Algèbre et arithmétique 3

1 Introduction générale

Ce cours, comme son nom l'indique, est la suite logique des cours intitulés *Algèbre et Arithmétique 1 & 2*. Son principe conducteur est de revisiter les résultats d'arithmétique étudiés en AR1 et AR2 (arithmétique des entiers d'une part, des polynômes d'autre part) en les replaçant dans un cadre plus général : celui des « structures algébriques abstraites ». On verra, entre autres exemples,

- que de nombreuses propriétés arithmétiques des entiers et des polynômes sont conséquences du fait « abstrait » suivant : $\mathbf{Z}$ et $\mathbf{K}[X]$ (où $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$) sont des « anneaux principaux » ;
- que le résultat connu sous le nom de petit théorème de Fermat (pour mémoire : si p est un nombre premier et n un entier non divisible par p, alors p divise $n^{p-1} - 1$) n'est qu'un cas très particulier d'un résultat général portant sur les « groupes finis » (et plus précisément sur la relation entre l'ordre d'un élément d'un groupe fini et le cardinal du groupe).

La motivation est double : d'une part ce cours vise la consolidation et (dans une moindre mesure) l'élargissement des connaissances arithmétiques vues en AR1 et AR2, d'autre part il se veut une introduction la plus élémentaire possible à ce formalisme des structures algébriques, notamment aux notions de *groupes* et d'*anneaux*.

Il est certain que lorsqu'on l'aborde pour la première fois, un tel formalisme peut sembler présenter plus d'inconvénients que d'avantages. Il va y avoir une certaine quantité de langage technique à assimiler, pas toujours très digeste, et le niveau d'abstraction est non négligeable. Les exemples concrets d'applications de la théorie générale à l'arithmétique [1] aideront, on l'espère, à adoucir cet aspect austère.

Par ailleurs, le formalisme des structures algébriques présente de multiples avantages qui finissent par surpasser très largement les inconvénients évoqués ci-dessus (même si un peu de temps et de pratique vont être nécessaires pour s'en convaincre). Dans le cadre de cette présentation succincte, on peut en dégager principalement deux.

1. La géométrie est également un réservoir inépuisable d'applications et d'illustrations de la théorie des groupes (pour un début d'explication, vous pouvez aller consulter la page Wikipédia consacrée au *programme d'Erlangen*) ; malheureusement et essentiellement par manque de temps, la géométrie tiendra une place réduite dans ce cours. Signalons que le master 1 de mathématiques de Rennes propose un module intitulé *Théorie des groupes et géométrie*.

Tout d'abord, les résultats obtenus dans le cadre abstrait des structures algébriques vont s'appliquer à énormément de situations différentes, ne se limitant pas, loin de là, au cadre étudié en AR1 et AR2 ni même à l'arithmétique en général [2] ; non seulement la notion de groupe est désormais un outil absolument fondamental de toutes les mathématiques, pures ou appliquées [3], mais elle apparaît également dans d'autres disciplines scientifiques, voire non scientifiques. En fait, en un certain sens, le concept de groupe peut être vu comme l'incarnation mathématique de l'idée naturelle de symétrie [4].

Ensuite, même s'il ne s'agit que de revisiter des résultats arithmétique déjà connus et qu'on peut obtenir par des moyens plus élémentaires, l'approche via les structures algébriques est intéressante et formatrice en termes de compréhension globale des phénomènes mis en jeu, car elle permet de dégager les propriétés (de $\mathbf{Z}$, disons) qui « servent vraiment » dans les démonstrations. Pour donner un exemple précis, la notion d'anneau principal, une fois correctement maîtrisée, apporte un éclairage extrêmement enrichissant sur la bonne vieille notion de pgcd et ses propriétés. C'est pour cela que posséder quelques notions, même rudimentaires, sur ces structures algébriques, est extrêmement utile notamment [5] à ceux qui se destinent à l'enseignement dans le primaire et le secondaire, car cela leur apportera le recul nécessaire à une diffusion sereine et maîtrisée des connaissances mathématiques au programme des classes qu'ils auront en charge [6].

Nous commençons ce cours par une petite introduction à la théorie des groupes. Nous donnerons le plus d'exemples possible pour illustrer la théorie.

La deuxième partie est consacré aux propriétés spécifiques de $\mathbf{Z}$ en tant que groupe mais aussi en tant qu'anneau, structure algébrique qu'on introduira alors. On parlera également de la notion délicate de structure quotient et d'un exemple qui va beaucoup nous occuper : les anneaux quotients $\mathbf{Z}/N\mathbf{Z}$.

La troisième partie est consacrée à l'arithmétique des polynômes. À cette occasion, on introduit la notion d'anneau principal. On explique un procédé général de construction, par quotient, d'objets algébriques appelés les « corps finis ».

