3.1 (Groupe)**.** Soit $(G, \star)$ un ensemble muni d'une loi. On dit que le couple $(G, \star)$ forme un *groupe* si :

(i) G possède un élément neutre e relativement à la loi $\star$;

(ii) la loi $\star$ est associative ;

(iii) tout élément de G est inversible par rapport à la loi $\star$.

Exercice 9. ✍ Réécrire les trois axiomes d'un groupe en écriture mathématique.

✍ Donner des exemples de groupes.

Définition 3.2 (Groupe abélien)**.** Soit $(G, \star)$ un groupe. On dit que le groupe G est *abélien* (ou *commutatif*) si la loi $\star$ est de plus commutative.

Nous avons vu qu'il existe des sous-ensembles $F \subset E$ qui peuvent être munis d'une loi induite d'une loi sur E. Lorsque cette loi munit F d'une structure de groupe, on parle alors de *sous-groupe*.

Définition 3.3 (Sous-groupe)**.** Soit $(G, \star_G)$ un groupe et soit $H \subset G$. On dit que H est un sous-groupe de $(G, \star_G)$ si :

(i) H est stable pour la loi $\star_G$.

(ii) $(H, \star_H)$ est un groupe.

Attention 3.4. Lorsqu'on veut prouver que H est un sous-groupe de G, la première condition est beaucoup trop souvent oubliée. Pourtant c'est « presque » la plus importante : si H n'est pas stable par $\star_G$, alors on ne peut pas définir la loi $\star_H$ sur H. Même si la preuve n'est souvent pas longue, il faut donc commencer par vérifier la stabilité de H.

Exercice 10. ✍ Quelle propriété mathématique faut-il vérifier pour montrer que H est stable par $\star_G$?

✍ Soit $(G, \star_G)$ un groupe quelconque. Donner deux sous-groupes « triviaux » de G.

✍ Donner des exemples de groupes et de sous-groupes non-triviaux.

En pratique, la structure d'un sous-groupe $(H, \star_H)$ et du groupe $(G, \star_G)$ sont très proches, comme énoncé par le lemme ci-dessous.

Lemme 3.5 (Structures communes à $(H, \star_H)$ et $(G, \star_G)$)**.** *Soit $(G, \star_G)$ et $(H, \star_H)$ un sous-groupe de G.*

(i) *Notons e_G le neutre de $(G, \star_G)$ et e_H le neutre de $(H, \star_H)$. Alors $e_G = e_H$.*

(ii) *Soit $x \in H$. Notons x_G^{-1} l'inverse de x relativement à $(G, \star_G)$ et x_H^{-1} l'inverse de x relativement à $(H, \star_H)$. Alors $x_G^{-1} = x_H^{-1}$.*

Démonstration. ***(i)*** Soit $e_H \in H$ le neutre de H. Alors $e_H \star e_H = e_H$. Or $e_H \in G$ donc admet un inverse dans G que l'on note $y \in G$ et qui vérifie $y \star e_H = e_H \star y = e_G$. En multipliant par y des deux côtés de l'égalité $e_H \star e_H = e_H$, on obtient :

$$y \star e_H \star e_H = y \star e_H. \qquad (\triangle)$$

Le membre de gauche de $(\triangle)$ est égal à $y \star e_H \star e_H = (y \star e_H) \star e_H = e_G \star e_H = e_H$ par associativité, puis en utilisant que y est l'inverse dans G de e_H et enfin que e_G est le neutre de G (donc peut être enlevé librement). D'autre part le membre de droite de $(\triangle)$, vérifie $y \star e_H = e_G$ car y est l'inverse de e_H dans G. On en déduit donc que $e_H = e_G$.

(ii) Soit $x \in H$ et x_H^{-1} son inverse dans H. Alors l'inverse vérifie $x \star x_H^{-1} = e_H = e_G$, d'après la définition de l'inverse dans H et le fait que $e_H = e_G$ montré ci-dessus. On en déduit donc que x_H^{-1} est donc aussi un inverse de H pour le groupe $(G, \star)$. Or l'inverse dans un groupe est unique (*c.f.* Proposition 2.14). On en déduit donc que $x_H^{-1} = x_G^{-1}$. □

Autrement dit, quand on regarde un sous-groupe, on ne fait qu'oublier la structure des éléments $x \in G \setminus H$ mais tout le reste est préservé. On en déduit la caractérisation équivalente suivante des sous-groupes.

Proposition 3.6 (Caractérisation équivalente d'un sous-groupe)**.** *Soit $(G, \star_G)$ un groupe. Soit $H \subset G$ un sous-ensemble. Alors H est un sous-groupe de G si et seulement si :*

(i) *$e_G \in H$,*

(ii) *H est stable pour la loi $\star_G$, et*

(iii) *H est stable par inversion : $\forall h \in H, \quad h_G^{-1} \in H$.*

Démonstration. ($\Longrightarrow$) Supposons que H est un sous-groupe. Alors d'après la définition d'un sous-groupe, H admet un élément neutre $e_H \in H$ et d'après le lemme $e_H = e_G$ donc $e_G \in H$. Le point **(ii)** est vérifié par définition d'un groupe. Enfin, soit $h \in H$. Puisque H est un groupe, il existe $h_H^{-1} \in H$. Or d'après le lemme $h_H^{-1} = h_G^{-1}$ donc $h_G^{-1} \in H$.

