Compléments de mathématiques discrètes
Algèbre et Arithmétique
student

Jules Baudrin*, d'après le polycopié de Yann Rotella

Version du 18 septembre 2025

Faire de l'exemple la règle. En algébre, 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 $+$ et $\times$, ainsi que 0 et 1). 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 que ces lois induisent sur 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 paraitre 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 connaitre, 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,

*Toute remarque, en particulier sur les typos et imprécisions peut m'être adressée à `jules.baudrin@uvsq.fr`.

la rigueur de rédaction et de démonstration étant des compétences attendues dans un master d'informatique, peu importe la nature des sujets étudiés.

1 Lois de composition

1.1 Définitions

Définition 1.1 (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. Généralement nous utilisons un symbole ($*$, $\times$, $\circ$, $+$) et nous notons en notation infixe ($a * b$, $u \circ v$, $g \times h$) à la place de la notation préfixe utilisée pour les fonctions ($*(a, b)$, $\circ(u, v)$, $\times(g, h)$).

✍ Pourquoi binaire ?

✍ Donner plusieurs exemples de loi.

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

Définition 1.2 (Loi induite - Partie stable)**.** Soit E un ensemble muni de la loi $\circ$, et F un sous-ensemble de E. On dit que F est *stable* pour la loi $\circ$ si :

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

La restriction à $F \times F$ de la loi $\circ$ définit alors une loi de composition sur F appelée *loi induite*, généralement notée de la même manière.

✍ Donner des parties stables de 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.

	♣	♢	♡	♠
♣				
♢				
♡				
♠				

1.2 Propriétés particulières

Définition 1.3 (Commutativité)**.** Soit $\circ$ une loi sur un ensemble E. On dit que la loi $\circ$ est *commutative* si :

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

Définition 1.4 (Associativité)**.** Soit $\circ$ une loi sur un ensemble E. On dit que la loi $\circ$ est *associative* si :

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

✍ 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.

Remarques.

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

— Si une loi est associative, une expression de type $a \circ u \circ v \circ b$ et correctement définie sans parenthèse, i.e. *l'ordre de calcul* n'importe pas.

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

✍ Quel est le souci avec "pour tout $n \in \mathbb{N}$" dans la remarque juste au dessus ?

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

Définition 1.5 (Distributivité)**.** Soit E un ensemble muni de **deux** lois $\cdot$ et $\circ$. On dit que la loi $\circ$ est *distributive* par rapport à la loi $\cdot$ si pour tout x, y, z dans E :

$$x \circ (y \cdot z) = (x \circ y) \cdot (x \circ z) \quad \text{et} \quad (x \cdot y) \circ z = (x \circ z) \cdot (y \circ z)\,.$$

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

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

1.3 Élément neutre et inversibilité

Définition 1.6 (Élément neutre)**.** Soit E un ensemble muni d'une loi de composition $\circ$. Soit e un élément de E. On dit que e est un *élément neutre* pour la loi $\circ$ si :

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

Proposition 1.7 (Unicité de l'élément neutre)**.** *Soit $(E, \circ)$ un ensemble muni d'une loi. Alors E possède au plus un élément neutre pour $\circ$. Autrement dit, si E possède un élément neutre pour $\circ$, alors cet élément est l'unique élément neutre.*

✍ Montrer la proposition.

✍ Donner des lois et des ensembles pour lesquel.le.s il existe un élément neutre.

✍ Donner des lois et des ensembles pour lesquel.le.s il n'y a pas d'élément neutre.

Définition 1.8 (Inversible ou symétrisable)**.** Soit E un ensemble muni de la loi $\circ$ qui possède un élément neutre e (relativement à la loi $\circ$). Soit x un élément de E. On dit que x est *inversible* (ou *symétrisable*) pour la loi $\circ$ s'il existe un élément x' de E tel que $x \circ x' = x' \circ x = e$. Si un tel élément existe, il est unique et on l'appelle l'*inverse* de x.

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

✍ Montrez pourquoi (dans le cas où la loi est associative) s'il existe, l'inverse est unique.

2 Groupes

Jusqu'à maintenant, nous avons vu une liste de propriétés étudiées séparément. Dans la suite nous allons plutôt combiner ces propriétés. Les combinaisons étudiées en algèbre sont nombreuses [1]. Dans un premier temps, nous allons nous restreindre à une combinaison particulière de ces propriétés : celle qui forment les *groupes*. Plus tard, nous en étudierons deux autres qui fondent les définitions d'un *anneau* et d'un *corps*.