2. Soulignons cependant encore une fois que dans le cadre de ce cours, on se limitera presque exclusivement à des applications arithmétiques, sans épuiser d'ailleurs, loin de là, les champs d'applications dans ce domaine précis.

3. Pour ne citer qu'un exemple : la topologie, discipline *a priori* assez éloignée de l'algèbre, utilise désormais tout un arsenal de techniques basées sur les structures algébriques, dont vous pourrez éventuellement avoir un aperçu en M1 de mathématiques ; la « topologie algébrique » est devenue une discipline mathématique à part entière.

4. « naturelle » au sens : « physique, qui vient de la nature » ; quelques suggestions de lectures parmi d'autres pour approfondir ce point de vue : *Symmetry* d'Hermann Weyl, *Finding moonshine* de Marcus du Sautoy ; le second est beaucoup plus récent et plus abordable ; les deux ouvrages ont été traduits en français ; le titre français du second est *La symétrie ou les maths au clair de lune* ; sachez que le terme « clair de lune » contient une allusion mathématique à la théorie des groupes.

5. « même », diraient certains...

6. Ce type de remarque vaut plus généralement pour beaucoup de notions mathématiques que ces aspirants enseignants auront vues en licence et dont on entend malheureusement trop souvent dire qu'« elles ne leur serviront plus jamais ensuite, puisqu'ils n'auront pas à les enseigner ».

La quatrième partie, assez courte, revient sur la notion de groupe cyclique, déjà entrevue dans la première partie. Le résultat principal est que le groupe multiplicatif d'un corps fini est cyclique.

La cinquième partie étudie la structure d'une famille particulière de groupes finis : les groupes de permutations d'ensembles finis.

Enfin, la sixième partie introduit un nouvel anneau, l'anneau des entiers de Gauss, dont on étudie l'arithmétique en s'appuyant notamment sur la théorie développée dans les premières parties. On en déduit la résolution d'un problème d'arithmétique sur $\mathbf{Z}$: la description des nombres premiers qui s'écrivent comme somme de deux carrés.

Ce texte est parsemé d'exercices dont le but premier est en général de s'assurer de la compréhension élémentaire des notions introduites. Il est donc plus que conseillé de chercher ces exercices (noter à cet égard la convention introduite à partir de l'exercice 18). Les questions en séance de cours pourront être notamment l'occasion de discuter du contenu de ces exercices.

2 Introduction à la notion de groupe

2.1 Une première approche : le groupe des permutations d'un ensemble et ses sous-groupes

2.1.1 Permutations d'un ensemble

Définition 2.1 *Soit E un ensemble. Une permutation de l'ensemble E est une application bijective de E sur E. On note $\mathfrak{S}_E$ l'ensemble des permutations de E.*

Exemple 2.2 : L'ensemble $\mathfrak{S}_E$ n'est jamais vide[7], car il contient toujours l'application identique de E, notée Id_E et qui vérifie, pour tout $x \in E$, $\mathrm{Id}_E(x) = x$. □

Exercice 1

Pour $E = \{0\}$ puis pour $E = \{0, 1\}$, décrire $\mathfrak{S}_E$. Donner quelques éléments de $\mathfrak{S}_{\mathbf{R}}$.

Proposition 2.3 *Soit E un ensemble et f et g deux éléments de $\mathfrak{S}_E$. Alors*

- *l'application composée $f \circ g$ est un élément de $\mathfrak{S}_E$*
- *On a*
$$\forall (f, g, h) \in \mathfrak{S}_E^3, \quad f \circ (g \circ h) = (f \circ g) \circ h$$
- *On a*
$$\forall f \in \mathfrak{S}_E, \quad f \circ \mathrm{Id}_E = \mathrm{Id}_E \circ f = f$$

7. même si E est vide !

- *On a*

$$\forall f \in \mathfrak{S}_E, \quad \exists g \in \mathfrak{S}_E, \quad f \circ g = g \circ f = \mathrm{Id}_E$$

Les démonstrations sont laissées en exercices (*cf.* feuille de TD 1). La première propriété nous dit en particulier qu'on peut définir une application

$$\begin{array}{ccc} \mathfrak{S}_E \times \mathfrak{S}_E & \longrightarrow & \mathfrak{S}_E \\ (f, g) & \longmapsto & f \circ g \end{array} .$$

2.1.2 Sous-groupe de l'ensemble des permutations d'un ensemble

Pour diverses raisons, on a souvent envie de travailler non pas avec toutes les permutations d'un ensemble mais seulement avec une certaine partie, caractérisée par une certaine propriété. Par exemple, si E est un espace vectoriel et on fait de l'algèbre linéaire, les seules permutations qui nous intéressent a priori sont celles qui sont en outre des applications linéaires.