($\Longleftarrow$) Réciproquement, supposons les trois points vérifiés. Premièrement H est stable pour $\star_G$ d'après le point **(ii)**. La loi $\star_H$ est donc bien définie. Montrons alors que $(H, \star_H)$

est un groupe. Pour cela, on observe que d'après **(i)**, $e_G \in H$. Puisque e_G vérifie $\forall g \in G, e_G \star g = g \star e_G = g$, c'est en partie le cas pour tout $h \in H$ puisque $H \subset G$. L'élément e_G est donc le neutre pour $\star_H$. Montrons enfin que tout élément $h \in H$ admet un inverse dans H. Puisque $(G, \star_G)$ est un groupe il existe un inverse h_G^{-1} de h dans G qui vérifie $h \star h_G^{-1} = h_G^{-1} \star h$. Or d'après le point **(iii)**, h_G^{-1} est un élément de H, c'est donc un inverse de h pour $\star_H$. Ce qui prouve que $(H, \star_H)$ est un groupe. □

Pour alléger les notations, nous ne ferons plus de distinction de notation (sauf lorsque c'est nécessaire) entre les lois $\star_G, \star_H$ qui seront notées $\star$. De même, le neutre sera noté e et l'inverse de x, x^{-1} qu'il s'agisse du groupe G ou d'un sous-groupe H, puisqu'il s'agit des mêmes éléments.

3.2 Groupes finis

Dans la majorité des cas en informatique, les groupes rencontrés sont des groupes finis.

Définition 3.7 (Ordre d'un groupe)**.** L'ordre d'un groupe $(G, \star)$ est le cardinal de G. On dit qu'un groupe est fini si son cardinal est un entier naturel, et infini sinon.

La structure de groupe fini est très bien comprise. Le théorème suivant est l'un des plus fondamentaux dont découlent beaucoup d'autres résultats.

Théorème 3.8 (Théorème de Lagrange)**.** *Soit $(G, \star)$ un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

Démonstration. En exercice (*c.f.* TD). □

Exercice 11. Comme vu dans certains exemples plus haut, pour un groupe fini, on peut écrire la *table* de la loi $\star$. Quelles propriétés cette table admet-elle toujours ?

3.3 Un exemple : le groupe symétrique

Définition 3.9 (Groupe symétrique)**.** Soit $n \geq 1$ un entier naturel non nul. Notons $E_n = \{1, \ldots, n\}$. On appelle *groupe symétrique* d'indice n le groupe de toutes les *bijections* de E_n vers E_n. Le groupe symétrique est aussi appelé groupe de permutations de E_n et il est noté $\mathcal{S}_n$.

Exercice 12. ✍ De quelle loi parle-t-on pour $\mathcal{S}_n$?

✍ Montrer que le groupe de permutations est un groupe.

✍ Quel est l'ordre du groupe symétrique $\mathcal{S}_n$?

4 Anneaux

La définition de groupe est très générale puisqu'elle porte seulement sur une seule loi $\star$. Or, il n'est pas rare (comme déjà évoqué avec la distributivité) qu'un ensemble soit muni de deux lois qui « se comportent bien ensemble » : pensez par exemple aux ensembles des entiers relatifs $\mathbb{Z}$, des réels $\mathbb{R}$, des complexes $\mathbb{C}$, aux matrices carrés (quelles lois ?) ou encore aux fonctions à valeurs réelles (quelles lois ?). Tous les exemples précédents sont *strictement plus structurés* qu'un groupe puisqu'il s'agit de groupes *avec des propriétés en plus*. Notre objectif est donc de définir ces cas particuliers de groupes.

Pour cela nous noterons dans la suite ces deux lois $+$ et $\times$. Nous pourrions tout à fait continuer avec les lois $\star$ et $\bullet$ mais les propriétés que nous décrivons généralisent des propriétés bien connues de $(\mathbb{R}, +, \times)$ par exemple. Il sera donc plus simple d'utiliser ces notations qui sont de plus les notations standards.

4.1 Définitions et propriétés

Définition 4.1 (Anneau)**.** Soit $(A, +, \times)$ un ensemble muni de deux lois. On dit que $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe commutatif,

(ii) la loi $\times$ est associative,

(iii) la loi $\times$ est distributive par rapport à la loi $+$, et

(iv) il existe un élément neutre pour la loi $\times$.

L'élément neutre pour la loi $+$ est noté 0 et l'élément neutre pour $\times$ est noté 1, l'inverse additif de $a \in A$ est notée $-a$, tandis que l'inverse multiplicatif de a, *lorsqu'il existe*, est noté a^{-1}.

Définition 4.2 (Anneau commutatif)**.** On dit qu'un anneau $(A, +, \times)$ est commutatif si la loi $\times$ est commutative.