2.1 Définitions

Définition 2.1 (Groupe)**.** Soit G un ensemble muni d'une loi de composition $\circ$. On dit que $(G, \circ)$, c'est à dire G muni de la loi $\circ$, est un *groupe* si :

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

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

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

1. Voir par exemple les demi-groupes `https://fr.wikipedia.org/wiki/Demi-groupe`.

Si de plus la loi $\circ$ est commutative, on dit que $(G, \circ)$ est un groupe *commutatif* (ou *abélien*).

✍ Donner des exemples de groupes.

✍ Pour un groupe fini, si on écrit la *table* de la loi $\circ$, que pouvons-nous dire sur cette table ?

Définition 2.2 (Sous-groupe)**.** Soit $(G, \circ)$ un groupe et soit $H \subset G$. On dit que H est un sous-groupe de $(G, \circ)$ si :

(i) H est stable pour la loi $\circ$, i.e. $\forall (x, y) \in H^2, x \circ y \in H$;

(ii) muni de la *loi induite*, H est un groupe.

✍ Quels sont les sous-groupes triviaux ?

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

2.2 Groupes finis

Définition 2.3 (Ordre d'un groupe)**.** L'ordre d'un groupe $(G, \circ)$ est le cardinal de G.

Théorème 2.4 (Théorème de Lagrange)**.** *Soit $(G, \circ)$ un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

La preuve est laissée en exercice (TD).

2.3 Le groupe symétrique

Définition 2.5. Pour tout entier $n \geq 1$, on note $E_n = \{1, \dots, n\}$. On appelle *groupe symétrique* d'indice n le groupe noté $\mathcal{S}_n$ de toutes les *permutations* de E_n.

✍ Quel est l'ordre du groupe symétrique ?

3 Anneaux

Pour l'instant, nous n'avons parlé que de structure algébrique avec une seule loi de composition. Or, dans certains cas nous avons envie de faire plusieurs opérations (cf. définition de la distributivité). Maintenant nous allons donc considérer deux lois et pour simplifier la compréhension nous notons ces lois $+$ et $\times$ (une loi notée additivement et une loi notée multiplicativement). Cela vient des propriétés que l'on souhaite pour ces lois pour avoir un anneau et avoir des notations qui "ressemblent" à ce que l'on connaît.

3.1 Définitions et propriétés

Définition 3.1 (Anneau)**.** Soit A un ensemble muni de deux lois de composition, notées $+$ et $\times$. On dit que $(A, +, \times)$ est un anneau si

(i) $(A, +)$ est un groupe commutatif (son neutre est généralement noté 0).

(ii) La loi $\times$ est associative et elle est distributive par rapport à l'addition $(+)$.

(iii) Il existe un élément neutre pour le produit $(\times)$, en général noté 1.

Si de plus la loi $\times$ est commutative, on parle d'anneau *commutatif*.

✍ 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.

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

(i) $a0 = 0a = 0$

(ii) $(a)(-b) = -(ab) = (-a)(b)$

(iii) $(a - b)c = ac - bc$

(iv) $a(b - c) = ab - ac$

(v) $a(mb) = (ma)b = m(ab)$

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

3.2 Éléments remarquables dans un anneau

Proposition 3.2 (Groupe des éléments inversibles)**.** *Soit $(A, +, \times)$ un anneau non réduit à $\{0\}$. On note $A^\times$ l'ensemble des éléments inversibles pour le produit. Alors $A^\times$ est un groupe pour la loi $\times$.*

Définition 3.3 (Diviseurs de zéro)**.** Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A. On dit que a est un *diviseur de zéro* s'il existe b non nul dans A tel que $ab = 0$ **ou** $ba = 0$.

Attention ! C'est justement pour ces raisons et 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 $\mathbb{R}$.

✍ Donner des exemples où on a des diviseurs de zéro.

✍ Montrer qu'un diviseur de zéro ne peut être inversible. Donner un exemple où on a un élément non inversible mais qui n'est pas un diviseur de zéro (inversibilité et diviseur de zéro ne sont pas des notions équivalentes).

Définition 3.4 (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 dans lequel $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Définition 3.5 (Éléments nilpotents)**.** Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A. On dit que a est *nilpotent* s'il existe un entier naturel n tel que $a^n = 0$. Avec ces notations, $\forall p \geq n, a^p = 0$. Le plus petit entier n tel que $a^n = 0$ est appelé *indice de nilpotence* de a.

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

✍ Donner un exemple d'élément nilpotent.