Définition 2.4 *Soit E un ensemble. Un* sous-groupe de $\mathfrak{S}_E$ *est une partie G de $\mathfrak{S}_E$ qui vérifie les propriétés suivantes :*

- Id_E *est dans G ;*
- *pour tout élément f de G, f^{-1} appartient aussi à G ;*
- *pour tout couple (f, g) d'éléments de G, $f \circ g$ appartient aussi à G.*

Exemple 2.5 : $\{\mathrm{Id}_E\}$ et Sym_E sont des sous-groupes de Sym_E (le vérifier). On verra beaucoup d'autres exemples (et contre-exemples) dans le TD 1. □

Remarque 2.6 : On verra un tout petit peu plus loin que Sym_E (« muni » de la composition des applications) est ce qu'on appelle un groupe, et on donnera la définition plus générale d'un sous-groupe d'un groupe ; bien entendu, pour les sous-groupes du groupe Sym_E, on retrouvera la définition ci-dessus. □

Exercice 2

Montrer que l'intersection de deux sous-groupes de $\mathfrak{S}_E$ est encore un sous-groupe de $\mathfrak{S}_E$. Généraliser à l'intersection d'un nombre fini de sous-groupes, voire...

2.1.3 Loi de composition interne

Définition 2.7 *Une loi de composition interne sur un ensemble F est une application $F \times F \to F$*

Une loi de composition interne peut donc être vue comme une « règle » qui à tout couple d'éléments de E associe un autre élément de E.

Exemple 2.8 : L'addition est une loi de composition interne sur $\mathbf{Z}$. On a vu ci-dessus que l'application $(f, g) \mapsto f \circ g$ est une loi de composition interne sur $\mathfrak{S}_E$. Plus généralement,

si G est un sous-groupe de $\mathfrak{S}_E$, la définition montre que l'application

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (f,g) & \longmapsto & f \circ g \end{array}$$

est bien définie ; c'est donc une loi de composition interne sur G. On l'appelle la loi de composition interne induite par la composition sur G. □

Exercice 3

Donner d'autres exemples de lois de composition interne sur $\mathbf{Z}$. L'application $(n,m) \mapsto (n-m)$ définit elle une loi de composition interne sur $\mathbf{N}$?

La définition d'une loi de composition interne est « peu exigeante », et en général une loi de composition interne quelconque n'a guère d'intérêt. Pour pouvoir travailler efficacement avec une loi de composition interne, il faut lui imposer des propriétés supplémentaires. Par exemple la proposition 2.3 montre que la loi de composition interne définit par la composition sur $\mathfrak{S}_E$ ou plus généralement sur un sous-groupe de $\mathfrak{S}_E$ a des propriétés intéressantes. C'est en fait ce type de propriété qui va caractériser, de manière plus générale [8], les ensembles muni d'une loi de composition interne que l'on va appeler « groupes ».

2.2 Définition d'un groupe

2.2.1 Notion d'associativité, d'élément neutre et de symétrique

Définition 2.9 *Soit $(F,\star)$ un ensemble muni d'une loi de composition interne $(f,g) \mapsto f\star g$.*

- *La loi $\star$ est dite* associative *si on a*

$$\forall (f,g,h) \in F^3, \quad f \star (g \star h) = (f \star g) \star h$$

- *Un* élément neutre *pour la loi $\star$ est un élément e de F vérifiant*

$$\forall f \in F, \quad f \star e = e \star f = f.$$

Remarque 2.10 : L'associativité permet de se passer de parenthèses dans les « compositions multiples ». Par exemple, si $\star$ est associative, on pourra écrire sans risque de confusion des expressions comme

$$f_1 \star f_2 \star f_3 \star f_4.$$

A priori, cette expression pourrait s'interpréter comme $(f_1 \star f_2) \star (f_3 \star f_4)$ ou $(f_1 \star (f_2 \star (f_3 \star f_4)))$ ou de bien d'autres façons encore. L'associativité nous dit que toutes les façons dont on peut placer les parenthèses de façon à donner un sens rigoureux à l'expression donnent le même résultat. □

Proposition 2.11 *Soit $(F,\star)$ un ensemble muni d'une loi de composition interne. On suppose que $\star$ admet un élément neutre. Alors il est unique.*

8. En fait, cette plus grande généralité n'est en un sens qu'apparente ; c'est en substance ce que nous dit le théorème de Cayley, énoncé plus loin.

Démonstration laissée en exercice (*cf.* exercice 7 du TD 1)

Définition 2.12 *Soit $(F, \star)$ un ensemble muni d'une loi de composition interne admettant un élément neutre, noté e. Soit $f \in F$. Un* symétrique *de f pour $\star$ est un élément $g \in F$ vérifiant*

$$g \star f = f \star g = e.$$

Proposition 2.13 *Soit $(F, \star)$ un ensemble muni d'une loi de composition interne associative et admettant un élément neutre. Alors il est unique. Soit $f \in F$. Si f admet un symétrique, ce symétrique est unique.*

Démonstration laissée en exercice (*cf.* exercice 7 du TD 1)

2.2.2 Définition d'un groupe

La proposition 2.3 montre que la loi de composition interne sur $\mathfrak{S}_E$ définie par la composition des applications a les propriétés suivantes : elle est associative, admet un élément neutre et tout élément admet un symétrique. Il en est de même pour la loi de composition induite sur tout sous-groupe de $\mathfrak{S}_E$ (attention, il y a une petite subtilité dans cette assertion).

