Compléments de mathématiques discrètes
Algèbre et Arithmétique

Yann Rotella

2023

Le but de l'algèbre est d'étudier les propriétés de certaines **opérations** que l'on peut vouloir faire dans un ensemble donné, qu'il soit fini ou non. Vous savez déjà réaliser des **calculs** avec des règles bien définies comme la multiplication, la division, l'addition. Vous savez déjà que chacunes de ces opérations se comportent différemment et n'ont pas les mêmes propriétés. Le but de ce cours ici est de voir de manière plus constructive des opérations (lois) différentes et de pouvoir identifier les propriétés que ces lois induisent sur les ensembles que l'on munira de ces opérations.

L'utilité de ce que nous allons voir ici est immédiatement utile en cryptographie et de manière générale en informatique (et dans d'autres sciences). Mais plus important que les applications de ce que nous allons voir ici, l'intérêt réside dans une compréhension *profonde* des règles et des structures de ce que nous utilisons. De plus, ce cours sert aussi à remettre à niveau les raisonnements et à la rédaction de preuves mathématiques simples. Ainsi ce cours n'est pas utile uniquement pour le contenu à proprement parler (les théorèmes du cours), mais il est très utile pour pouvoir faire des preuves dans un contexte de master d'informatique. Il est donc demandé une rigueur dans la rédaction, à garder pendant la suite des études.

1 Lois de composition

1.1 Définitions

Définition 1 (Loi de composition)**.** *Une loi de composition sur un ensemble E quelconque est une fonction de $E \times E$ vers E.*

On peut vouloir parler d'opération (opération binaire) ou simplement de loi. Généralement nous utilisons un symbole ($*$, $\times$, $\circ$, $+$) et nous notons en notation infixe ($a * b$, $u \circ v$, $f \times g$) à la place de la notation préfixe utilisée pour les fonctions.

✍ Pourquoi binaire ?

✍ Donner plusieurs exemples de loi.

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

Définition 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 $\forall (x, y) \in F \times F, x \circ y \in F$. 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 3 (Commutativité)**.** *Soit $\circ$ une loi sur un ensemble E. On dit que la loi $\circ$ est commutative si $\forall (x, y) \in E \times E, x \circ y = y \circ x$.*

Définition 4 (Associativité)**.** *Soit $\circ$ une loi sur un ensemble E. On dit que la loi $\circ$ est associative si $\forall (x, y, z) \in E, (x \circ y) \circ z = x \circ (y \circ z)$.*

✍ 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 poser $x^n = x \circ x \cdots x$ 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 5 (Distributivité)**.** *Soit E un ensemble muni de **deux** lois $\circ$ et $\cdot$. On dit que la loi $\circ$ est distributive par rapport à la loi $\cdot$ si pour tout x, y, z dans E*

$$x \circ (y \cdot z) = (x \circ y) \cdot (x \circ z)$$

et

$$(x \cdot y) \circ z = (x \circ z) \cdot (y \circ z)\,.$$

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

Proposition 1 (Unicité de l'élément neutre)**.** *L'élément neutre de E pour la loi $\circ$, s'il existe est unique.*

✍ 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.

Remarque. On dira plutôt que E possède un élément neutre pour la loi $\circ$.

Définition 7 (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 un ensemble de propriétés séparément. Nous pourrions considérer plusieurs de ces propriétés combinées de manière différentes[1]. Cependant dans ce cours, nous allons nous restreindre à une combinaison particulière de propriétés, celle qui forment les groupes (et plus tard les anneaux et les corps).

[1] `https://fr.wikipedia.org/wiki/Demi-groupe`

2.1 Définitions

Définition 8 (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 $\circ$.

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 9 (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 10 (Ordre d'un groupe)**.** *L'ordre d'un groupe $(G, \circ)$ est le cardinal de G.*

Théorème 1 (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 11. *Pour tout entier $n \geq 1$, on note $E_n = \{1, \ldots, n\}$. 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 12 (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 (ou abélien).

✍ Donner des exemples d'anneaux abéliens et non abéliens

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

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

(1) $a0 = 0a = 0$

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

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

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

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

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

3.2 Éléments remarquables dans un anneau

Proposition 2 (Groupe des éléments inversibles)**.** *Soit $(A, +, \times)$ un anneau non nul. On note $A^\times$ l'ensemble des éléments inversibles pour le produit. Alors $A^\times$ est un groupe pour la loi $\times$.*

Définition 13 (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 14 (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 15 (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, et c'est globalement la dernière *structure* que nous allons avoir besoin dans ce cours: les corps. Ceux-ci se rapprochent (complètement ?) de ce que vous connaissez (en fait $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps). Il en existe bien d'autres.

Définition 16 (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 $\{0\}$.*
- *$K^\times = K^* = K\backslash\{0\}$, c'est à dire que tout élémet 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 !

4 Les nombres entiers, l'arithmétique

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

4.1 Divisibilité

Définition 17 (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 retstreint 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 18 (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 et principalement en cryptographie et 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 ?

4.2 Structure

Théorème 2 (Le groupe additif)**.** $(\mathbb{Z}, +)$ *est un groupe dont le neutre est* 0.

Preuve:
Admis ■

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

Définition 19 ($n\mathbb{Z}$)**.** *Soit* $n \in \mathbb{N}$*. On note* $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$*.*

Proposition 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 3 (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.*

4.3 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. *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 20 (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 1.
- *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 5. *Pour tout entier a, b, c, on a*

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

4.4 Primalité

Définition 21 (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 6 (Identité de Bézout)**.** *Soient a et b deux entiers relatifs. a et b sont premiers entre eux si et seulement si il existe u, v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Et de manière plus générale:

Théorème 4 (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 22 (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 c'est 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 utilisé à la base du cryptosystème RSA et les nombres premiers forment finalement une sorte de base de tous les nombres, au sens multiplicatif du terme.

Définition 23 (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 7. *Tout entier naturel $n \geq 2$ est divisible par au moins un nombre premier.*

Proposition 8. *L'ensemble des nombres premiers est infini*

Théorème 5 (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 24 (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 25 ($a + n\mathbb{Z}$)**.** *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 26 (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 6 (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 27 (Fonction indicatrice d'Euler)**.** *La fonction indicatrice d'Euler est une fonction $\phi : \mathbb{N} \to \mathbb{N}$ définie par*

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

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

(i) $\phi(0) = 0$

(ii) $\phi(1) = 1$

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

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

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

Théorème 8. *Soit $n \geq 2$ un entier naturel. soit $a \in \mathbb{Z}$ tel que* $\operatorname{pgcd}(a, n) = 1$*, alors*

$$a^{\phi(n)} = 1 \mod n .$$

Théorème 9 (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*

$$x = a \mod n \text{ et } x = b \mod m .$$