Enfin, la dernière *structure* dont nous allons avoir besoin dans ce cours sont 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 3.6 (Corps)**.** Soit K un ensemble muni de deux lois $+$ et $\times$. On dit que $(K, +\times)$ est un corps si :

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

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

Attention ! $A^\times$ 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 $A^* := A \setminus \{0\}$. La notation $A^\times$ signifie « ensemble des inversibles de A pour la multiplication ». Ces deux sous-ensembles sont égaux dans le cas des corps, mais ce n'est pas vrai pour tous les anneaux !

4 Les nombres entiers, l'arithmétique

À partir de maintenant, nous allons travailler spécifiquement sur l'ensemble des entiers naturels $\mathbb{Z}$.

4.1 Structure

Théorème 4.1 (Le groupe additif)**.** $(\mathbb{Z}, +)$ *est un groupe dont le neutre est* 0*.*

✍ Preuve.

De plus, nous pouvons aussi caractériser les sous-groupes de $\mathbb{Z}$:

Définition 4.2 ($n\mathbb{Z}$)**.** Soit $n \in \mathbb{N}$. On note $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$.

Proposition 4.3 (Sous-groupes de $\mathbb{Z}$)**.** *Les sous-groupes de* $(\mathbb{Z}, +)$ *sont les* $n\mathbb{Z}$*,* $n \in \mathbb{N}$*.*

✍ Preuve.

Et enfin, $\mathbb{Z}$ peut être muni d'une structure d'anneau.

Théorème 4.4 (L'anneau $(\mathbb{Z}, +, \times)$)**.** $(\mathbb{Z}, +, \times)$ *est un anneau dont le neutre pour* $\times$ *est* 1*.*

Et encore plus intéressant, nous pouvons munir cet anneau d'une *relation* appelée *division*.

4.2 Divisibilité

Définition 4.5 (Divisibilité)**.** Soient a et b deux entiers relatifs. On dit que b est un *diviseur* de a ou encore que a est un *multiple* de b et on note $b|a$ s'il existe un entier relatif q tel que $a = qb$.

✍ Rappelez ce qu'est une relation. Que peut-on dire de la relation "division" ? Que peut-on dire si on se restreint à $\mathbb{N}$?

En plus de munir $\mathbb{Z}$ de cette relation, il s'avère que l'anneau $(\mathbb{Z}, +, *)$ est un anneau dit euclidien, c'est à dire un anneau dans lequel nous pouvons définir une division euclidienne comme suit.

Définition 4.6 (Division euclidienne)**.** Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors il existe un unique couple (q, r) de $\mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r \leq b - 1$. 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*.

✍ Preuve.

Notez qu'il existe d'autres anneaux (comme par exemple l'anneau des polynômes) ou les anneaux $\mathbb{Z}/n\mathbb{Z}$ pour lesquels nous pouvons aussi avoir une division euclidienne (avec les polynômes, vous en aurez besoin pour le cours de cryptographie). Si vous vous y intéressez, sachez que nous allons voir en partie les structures quotients $(\mathbb{Z}/n\mathbb{Z})$ à la fin de ce cours, qui sont utiles en informatique, en particulier en cryptographie ou pour la construction de codes correcteurs d'erreurs. Il existe donc d'autres types d'arithmétique que l'arithmétique dite élémentaire : l'arithmétique des polynômes, l'arithmétique modulaire, l'arithmétique des ordinateurs (qui étudie les règles de calcul que l'on peut faire avec un ordinateur), etc.

✍ Redéfinissez la divisibilité avec la division euclidienne.

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

4.3 Tiens une autre manière de définir le PGCD...

Vous connaissez très probablement la notion de pgcd comme plus grand diviseur commun. Afin de voir les liaisons avec le début du cours sur les groupes, nous allons utiliser uniquement la structure de groupe.

Proposition 4.7. *Soit $(G,+)$ un groupe abélien. Soient 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 (abélien) qui contient H et K.*

✍ Preuve.

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

Définition 4.8 (pgcd de deux entiers)**.** Soient 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 $n=\text{pgcd}(a,b)$.

✍ Donc pgcd est une loi de composition. Que pouvons-nous dire sur cette loi ?

Remarque 4.9.
— Tout d'abord, cette définition nous donne directement le théorème de Bezout facilement (voir plus loin).
— Ensuite, remarquez que nous n'avons pas utilisé la divisibilité pour faire cela. À vous de montrer les propriétés du pgcd comme plus grand commun diviseur que vous connaissez (cf TD).

En particulier, ce pgcd nous permet de réaliser l'algorithme d'euclide qui permet de calculer le pgcd de deux entiers.