Définition 2.14 *Un groupe est un couple $(G, \star)$ où G est un ensemble et $\star$ une loi de composition interne associative sur G, admettant un élément neutre, et tel que tout élément de G admet un symétrique.*

Il est à noter qu'en vertu de ce qui a été vu ci-dessus, dans un groupe l'élément neutre est unique et tout élément admet un unique symétrique (ces propriétés *découlent* de la définition et n'en font pas partie).

Exercice 4

Montrer que $(\mathfrak{S}_E, \circ)$, $(\mathbf{Z}, +)$, $(\mathbf{R}^\times, \times)$, et $(\{0, 1, \ldots, N-1\}, \oplus)$ (où pour $m, n \in N$, $m \oplus n$ est le reste de la division euclidienne de $m + n$ par N) sont des groupes.

Pour des raisons qui seront explicitées plus loin, dans la pratique on utilisera rarement la définition ci-dessus pour montrer qu'un ensemble muni d'une loi de composition interne est un groupe.

Définition 2.15 *Soit $(G, \star)$ un groupe d'élément neutre e. Un* sous-groupe *de G est une partie H de G vérifiant les propriétés suivantes :*

- *e est dans H ;*
- *pour tout élément f de H, le symétrique de f appartient aussi à H ;*
- *pour tout couple (f, g) d'éléments de H, $f \star g$ appartient aussi à H.*

Exemple 2.16 : Si e est l'élément neutre du groupe G, G et $\{e\}$ sont toujours des sous-groupes de G (le vérifier).

Si G est un sous-groupe de $\mathfrak{S}_E$ au sens de la définition 2.4, G est un sous-groupe du groupe $(\mathfrak{S}_E, \circ)$, et réciproquement (*cf.* la remarque 2.6). □

Définition 2.17 *Un groupe $(G, \star)$ est dit* commutatif *(ou* abélien*) si la loi $\star$ est commutative, en d'autres termes vérifie la propriété*

$$\forall (g,h) \in G^2, \quad g \star h = h \star g.$$

Exemple 2.18 : $(\mathbf{Z}, +)$ est un groupe commutatif ; $\mathfrak{S}_{\{1,2\}}$ également. □

Exercice 5

Donner d'autres exemples de groupes commutatifs. $\mathrm{GL}_2(\mathbf{R})$ est-il commutatif ? Montrer que le groupe $\mathfrak{S}_{\{1,2,3\}}$ n'est pas commutatif. Montrer plus généralement que si E est un ensemble de cardinal au moins 3, le groupe $\mathfrak{S}_E$ n'est pas commutatif.

2.2.3 Puissances itérées d'un élément d'un groupe

C'est une notion capitale.

Définition 2.19 *Soit $(G, \star)$ un groupe dont on note e l'élément neutre. Soit $g \in G$. On définit, pour tout $n \in \mathbf{Z}$, un élément $g^{\star n} \in G$ de la façon suivante :*

1. *on définit par récurrence $g^{\star n}$ pour tout $n \in \mathbf{N}$ en posant $g^{\star 0} = e$ et*

$$\forall n \in \mathbf{N}, \quad g^{\star(n+1)} = g \star g^{\star n}.$$

2. *Soit h le symétrique de g. Pour $n \in \mathbf{Z} \setminus \mathbf{N}$, on pose $g^{\star n} = h^{\star(-n)}$.*

On peut énoncer et démontrer quelques règles de calcul, que vous connaissez a priori déjà au moins pour des exemples particuliers de groupes (lesquels ?).

Proposition 2.20 *[Règles de calcul des puissance] Soit $(G, \star)$ un groupe dont on note e l'élément neutre. Soit $g \in G$.*

On a $g^{\star 0} = e$ et $g^{\star 1} = g$; $g^{\star(-1)}$ est le symétrique de g.

On a

$$\forall (n,m) \in \mathbf{Z}^2, \quad g^{\star(m+n)} = g^{\star m} \star g^{\star n} = g^{\star n} \star g^{\star m}$$

$$\forall (n,m) \in \mathbf{Z}^2, \quad (g^{\star m})^{\star n} = g^{\star m\, n}$$

Soit h un autre élément de G. On suppose que g et h commutent, c'est-à-dire $g \star h = h \star g$. Alors on a

$$\forall n \in \mathbf{Z}, \quad (g \star h)^{\star n} = g^{\star n} \star h^{\star n} = h^{\star n} \star g^{\star n}$$

Les démonstrations se font par récurrence et sont laissées à titre d'exercices.