On rappelle la notation additive suivante :

$$\forall m \in \mathbb{N}, \forall a \in A, \quad m \cdot a \overset{\text{def}}{=} \underbrace{a + \cdots + a}_{m \text{ fois}} .$$

Exercice 13. ✍ L'opération $\cdot$ est-elle une loi au sens de la Définition 2.1 ?

✍ Donner des exemples d'anneaux commutatifs et non commutatifs.

✍ Montrer que si $0 = 1$, alors l'anneau $(A, +, \times)$ est réduit à l'élément nul : $A = \{0\}$.

✍ Montrer les règles de calcul suivantes : pour tout $a, b, c \in A$ et tout $m \in \mathbb{N}$,

(i) $a \times 0 = 0 \times a = 0$.

(ii) $a \times -b = -(a \times b) = (-a) \times b$.

(iii) $(a - b) \times c = ac - bc$.

(iv) $a \times (b - c) = (a \times b) - (a \times c)$.

(v) $a \times (m \cdot b) = (m \cdot a) \times b = m \cdot (a \times b)$.

✍ Que pouvez-vous faire dans un anneau ? Que ne pouvez-vous pas faire ?

4.2 Éléments inversibles et corps

Comme vous avez pu le remarquer, si $(A, +, \times)$ est un anneau, alors ni $(A, \times)$, ni $A \backslash \{0\}$ n'est en général un groupe. Pour construire un groupe, il faut considérer un sous-ensemble particulier de A : l'ensemble des éléments inversibles pour la loi $\times$.

Définition 4.3 ($A^\times$)**.** Soit $(A, +, \times)$ un anneau non réduit à $\{0\}$. L'ensemble des éléments inversibles pour le produit est l'ensemble $A^\times$ défini par :

$$A^\times \stackrel{\text{def}}{=} \{a \in A \mid \exists b \in A, \text{ t.q. } a \times b = b \times a = 1\} .$$

Attention 4.4. Les ensembles $A^\times$ et A^* sont deux notions différentes et tout le monde ne fait pas attention à la notation. La notation A^* signifie « A privé de zéro », c'est-à-dire $A^* \stackrel{\text{def}}{=} A \setminus \{0\}$.

Proposition 4.5 (Groupe des éléments inversibles)**.** *Soit $(A, +, \times)$ un anneau non réduit à $\{0\}$. Alors $(A^\times, \times)$ est un groupe.*

Démonstration. En exercice.

□

Attention 4.6. Même si $A^\times$ est un sous-ensemble de A, cela ne signifie pas que $(A^\times, \times)$ est un *sous-groupe* de A. Cela n'a d'ailleurs pas de sens puisque $(A, \times)$ n'est pas un groupe.

Enfin, nous présentons des cas particuliers d'anneaux (et donc un cas particulier de groupes) encore plus structurés : les corps. Ceux-ci se rapprochent (complètement ?) de ce que vous connaissez puisque $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps. Il en existe bien d'autres.

Définition 4.7 (Corps)**.** Soit $(K, +, \times)$ un ensemble muni de deux lois. On dit que $(K, +, \times)$ est un corps si :

(i) $(K, +, \times)$ est un anneau commutatif non réduit à $\{0\}$, et

(ii) $K^\times = K \setminus \{0\}$, c'est à dire que tout élément non nul de K est inversible pour le produit.

Remarque 4.8. Reprenez la Remarque 4.2. Les corps sont précisément les anneaux pour lesquels la propriété $A^\times = A^*$ est vérifiée, ce qui n'est pas le cas en général pour un anneau quelconque.

4.3 Complément : d'autres éléments remarquables des anneaux

Définition 4.9 (Diviseur de zéro)**.** Soit A un anneau non réduit à $\{0\}$. Soit $a \in A$ tel que $a \neq 0$. On dit que a est un *diviseur de zéro* s'il existe $b \in A, b \neq 0$ tel que $a \times b = 0$ **ou** $b \times a = 0$.

Attention 4.10. C'est justement parce que tous les éléments ne sont pas nécessairement inversibles et/ou qu'il y a des diviseurs de zéro que vous ne pouvez pas nécessairement réaliser les mêmes calculs que dans $\mathbb{R}$.

Exercice 14. ✍ Donner des exemples d'anneaux avec des diviseurs de zéro.

✍ Montrer qu'un diviseur de zéro n'est jamais inversible. Donner un exemple d'un élément non-inversible qui n'est pas un diviseur de zéro (inversibilité et diviseur de zéro ne sont pas des notions équivalentes).

Définition 4.11 (Anneau intègre)**.** On dit qu'un anneau $(A, +, \times)$ est *intègre* s'il est commutatif et sans diviseur de zéro. Un anneau intègre est donc un anneau commutatif qui vérifie la propriété suivante :

$$\forall a, b \in A, \quad [a \times b = 0] \implies [a = 0 \text{ ou } b = 0]\,.$$

Définition 4.12 (Élément nilpotent)**.** Soit A un anneau non réduit à $\{0\}$. Soit $a \in A, a \neq 0$. On dit que a est *nilpotent* s'il existe un entier naturel n tel que

$$a^n = \underbrace{a \times \cdots \times a}_{n \text{ fois}} = 0\,.$$

S'il existe, le plus petit entier n tel que $a^n = 0$ est appelé *indice de nilpotence* de a.