Proposition 4.10. *Pour tout entier a,b,c, on a*

$$\text{pgcd}(a,b)=\text{pgcd}(a+bc,b)$$

Théorème 4.11 (Algorithme d'Euclide)**.** ✍

4.4 Primalité

Définition 4.12 (Entiers premiers entre eux)**.** On dit que deux entiers a et b sont premiers entre eux si $\text{pgcd}(a, b) = 1$

Deux entiers premiers entre eux permettent donc d'engendrer tout $\mathbb{Z}$ et non un sous-groupe strict de $\mathbb{Z}$ via l'addition. Nous pouvons alors prouver les deux résultats suivants.

Proposition 4.13 (Identité de Bézout)**.** *Soient a et b deux entiers relatifs. Les deux propositions suivantes sont équivalentes.*

(i) *Les entiers a et b sont premiers entre eux.*

(ii) *Il existe u, v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Et de manière plus générale :

Théorème 4.14 (Théorème de Bézout)**.** *Soient a et b non tous nuls, alors il existe u, v dans $\mathbb{Z}$ tels que*

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

✍ Montrez les deux théorèmes précédents.

Définition 4.15 (ppcm)**.** Soient a, b dans $\mathbb{Z}$. 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

✍ Pourquoi est-ce vrai ?

✍ Que dire de la loi induite de cette définition ?

Le pgcd et le ppcm mais surtout la divisibilité nous permettent de classifier les nombre entiers par rapport à une notion très importante : la **primalité**. Ceci est le fondement du cryptosystème RSA et les nombres premiers forment une sorte de base de tous les nombres, au sens multiplicatif du terme.

Définition 4.16 (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.

De là nous pouvons avoir plusieurs résultats qui sont démontrables relativement facilement.

Proposition 4.17. *Tout entier naturel $n \geq 2$ est divisible par au moins un nombre premier.*

Proposition 4.18. *L'ensemble des nombres premiers est infini.*

Théorème 4.19 (Décomposition en produit de facteurs premiers)**.** *Tout entier $n \geq 2$ s'écrit $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ où*

- *m est un entier strictement positif*
- *les p_i sont des nombres premiers deux à deux distincts*
- *les α_i sont des entiers strictement positifs*

Une telle écriture est unique à l'ordre des facteurs près.

5 Algèbre modulaire, classes de congruence

5.1 Principe

Dans un ensemble donné arbitraire (sans parler de structure algébrique particulière), certains éléments peuvent vouloir être considérés comme identiques, au regard d'un certain critère. Par exemple, si j'ai un ensemble de chaises, certaines chaises pourraient être vertes, d'autres rouges, d'autres bleues, etc. En regardant les chaises selon leur couleur et uniquement leur couleur, je pourrais considérer ces chaises comme *équivalentes* au sens de leur couleur, si jamais je veux décorer mon salon d'une certaine manière, alors peut-être que seule la couleur de mes chaises importe. C'est la même chose que l'on souhaite faire ici avec les entiers. Pour cela nous avons besoin d'abord d'une *relation d'équivalence*.

✍ Redonnez ici ce qu'est une relation d'équivalence.

✍ Soit $n \in \mathbb{N}^*$. Montrez que la relation définie par" $a \equiv b$ si et seulement si a et b ont le même reste dans leur division euclidienne par n" est une relation d'équivalence.

✍ Donnez d'autres relations d'équivalences

Une relation d'équivalence permet donc de "couper" notre ensemble en classes dites classes d'équivalence. Plus formellement, une classe d'équivalence est un sous-ensemble et l'ensemble des classes d'équivalences d'un ensemble (construites par rapport à une relation d'équivalence) forment une *partition* de l'ensemble.

Définition 5.1 (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 si a est de la forme $b + kn$ avec k entier.

La congruence est une relation d'équivalence pour tout n non nul.

✍ Montrez que la définition ci-dessus est équivalente à la première définition.

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

Définition 5.2 ($a + n\mathbb{Z}$)**.** Soit a et n deux entiers, l'ensemble $a + n\mathbb{Z}$ est défini par

$$a + n\mathbb{Z} := \{k \in \mathbb{Z}, \exists j \in n\mathbb{Z}, k = a + jn\}$$

Ainsi les classes d'équivalences construites par rapport à la relation de congruence à n sont les $a + n\mathbb{Z}$ pour n'importe quels représentants a. On remarque que plusieurs représentants donnent la même classe d'équivalence, dès que l'on prend des a qui appartiennent à la même classe. Chaque élément d'une classe d'équivalence dans notre cas peut alors être considéré comme un *représentant* d'une classe d'équivalence. Si de plus on munit notre ensemble d'une relation d'ordre, alors nous pouvons définir des représentants *canoniques* en utilisant cet ordre. Dans le cas de l'arithmétique, les représentants canoniques sont les entiers de 0 à $n - 1$ lorsqu'on travaille modulo n.