Exercice 6

Soit $(G, \star)$ un groupe, g et h des éléments de G qui commutent. Montrer que pour tout couple $(n, m) \in \mathbf{Z}^2$, $g^{\star n}$ et $h^{\star m}$ commutent.

2.2.4 Notations : abus de notation, notations multiplicative et additive

En toute rigueur, un groupe, en tant qu'objet mathématique, est un *couple* $(G, \star)$, où G est un ensemble et $\star$ une loi de composition interne sur G. Très souvent la loi de composition interne n'est pas explicitement indiquée. On verra par exemple très souvent des expressions du genre « Soit G un groupe... » ou « Considérons le groupe $\mathfrak{S}_E$ des permutations de E... ». C'est en toute rigueur un abus de notation mais qui est très largement toléré et pratiqué, et il en sera de même dans ce module. Le lecteur attentif aura d'ailleurs remarqué que cet abus a en fait déjà été pratiqué antérieurement dans ce texte. La plupart du temps, les problèmes créés par cet abus sont minimes [9], soit parce que la loi de composition interne utilisée est « évidente » (par exemple, pour $\mathfrak{S}_E$, il s'agit a priori de la composition), soit parce que l'on va adopter une des deux notations « génériques » traditionnelles pour exprimer la loi de composition interne d'un groupe, à savoir la *notation multiplicative* ou la *notation additive*. Le tableau ci-dessous en donne les principales caractéristiques. On insistera très lourdement sur le fait que la notation additive est STRICTEMENT réservée à des groupes *commutatifs* ; cette règle est absolument inviolable, car les risques de confusion causés par son non-respect sont assez graves. Par ailleurs le fait qu'un groupe soit commutatif n'entraîne pas systématiquement que l'on emploie la notation additive pour ce groupe. La notation multiplicative s'emploie a priori pour n'importe quel type de groupe.

Notation spécifique	Notation multiplicative	Notation additive
$g \perp h$	$g.h$ ou gh	$g + h$
$g^{\perp n}$, $n \in \mathbf{Z}$	g^n	$n.g$ ou $n\,g$
élément neutre, e	1 ou e	0
« symétrique de g », $g^{\perp(-1)}$	« inverse de g », g^{-1}	« opposé de g », $-g$

Exercice 7

Réécrire les règles de calculs des puissances en notation multiplicative puis en notation additive.

Par notation spécifique, on entend que l'on a choisi un symbole particulier pour désigner la loi du groupe sur lequel on travaille. Dans les exemples donnés par le tableau, ce symbole est $\perp$; jusqu'ici on avait surtout utilisé $\star$; a priori n'importe quel symbole qui n'a pas déjà

9. ou plutôt « devraient être minimes » ; la pratique montre que ça n'est pas toujours le cas pour beaucoup d'étudiants ; n'hésitez pas à solliciter les enseignants en cas de doute ! Le moindre abus de notation reste finalement potentiellement dangereux au niveau pédagogique.

une signification mathématique standard dans le contexte où l'on se trouve convient ; par ailleurs si on travaille avec un groupe de permutation on peut bien sûr utiliser le symbole $\circ$.

La frontière est parfois un peu floue entre notations spécifique et multiplicative. Par exemple, même quand la loi de groupe est désignée par un symbole spécifique, disons $\perp$ pour l'exemple, les puissances itérées $g^{\perp n}$ sont très souvent notées simplement g^n. Ainsi la formule de calcul des puissances

$$g^{\perp n} \perp g^{\perp m} = g^{\perp (m+n)}$$

s'écrira plus simplement

$$g^n \perp g^m = g^{m+n}.$$

On prendra bien garde en revanche à ne *jamais* mélanger la notation additive avec l'une des deux autres notations. Sinon, c'est le désastre assuré...

2.2.5 Sous-groupe engendré par une partie

Théorème 2.21 *Soit G un groupe noté multiplicativement et $\mathcal{P}$ une partie de G. Il existe un unique sous-groupe H de G vérifiant les deux propriétés suivantes :*

1. *$\mathcal{P} \subset H$*
2. *si H' est un sous-groupe de G contenant $\mathcal{P}$, alors $H \subset H'$.*

Démonstration : Unicité : si H_1 et H_2 vérifient les deux propriétés, on a $H_1 \subset H_2$ et $H_2 \subset H_1$ d'où $H_2 = H_1$.

Existence : il existe un sous-groupe de G contenant $\mathcal{P}$: G lui-même. L'intersection de tous les sous-groupes de G contenant $\mathcal{P}$ est un sous-groupe (*cf.* exercice 2) vérifiant les propriétés demandées. □

Dans la pratique, on a souvent besoin d'une description relativement explicite du sous-groupe engendré par une partie, que ne fournit pas la construction de la démonstration précédente. Une telle description existe notamment quand la partie $\mathcal{P}$ est réduite à un élément.