Exercice 15. ✍ Un élément nilpotent est-il un diviseur de zéro ?

✍ Donner un exemple d'élément nilpotent.

5 Arithmétique dans $\mathbb{Z}$

Cette section est consacrée à l'étude de l'ensemble des entiers relatifs $\mathbb{Z}$, à sa structure algébrique mais surtout à son arithmétique, c'est-à-dire à la façon dont on peut effectuer des calculs et étudier les éléments de $\mathbb{Z}$ à partir de ses lois de composition.

Ce n'est pas la seule arithmétique qui existe. Nous étudions plus loin les structures quotients ($\mathbb{Z}/n\mathbb{Z}$), qui sont omniprésentes en informatique, et qui possède une arithmétique particulière : certaines règles seront les mêmes que dans $\mathbb{Z}$ mais d'autres ne le seront pas. En dehors du programme de ce cours, il en existe également d'autres comme l'arithmétique des polynômes ou encore l'arithmétique des ordinateurs qui étudie les règles de calcul que l'on peut faire avec un ordinateur.

5.1 Structure

Théorème 5.1 (Le groupe additif)**.** $(\mathbb{Z}, +)$ *est un groupe abélien dont le neutre est* 0.

Il est également tout à fait possible de caractériser les sous-groupes de $\mathbb{Z}$.

Définition 5.2 (Multiples de n)**.** Soit $n \in \mathbb{N}$. On note $n\mathbb{Z}$ l'ensemble des multiples de n, c'est-à-dire : $n\mathbb{Z} \stackrel{\text{def}}{=} \{nk \mid k \in \mathbb{Z}\}$.

Proposition 5.3 (Sous-groupes de $\mathbb{Z}$)**.** *Les sous-groupes de* $(\mathbb{Z}, +)$ *sont les* $n\mathbb{Z}$*,* $n \in \mathbb{N}$.

Démonstration. Soit $n \in \mathbb{N}$. Montrons d'abord que les $n\mathbb{Z}$ sont des sous-groupes. Tout d'abord, $n\mathbb{Z}$ n'est pas vide puisque $0 = n \times 0 \in n\mathbb{Z}$. De plus $n\mathbb{Z}$ est stable par addition puisque la somme de deux multiples de n est un multiple de n. L'ensemble $n\mathbb{Z}$ est également stable par inverse (additif) puisque l'opposé d'un multiple de n est un multiple de n. Il s'agit donc d'un sous-groupe de $(\mathbb{Z}, +)$.

Réciproquement, soit $H \subset \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Montrons qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$ ce qui prouvera la proposition. Puisque le sous-groupe $\{0\}$ vérifie déjà $\{0\} = 0\mathbb{Z}$, on peut supposer $H \neq \{0\}$. Cela signifie qu'il existe un élément $h \in H$ tel que $h > 0$ ou $h < 0$. Puisque H est un sous-groupe, il est stable par inversion (additive), donc $-h \in H$. L'ensemble $H \cap \mathbb{N}^*$ est donc non vide. Il s'agit d'un sous-ensemble non vide de $\mathbb{N}$ qui admet donc un plus petit élément, que l'on note n. Tout d'abord on observe que $n\mathbb{Z} \subset H$. En

effet, les multiples positifs de n sont dans H par stabilité par l'addition. De plus $-n \in H$ par stabilité par l'inversion (additive) et donc les multiples positifs de $-n$ sont dans H également.

Il nous reste donc à prouver que $H \subset n\mathbb{Z}$. Soit $h \in H$ que l'on suppose positif. Soit $h = nq + r$ la division euclidienne de h par n. Alors par définition $0 \leq r < n$ et il est nécessaire que $r = 0$. En effet, puisque $h \in H$ et $nq \in H$, on a $r = h - nq \in H$. Or n est par construction le plus petit entier strictement positif de H, ce qui n'est possible que si $r = 0$. Donc $h = nq$ et donc $h \in n\mathbb{Z}$. Si h est négatif, la même preuve appliquée à $-h$ montre que $-h \in n\mathbb{Z}$ et donc $h \in n\mathbb{Z}$. Finalement, on a montré que $H = n\mathbb{Z}$. □

Exercice 16. Le premier paragraphe de la preuve est écrite en français. Proposer une version mathématique la plus rigoureuse possible.

Comme déjà mentionné, $\mathbb{Z}$ est encore plus structuré.

Théorème 5.4 (L'anneau $(\mathbb{Z}, +, \times)$)**.** $(\mathbb{Z}, +, \times)$ *est un anneau dont le neutre pour* $\times$ *est* 1*.*

5.2 Divisibilité

En plus des lois $+, \times$, l'ensemble $\mathbb{Z}$ peut être muni d'une *relation* : la *divisibilité*.