5.2 Structure additive et multiplicative des quotients

Alors que $\mathbb{Z}$ est infini, pour un n donné, le nombre de classes d'équivalence défini par la congruence modulo n est toujours fini (de taille n). Ceci nous permet de donner une définition d'un ensemble fini, tout en utilisant les propriétés sur les entiers, mais dans un ensemble fini. Cela donnera des propriétés légèrement différentes et assez intéressantes.

Définition 5.3 (L'ensemble $\mathbb{Z}/n\mathbb{Z}$)**.** Soit n un entier non nul. On définit l'ensemble $\mathbb{Z}$ *quotienté* par $n\mathbb{Z}$ noté $\mathbb{Z}/n\mathbb{Z}$ par l'expression

$$\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z}, a \in \mathbb{Z}\}$$

✍ Remarquez que a peut varier dans $\mathbb{Z}$. Définissez alors la relation d'addition entre classes d'équivalence. Que remarquez-vous quand vous additionnez deux classes d'équivalence pour un n fixé ?

✍ Définissez de la même manière la multiplication entre classes de congruences. Que remarquez-vous ?

✍ Montrez alors le théorème suivant en utilisant les propriétés sur les entiers vues précédemment.

Théorème 5.4 (L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$)**.** $(\mathbb{Z}/n\mathbb{Z}, +, *)$ *est un anneau commutatif.*

Comme nous l'avons vu dans le cours précédent, nous pouvons aussi nous demander, comme nous sommes dans un anneau, si cet anneau est intègre, s'il y a des diviseurs de zéro, et quels éléments sont inversibles ou non.

✍ Donner la table de $\mathbb{Z}/6\mathbb{Z}$ et de $\mathbb{Z}/10\mathbb{Z}$.

✍ Quels sont les éléments inversibles ?

✍ Donner le théorème qui caractérise les éléments inversibles.

✍ Prouver le théorème.

✍ Donnez l'algorithme qui permet de calculer l'inverse dans $\mathbb{Z}/10\mathbb{Z}$.

Maintenant, lorsqu'on parle de $\mathbb{Z}/n\mathbb{Z}$, vous savez que chaque élément est une classe de $\mathbb{Z}$ et vous connaissez les propriétés qui en découlent. On peut donc aussi pour se simplifier la vie, enlever la notion de classe et considérer tout simplement n éléments différents et identifier classes d'équivalence avec éléments notés de 0 à $n-1$.

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

Comme nous l'avons vu plus haut, $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des éléments inversibles de l'anneau et constitue un groupe pour la loi $\times$. Vous avez compris ce qui caractérisait les éléments inversibles via le pgcd. On peut vouloir s'intéresser au nombre de ces éléments inversibles. Ce nombre, pour n donné est donné par la *fonction indicatrice d'Euler* (ou indicateur d'Euler ou fonction d'Euler) notée φ ou φ.

Définition 6.1 (Fonction indicatrice d'Euler)**.** La fonction indicatrice d'Euler est une fonction $\varphi : \mathbb{N} \to \mathbb{N}$ définie par

$$n \mapsto \varphi(n) = |\{k | 1 \leq k \leq n \text{ et } \operatorname{pgcd}(k,n) = 1\}|\,.$$

On pourrait vouloir calculer "à la main" la valeur, par exemple en parcourant toutes les valeurs en dessous d'un entier n, calculer le pgcd, et compter.

Théorème 6.2. *Soit φ la fonction indicatrice d'Euler. Alors,*

(i) $\varphi(0) = 0$

(ii) $\varphi(1) = 1$

(iii) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ *pour tout p premier et tout naturel α non-nul.*

(iv) $\varphi(m \times n) = \varphi(m) \times \varphi(n)$ *pour tout entier m, n premiers entre eux.*

Cette fonction indicatrice d'Euler permet alors d'obtenir le résultat suivant.

Théorème 6.3 (Théorème d'Euler-Fermat)**.** *Soit $n \geq 2$ un entier naturel. Soit $a \in \mathbb{Z}$ tel que* $\operatorname{pgcd}(a,n) = 1$*, alors*

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

Théorème 6.4 (Théorème des Restes Chinois)**.** *Soient n et m deux entiers premiers entre eux. Alors pour tout a, b, il existe un unique entier x modulo nm tel que*

$$x \equiv a \mod n \quad \text{et} \quad x \equiv b \mod m\,.$$