Théorème 2.22 *Soit G un groupe noté multiplicativement et g un élément de G. Le sous-groupe de G engendré par $\{g\}$ est*

$$\{g^n, \quad n \in \mathbf{Z}\}$$

Démonstration : exercice 4 du TD 1 □

Exercice 8

Soit G un groupe noté multiplicativement, g et h des éléments de G qui commutent. Montrer que le sous-groupe de G engendré par $\{g, h\}$ est

$$\{g^n\, h^m, \quad (n, m) \in \mathbf{Z}^2\}$$

(indication : faites d'abord l'exercice 8 du TD 1).

2.2.6 Structure de groupe sur un sous-groupe

Soit $(G, \star)$ un groupe et H un sous-groupe de G. En particulier pour tout couple (h, h') d'élément de H, $h \star h'$ est encore un élément de H. Ainsi $\star$ induit une loi de composition interne $\star_H$ sur H, et on vérifie que $(H, \star_H)$ est un groupe [10]. On dit que H a été muni de la structure de groupe induite par celle de G. Par la suite tout sous-groupe d'un groupe sera systématiquement muni de la structure de groupe induite. Quasi-systématiquement, $\star_H$ sera notée $\star$, même si en toute rigueur, $\star$ et $\star_H$ désignent des objets mathématiques différents. D'ailleurs assez souvent les notations multiplicatives ou additives sont utilisées, et ce sont évidemment « les mêmes » pour G et pour H.

En particulier, tout sous-groupe d'un groupe de permutations $\mathfrak{S}_E$ est un groupe (pour la loi de composition interne donnée par la composition des applications). Le théorème de Cayley (qui ne sera pas utilisé dans la suite de ce cours) affirme qu'en fait n'importe quel groupe peut être obtenu par ce procédé.

Théorème 2.23 *[Théorème de Cayley] Tout groupe peut être identifié à un sous-groupe d'un groupe de permutations.*

On se reportera à exercice 12 de la feuille de TD 1 pour un énoncé formellement plus rigoureux et des indications sur la démonstration. On y verra que le théorème de Cayley est en fait plus précis : il dit qu'un groupe $(G, \star)$ peut être identifé à un sous-groupe de $\mathfrak{S}_G$, et il explicite une telle identification.

2.2.7 Comment montrer qu'un couple $(G, \star)$ est un groupe ?

La première méthode est d'appliquer la définition 2.14. Il s'agit donc de montrer que $\star$ est associative, admet un élément neutre, et que tout élément admet un symétrique.

La seconde méthode consiste à idendifier $(G, \star)$ à un sous-groupe d'un groupe « connu ». Plus précisément, il s'agit d'exhiber un groupe « connu » $(\Gamma, \perp)$ tel que G est un sous-groupe de Γ et la loi induite par $\perp$ sur G est la loi $\star$. Par le résultat principal du paragraphe précédent, on conclut que $(G, \star)$ est un groupe.

La première méthode est dans la pratique souvent assez laborieuse, notamment en ce qui concerne la démonstration de l'associativité ; la seconde méthode, quand on peut l'appliquer, est souvent beaucoup plus rapide que la première. Il sera très rare au cours de ce module que ce ne soit pas la méthode à utiliser lorsqu'on vous demandera de montrer qu'un certain ensemble muni d'une certaine loi de composition est un groupe.

10. Le plus difficile dans la démonstration est peut-être de devoir accepter qu'elle n'est constituée que d'une longue suite d'évidences, qu'on est pourtant bien obligé d'écrire explicitement si on veut faire rigoureusement les choses.

Au niveau de ce module, les groupes réputés « connus » seront les suivants : $(\mathbf{Z},+)$, $(\mathbf{Q},+)$, $(\mathbf{R},+)$, $(\mathbf{C},+)$, $(\mathbf{Q}^\times,\times)$, $(\mathbf{R}^\times,\times)$, $(\mathbf{C}^\times,\times)$, $\mathrm{GL}_n(\mathbf{R})$, $\mathrm{GL}_n(\mathbf{C})$, $\mathfrak{S}_E$ où E est un ensemble, et en anticipant un peu : $\mathbf{Z}/N\mathbf{Z}$ pour tout entier $N \geqslant 1$, le groupe additif d'un anneau connu, le groupe des éléments inversibles d'un anneau connu. On se reportera à la section 3.3.6 pour la liste des anneaux réputés connus.

Exercice 9

Soit $\mathbf{D}$ l'ensemble des nombres décimaux, c'est-à-dire les rationnels qui peuvent s'écrire sous la forme $\frac{a}{10^n}$, où $a, n \in \mathbf{Z}$. Montrer que $(\mathbf{D},+)$ est un groupe.