Définition 5.5 (Relation)**.** Soit E un ensemble. Une relation sur E est un sous-ensemble $\mathcal{R}$ de $E \times E$, c'est-à-dire une liste de paires d'éléments de E. Si $(x, y) \in \mathcal{R}$ on dit que x est en relation avec y (pour la relation $\mathcal{R}$).

Définition 5.6 (Divisibilité)**.** Soit $a, b \in \mathbb{Z}$. On dit que b *divise* a (ou que b est un *diviseur* de a) ou encore que a *est divisible par* b (ou que a est un *multiple* de b) s'il existe un entier relatif $q \in \mathbb{Z}$ tel que $a = qb$. On note alors $b \mid a$.

Exercice 17. Que peut-on dire de la relation de divisibilité ? Si on la restreint à $\mathbb{N}$?

En munissant l'anneau $(\mathbb{Z}, +, \times)$ de la relation de divisibilité, on obtient un anneau dit *euclidien*, c'est à dire un anneau dans lequel nous pouvons définir une division euclidienne.

Définition 5.7 (Division euclidienne)**.** Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$. Le couple (q, r) est le résultat de la *division euclidienne* de a par b. Dans cette division, a est le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*.

Démonstration. **Unicité.** Soit (q_1, r_1) et (q_2, r_2) deux couples vérifiant les conditions. Alors $bq_1 + r_1 = a = bq_2 + r_2$ donc $bq_1 + r_1 = bq_2 + r_2$. Ainsi, $b(q_1 - q_2) = r_2 - r_1$. Donc b divise $r_2 - r_1$. Or $0 \leq r_1 < b$ et $0 \leq r_2 < b$ donc $-b < r_2 - r_1 < b$. Le seul multiple de b dans l'intervalle $]-b, b[$ est 0 donc $r_2 - r_1 = 0$. D'où $r_1 = r_2$ et $0 = b(q_1 - q_2)$. Or $b \neq 0$ donc nécessairement $q_1 - q_2 = 0$ c'est-à-dire $q_1 = q_2$.

Existence. On considère l'ensemble $E = \{k \in \mathbb{Z} \mid kb \leq a\}$ des multiples de b inférieurs à a. Il s'agit d'une partie non vide et majorée de $\mathbb{Z}$: si $a \geq 0$ alors $0 \in E$ et a majore E car $b \geq 1$. Si $a < 0$ alors $a \in E$ car $ab \leq a$ et 0 majore E car E est constitué d'éléments négatifs. Ainsi E admet un plus grand élément q. On a donc $qb \leq a < (q+1)b$ (sinon $q+1$ serait dans E et donc contredit la maximalité de q). On peut alors poser $r = a - bq$ et r vérifie bien $0 \leq r < b$. □

Notez qu'il existe d'autres anneaux qui peuvent être munis d'une division euclidienne, comme par exemple l'anneau des polynômes à coefficients réels $\mathbb{R}[X]$.

Exercice 18. ✍ Redéfinissez la divisibilité avec la division euclidienne.

✍ Quelle relation d'équivalence pouvez-vous construire sur $\mathbb{Z}$ avec la division euclidienne ?

5.3 PGCD

Vous connaissez très probablement la notion de pgcd comme plus grand diviseur commun. L'objectif de cette partie est de donner une définition équivalente à la définition classique. Cette définition utilise les propriétés de groupe de $\mathbb{Z}$. L'avantage est que les preuves des propriétés du pgcd seront très simplifiées.

Proposition 5.8 (Somme de sous-groupes)**.** *Soit $(G, +)$ un groupe abélien. Soit H et K deux sous-groupes de G. On note $H + K = \{h + k, h \in H, k \in K\}$. Alors $H + K$ est un sous-groupe de G qui contient H et K.*

Démonstration. ✍

□

Comme les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$, le plus grand commun diviseur peut être défini comme suit.

Définition 5.9 (PGCD de deux entiers)**.** Soit a et b deux entiers relatifs. Il existe un unique entier naturel n tel que $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$. On dit que n est le pgcd de a et de b. On notera $n = \mathrm{PGCD}(a, b)$.

Remarque 5.10. Cette définition ne fait pas intervenir la divisibilité (ou plus exactement elle intervient indirectement). On montrera en TD les propriétés calculatoires du pgcd.

Le théorème de Bézout, s'obtient en une ligne à partir de la définition précédente.

Algorithme 1 Algorithme d'Euclide

Entrée : Deux entiers positifs a, b.
Sortie : PGCD(a, b)

1: **Tant que** $b \neq 0$ **faire**
2: $r \leftarrow a \bmod b$
3: $a \leftarrow b$
4: $b \leftarrow r$
5: **fin Tant que**
6: **Retourner** a

Théorème 5.11 (Identité de Bézout)**.** *Soit $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tels que*

$$au + bv = \text{PGCD}(a, b)\,.$$

Démonstration. ✍

□

Cette définition permet également d'obtenir rapidement un moyen calculatoire efficace de calculer le PGCD de deux entiers. Il s'agit de l'algorithme d'Euclide. Nous verrons en TD que les preuves de *terminaison* et *correction* de l'algorithme découlent facilement.