2.3 Morphismes de groupes

Un morphisme de groupes est une application d'un groupe vers un autre qui respecte la structure de groupe. Cette notion est l'analogue de celle d'application linéaire en théorie des espaces vectoriels. Moralement, exhiber un morphisme entre deux groupes nous dit qu'il existe un certain lien entre les structures de groupes mises en jeu. C'est intéressant par exemple quand l'un des groupes est « bien connu » et pas l'autre : cela amène une meilleure compréhension du groupe « moins bien connu ». Le lien est le plus étroit possible lorsque l'application est bijective : on a alors ce qu'on appelle un isomorphisme entre deux groupes. Cela signifie moralement que les deux groupes sont « les mêmes », bien que les descriptions initiales de ces groupes diffèrent.

Donnons un premier exemple. Soit $N \geqslant 1$ un entier et $\mathbf{U}_N$ le groupe des racines N-ème de l'unité. Si $\zeta \in \mathbf{U}_N$ est une racine dite primitive, on verra que l'application

$$\begin{array}{ccc} \{0,1,\ldots,N-1\} & \longrightarrow & \mathbf{U}_N \\ n & \longmapsto & \zeta^n \end{array}$$

induit un ismorphisme entre le groupe $(\{0,1,\ldots,N-1\},\oplus)$ et le groupe des racines N-èmes de l'unité. Ces deux groupes, d'origine a priori assez différente, ont donc en fait la même structure.

2.3.1 Définition, propriétés élémentaires, premiers exemples

Définition 2.24 *Soit $(G,\star)$ et $(H,\otimes)$ des groupes. Soit $\varphi : G \to H$ une application. On dit que φ est un morphisme de groupes si on a pour tout $(g,h) \in G^2$ la relation*

$$\varphi(g \star h) = \varphi(g) \otimes \varphi(h).$$

Remarque 2.25 : Si G et H sont notés multiplicativement, la relation s'écrit

$$\varphi(g\,h) = \varphi(g)\varphi(h).$$

□

Proposition 2.26 *Soit $(G,\star)$ et $(H,\otimes)$ des groupes et $\varphi : G \to H$ un morphisme de groupes. Alors « le neutre est envoyé sur le neutre, l'image du symétrique est le symétrique de l'image ». Plus formellement :*

1. *si e_G est l'élément neutre de G et e_H celui de H, on a $\varphi(e_G) = e_H$*
2. *pour tout $g \in G$, si g' est le symétrique de G, $\varphi(g')$ est le symétrique de $\varphi(g)$.*

Démonstration : On a

$$\varphi(e_G) = \varphi(e_G \star e_G) = \varphi(e_G) \otimes \varphi(e_G)$$

Si h désigne le symétrique de $\varphi(e_G)$, on a donc

$$e_H = h \otimes \varphi(e_G) = h \otimes (\varphi(e_G) \otimes \varphi(e_G))$$

or par associativité

$$h \otimes (\varphi(e_G) \otimes \varphi(e_G)) = (h \otimes \varphi(e_G)) \otimes \varphi(e_G) = e_H \otimes \varphi(e_G) = \varphi(e_G)$$

d'où $e_H = \varphi(e_G)$.

On a

$$e_H = \varphi(e_G) = \varphi(g \star g') = \varphi(g' \star g)$$

soit

$$e_H = \varphi(g) \otimes \varphi(g') = \varphi(g') \otimes \varphi(g).$$

□

Exemple 2.27 : Voici des exemples de morphismes de groupes.

- l'inclusion d'un sous-groupe dans un groupe ;
- l'exponentielle de $\mathbf{R}$ dans $\mathbf{R}$ ou de $\mathbf{C}$ dans $\mathbf{C}^\times$;
- pour $N \geqslant 1$, l'application de $\mathbf{Z}$ dans $\{0, \ldots, N-1\}$ qui à n associe le reste de la division euclidienne de n par N ;
- pour $N \geqslant 1$ et ζ une racine N-ème de l'unité, l'application de $\{0, \ldots, N-1\}$ dans $\mathbf{C}^\times$ qui à n associe ζ^n ;
- l'application $\mathbf{R} \to [0,1[$ qui à un réel associe sa partie fractionnaire (la loi de groupe sur $[0,1[$ associe à (x,y) la partie fractionnaire de $x+y$).

□

Exercice 10

Montrer que les exemples précédents sont bien des morphismes de groupes.

Proposition 2.28 *Si φ est un morphisme de groupes bijectif, alors l'application réciproque de φ est encore un morphisme de groupes.*

La composée de deux morphismes de groupes en est un.

Si $\varphi : (G,\star) \to (H,\otimes)$ est un morphisme de groupes, alors pour tout $g \in G$ et tout $n \in \mathbf{Z}$, on a $\varphi(g^{\star n}) = \varphi(g)^{\otimes n}$.