Lemme 5.12. *Soit $a, b, c \in \mathbb{Z}$. Alors* PGCD$(a, b) =$ PGCD$(a + bc, b)$.

Théorème 5.13 (Algorithme d'Euclide)**.** *L'algorithme 1 termine et calcule le pgcd de deux entiers a, b positifs.*

5.4 Primalité

Définition 5.14 (Entiers premiers entre eux)**.** On dit que deux entiers a et b sont premiers entre eux si PGCD$(a, b) = 1$.

Deux entiers premiers entre eux vérifient donc $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Ils engendrent donc $\mathbb{Z}$ *en entier* et non un sous-groupe strict $n\mathbb{Z} \subsetneq \mathbb{Z}$. Pour qu'un sous-groupe $H \subset \mathbb{Z}$ soit égal à $\mathbb{Z}$, il faut et il suffit que $1 \in H$: en effet tout entier peut s'écrire comme une somme 1 ou de -1. On en déduit donc la proposition suivante.

Proposition 5.15 (Théorème de Bézout)**.** *Soit a et b deux entiers relatifs. Alors a et b sont premiers entre eux* si et seulement si *il existe u, v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration. Le sens direct est immédiat d'après l'identité de Bézout. Réciproquement, notons $n =$ PGCD(a, b). S'il existe u, v tq $au + bv = 1$. Alors $1 \in n\mathbb{Z}$. Montrons que $n\mathbb{Z} = \mathbb{Z}$. Soit k un entier positif, alors $k = \underbrace{1 + \cdots + 1}_{k \text{ fois}}$ et $k \in n\mathbb{Z}$ par stabilité par

l'addition. Il en va de même pour les entiers négatifs puisque $-1 \in n\mathbb{Z}$ par stabilité par inversion du groupe $n\mathbb{Z}$ et $-k = \underbrace{-1 + \cdots + (-1)}_{k \text{ fois}}$. Donc $n\mathbb{Z} = \mathbb{Z}$, d'où $n = 1$ car il n'existe qu'un seul générateur positif. □

On peut définir de manière similaire le ppcm de deux entiers.

Proposition 5.16 (Intersection de sous-groupes)**.** *Soit $(G, \star)$ un groupe. Soit H et K deux sous-groupes de G. Alors $H \cap K$ est un sous-groupe de G.*

Définition 5.17 (PPCM)**.** Soit $a, b \in \mathbb{Z}$. Il existe un unique n dans $\mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$. On dit que n est le ppcm de a et de b.

Le pgcd et le ppcm mais surtout la divisibilité nous permettent de classifier les nombres entiers par rapport à une notion très importante : la *primalité*. Les nombres premiers forment une sorte de « base » de tous les nombres, au sens multiplicatif du terme. Nous rappelons la définition et les principaux résultats à connaître.

Définition 5.18 (Nombre premier)**.** On dit que $p \in \mathbb{Z}$ est un nombre premier si $p \geq 2$ et si ses seuls diviseurs sont 1 et p.

Proposition 5.19. *Soit $n \geq 2$ un entier naturel. Alors n est divisible par au moins un nombre premier.*

Proposition 5.20. *L'ensemble des nombres premiers est infini.*

Théorème 5.21 (Décomposition en produit de facteurs premiers)**.** *Soit $n \geq 2$. Alors il existe $m > 0$, $p_1, \ldots, p_m$ des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_m$ des entiers positifs non nuls tels que :*

$$n = \prod_{i=1}^{m} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} .$$

Une telle écriture est unique à l'ordre des facteurs $p_i^{\alpha_i}$ près.

6 Arithmétique modulaire et anneaux quotients $\mathbb{Z}/n\mathbb{Z}$

6.1 Principe

Étant donné un ensemble quelconque (sans structure algébrique particulière), il n'est pas rare de vouloir considérer des éléments distincts comme « similaires », au regard d'un certain critère. Par exemple, étant donnée un groupe d'étudiant.e.s, on pourrait vouloir identifier les étudiant.e.s né.e.s le même mois. On obtient alors une *partition* du groupe en 12 sous-ensembles deux à deux disjoints (puisqu'on ne peut pas être né deux mois

différents). C'est le principe des *relations d'équivalence* (ici notre relation est « être né le même mois que ») : elles permettent de regrouper en *classes* les éléments équivalents entre eux et de *partitionner* l'ensemble en classes deux à deux disjointes.

Définition 6.1 (Relation d'équivalence)**.** Soit E un ensemble et $\mathcal{R}$ une relation sur E. On dit que $\mathcal{R}$ est une relation d'équivalence si elle est :

(i) *réflexive* : $\forall x \in E, \quad x\mathcal{R}x$,

(ii) *symétrique* : $\forall x, y \in E, \quad x\mathcal{R}y \implies y\mathcal{R}x$, et

(iii) *transitive* : $\forall x, y, z \in E, \quad [x\mathcal{R}y \text{ et } y\mathcal{R}z] \implies [x\mathcal{R}z]$.

On notera $\overline{x} \subset E$ la classe de x, c'est à dire le *sous-ensemble* défini par $\overline{x} = \{y \in E \mid x\mathcal{R}y\}$. Étant donné une relation d'équivalence, on peut toujours trouver une suite $(x_i)_{i\in I}$ d'éléments x_i distincts tels que les classes $\overline{x_i}, \overline{x_j}$ sont deux à deux disjointes et tels que : $E = \bigcup_{i\in I} \overline{x_i}$. On dit que les classes d'équivalence partitionnent l'ensemble E.

Exercice 19. Soit $n \in \mathbb{N}^*$. Montrer que la relation définie par « $a \equiv b$ si et seulement si a et b ont le même reste par leur division euclidienne par n » est une relation d'équivalence.

Définition 6.2 (Congruence)**.** Soit n un entier naturel. Deux entiers relatifs a et b sont dits *congrus modulo* n si leur différence est divisible par n, c'est à dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn \iff a - b = kn$.

Exercice 20. ✍ Montrer que la congruence est une relation d'équivalence.

✍ Montrer que la définition de congruence est équivalente à la relation de l'exercice 19.

✍ Donnez les classes d'équivalence pour la congruence modulo 5.

Notation 6.3 (Classe d'équivalence pour la congruence.)**.** *Soit a et n deux entiers. La classe d'équivalence de a pour la congruence modulo n est l'ensemble $a + n\mathbb{Z}$ défini par*

$$a + n\mathbb{Z} := \{a + nk \mid k \in \mathbb{Z}\} .$$

En effet, on remarque :

$$\overline{a} = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, b - a = nk\} = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, b = a + nk\} = a + n\mathbb{Z}\,.$$

Lorsqu'on parle de congruence modulo n, on utilisera donc de manière interchangeable $\overline{a}$ et $a + n\mathbb{Z}$. On remarque également qu'une même classe $a + n\mathbb{Z}$ admet en fait une infinité de *représentants*. En effet, d'après la propriété de transitivité, pour tout $b \in \overline{a}$, on a $\overline{b} = \overline{a}$ ou dit autrement $b + n\mathbb{Z} = a + n\mathbb{Z}$.

Parmi tous les représentants possibles d'un ensemble $a + n\mathbb{Z}$, on choisit souvent a comme étant le plus petit élément positif de la classe, qui est le choix « le plus naturel ». Dans ce cas, les n classes de congruence modulo n sont la classe de 0, ..., la classe de $n-1$, ou encore : $\overline{0}, \ldots, \overline{n-1}$.

6.2 Structure additive et multiplicative des quotients

Soit $n \geq 1$. Alors que $\mathbb{Z}$ est infini, le nombre de classes d'équivalence pour la congruence modulo n est toujours fini (de taille n). On obtient donc un *ensemble* de taille n en considérant l'ensemble $\{\overline{0}, \ldots, \overline{n-1}\}$.

Définition 6.4 (L'ensemble $\mathbb{Z}/n\mathbb{Z}$)**.** Soit n un entier non nul. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ (on parle de $\mathbb{Z}$ *quotienté* par $n\mathbb{Z}$ ou encore d'ensemble quotient) est défini par :

$$\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{\overline{0}, \ldots, \overline{n-1}\} .$$

Remarque 6.5. Dans la première définition de $\mathbb{Z}/n\mathbb{Z}$, a peut varier dans $\mathbb{Z}$, on a donc l'impression que $\mathbb{Z}/n\mathbb{Z}$ est infini *mais ce n'est pas le cas* : même si l'énumération est infinie le *nombre de classes distinctes est fini*.

Comme nous allons le voir, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ hérite de beaucoup de propriétés de $\mathbb{Z}$, tout en étant un ensemble fini. Certaines différences importantes seront tout de même mises en avant.

On peut en fait définir une addition $+_n$ et une multiplication $\times_n$ pour les éléments de $\mathbb{Z}/n\mathbb{Z}$ (c'est-à-dire une addition et une multiplication entre des ensembles). Leurs définitions sont très naturelles : pour tout $a, b \in \mathbb{Z}$, elles sont définies par :

$$\overline{a} +_n \overline{b} \overset{\text{def}}{=} \overline{a+b} \qquad \overline{a} \times_n \overline{b} \overset{\text{def}}{=} \overline{a \times b} .$$

Autrement dit, on définit une addition (resp. multiplication) de classes à partir de l'addition (resp. multiplication) d'entiers qui est déjà définie.

Attention 6.6. La façon dont les opérations sont définies est *a priori* ambiguë. En effet, on les a définies en fonction des représentants a et b, et il se pourrait que d'autres représentants donnent un autre résultat, ce qui voudrait dire que les fonctions $+_n, \times_n$ sont mal définies. Il faut donc vérifier que tout choix de représentants donne le même résultat.

Proposition 6.7 (Les définitions ci-dessus ne sont pas ambiguës)**.** *Soit a_1, b_1, a_2, b_2 tels que $\overline{a_1} = \overline{a_2}$ et $\overline{b_1} = \overline{b_2}$. Alors :*

$$\overline{a_1 + b_1} = \overline{a_2 + b_2} \quad \text{et} \quad \overline{a_1 + b_1} = \overline{a_2 + b_2} .$$

Autrement dit, les fonctions $+_n$ et $\times_n$ sont bien définies.

Démonstration. On prouve le cas de l'addition et le cas de la multiplication est laissé en exercice. Puisque $\overline{a_1} = \overline{a_2}$ et $\overline{b_1} = \overline{b_2}$ alors il existe $k_a, k_b \in \mathbb{Z}$ tels que $a_1 = a_2 + nk_a$ et $b_1 = b_2 + nk_b$. On en déduit donc :

$$\overline{a_1 + b_1} = (a_1 + b_1) + n\mathbb{Z} = (a_2 + b_2) + n(k_a + k_b) + n\mathbb{Z} = (a_2 + b_2) + n\mathbb{Z}\,,$$

où la dernière égalité vient du fait que $n(k_a + k_b) + n\mathbb{Z} = \{n(k_a + k_b) + nk \mid k \in \mathbb{Z}\} = \{n(k_a + k_b + k) \mid k \in \mathbb{Z}\} = \{nk' \mid k' \in \mathbb{Z}\} = n\mathbb{Z}$ où l'on a effectué le changement de variables $k' \leftarrow k_a + k_b + k$. □

Ainsi, $\mathbb{Z}/n\mathbb{Z}$ muni des deux opérations admet une structure algébrique déjà connue.

Théorème 6.8 (L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$)**.** $(\mathbb{Z}/n\mathbb{Z}, +, *)$ *est un anneau commutatif.*

La preuve de ce résultat est laissé à titre d'exercice. Il s'agit d'un exercice *très important* pour maîtriser la différence entre classes et entiers. Chacune des propriétés à prouver (il y a en 8 pour les anneaux commutatifs) provient de la même propriété sur les entiers.

Maintenant, lorsqu'on parle de $\mathbb{Z}/n\mathbb{Z}$, vous savez que chaque élément est une classe de $\mathbb{Z}$ (*c.-à-d.* un sous-ensemble de $\mathbb{Z}$) et vous connaissez les propriétés qui en découlent. Lorsqu'on fait des calculs dans $\mathbb{Z}/n\mathbb{Z}$, on évite cependant de penser aux classes comme des ensembles, on préfère y penser comme des nombres puisque l'addition et la multiplication sont définies exactement comme l'addition et la multiplication d'entiers. Pour simplifier les notations et le raisonnement, on utilise en pratique $+$ et non $+_n$, $\times$ et non $\times_n$, mais aussi a et non plus $\overline{a}$. On écrit seulement « mod n » en fin de ligne pour signifier qu'on travaille modulo n, *c.-à-d.* dans $\mathbb{Z}/n\mathbb{Z}$.

6.3 Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$

On peut également s'intéresser aux éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ car nous avons tous les outils pour les caractériser et pour calculer un inverse multiplicatif lorsqu'il existe.

Proposition 6.9 (Groupe des inversibles $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$)**.** *Soit n un entier. Le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^\times$ est donné par :* $\mathbb{Z}/n\mathbb{Z}^\times = \{x \in \mathbb{Z} \mid \mathrm{PGCD}(x, n) = 1\}$.

Démonstration. ✍

□

Proposition 6.10. *Soit $n \in \mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si* ✍

Le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est une quantité importante, généralement notée $\varphi(n)$.

Définition 6.11 (Fonction indicatrice d'Euler)**.** La fonction indicatrice d'Euler est la fonction $\varphi : \mathbb{N} \to \mathbb{N}$ définie par $\varphi(n) \stackrel{\text{def}}{=} |\{k \mid 0 \leq k \leq n-1 \text{ et } \mathrm{PGCD}(k, n) = 1\}|$.

Théorème 6.12 (Régles de calculs)**.** *Soit φ la fonction indicatrice d'Euler. Les propriétés suivantes sont vérifiées.*

(i) $\varphi(0) = 0$ *et* $\varphi(1) = 1$.

(ii) *Soit p un nombre premier et α un entier strictement positif. Alors* $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(iii) *Soit m, n deux entiers premiers entre eux. Alors* $\varphi(m \times n) = \varphi(m) \times \varphi(n)$.

Théorème 6.13 (Théorème d'Euler-Fermat)**.** *Soit $n \geq 2$ un entier naturel. Soit $a \in \mathbb{Z}$ tel que* $\mathrm{PGCD}(a, n) = 1$, *alors*

$$a^{\varphi(n)} \equiv 1 \mod n\,.$$

Théorème 6.14 (Théorème de Sun Zi (dit des « restes chinois »))**.** *Soit $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux. Alors pour tous entiers $a_1, \ldots, a_k$, le système $x \equiv a_1 \bmod n_1,\ x \equiv a_2 \bmod n_2, \ldots, x \equiv a_k \bmod n_k$ admet une infinité de solutions dans $\mathbb{Z}$, mais une unique solution modulo $n = \prod_{i=1}^{k} n_i$.*