Démonstration : laissée en exercice. □

2.3.2 Noyau d'un morphisme de groupes

Définition 2.29 *Soit $(G, \star)$ et $(H, \otimes)$ des groupes, $\varphi : G \to H$ un morphisme de groupes et e_H l'élément neutre de H.*

Le noyau de φ, noté $\mathrm{Ker}(\varphi)$ *est le sous-ensemble de G défini par*

$$\mathrm{Ker}(\varphi) = \{g \in G, \quad \varphi(g) = e_H\}.$$

Exercice 11

Pour les exemples de morphismes de groupes donnés ci-dessus, déterminer à chaque fois le noyau.

Proposition 2.30 *Soit $(G, \star)$ et $(H, \otimes)$ des groupes, et $\varphi : G \to H$ un morphisme de groupes. Alors* $\mathrm{Ker}(\varphi)$ *est un sous-groupe de G.*

Démonstration : exercice, figure dans le TD 2. □

Remarque 2.31 : On peut montrer plus généralement sous ces hypothèses que si K est un sous-groupe de H alors $\varphi^{-1}(K)$ est un sous-groupe de G. Le cas du noyau correspond à $K = \{e_H\}$. Une propriété similaire vaut pour les images directes. □

Remarque 2.32 : Dans le cas où G est commutatif, on verra une sorte de réciproque : tout sous-groupe de G est le noyau d'un certain morphisme ; la situation est plus compliquée si G n'est pas commutatif ; on a besoin d'introduire la notion de « sous-groupe distingué » ; cette notion cruciale en théorie des groupes ne sera pas abordée dans ce cours. □

Remarque 2.33 : Cette proposition fournit dans certain cas un moyen pratique de montrer qu'une certaine partie d'un groupe est un sous-groupe : il suffit en effet de montrer que c'est le noyau d'un certain morphisme. □

L'un des intérêts de la notion de noyau apparaît dans la proposition suivante.

Proposition 2.34 *Soit $(G, \star)$ et $(H, \otimes)$ des groupes, et $\varphi : G \to H$ un morphisme de groupes. Soit e_G l'élément neutre de G. Alors φ est injectif si et seulement si* $\mathrm{Ker}(\varphi) = \{e_G\}$.

Démonstration : Remarquons tout d'abord que pour n'importe quel morphisme φ, on a $e_G \in \mathrm{Ker}(\varphi)$. Ainsi la deuxième condition peut se réécrire $\mathrm{Ker}(\varphi) \subset \{e_G\}$.

Supposons φ injectif. Soit $g \in \mathrm{Ker}(\varphi)$. Alors

$$\varphi(e_G) = e_H = \varphi(g).$$

Comme φ est injectif, on a $e_G = g$, ce qu'il fallait démontrer.

Supposons $\mathrm{Ker}(\varphi) = \{e_G\}$. Soit $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$. Pour simplifier l'écriture, adoptons la notation multiplicative. On déduit de l'égalité précédente

$$\varphi(g_2)^{-1}\varphi(g_1) = \varphi(g_2)^{-1}\varphi(g_2) = e_H$$

d'où

$$\varphi(g_2^{-1}.g_1) = e_H,$$

en d'autres termes $g_2^{-1}.g_1 \in \mathrm{Ker}(\varphi)$. Ainsi $g_2^{-1}.g_1 = e_H$ et en multipliant cette égalité à gauche par g_2 on obtient $g_1 = g_2$, ce qu'il fallait démontrer. □
Ainsi plus le noyau est « petit », plus le morphisme est « proche » d'être injectif, et plus G est « proche » d'être un sous-groupe de G'.

2.4 Groupes monogènes, ordre d'un élément, groupes cycliques, théorème de Lagrange

2.4.1 Groupes monogènes

Les groupes monogènes sont les groupes les plus simples à comprendre en termes de partie génératrice (si G est un groupe, une partie génératrice de G est une partie $\mathcal{P}$ de G telle que le sous-groupe de G engendré par $\mathcal{P}$ est G lui-même).

Définition 2.35 *Un groupe est dit* monogène *s'il est engendré par un élément. En d'autres termes, un groupe est monogène s'il contient un élément g tel que le sous-groupe engendré par g est le groupe lui-même.*

Remarque 2.36 : D'après le théorème 2.22, un groupe G noté multiplicativement est monogène si et seulement s'il contient un élément g tel qu'on ait

$$G = \{g^n, \quad n \in \mathbf{Z}\}.$$

Les règles de calcul des puissances (proposition 2.20) montrent alors qu'un groupe monogène est nécessairement commutatif. □
Exemple 2.37 : $(\mathbf{Z}, +)$ et $(\{0, 1, \ldots, N-1\}, \oplus)$ sont des exemples de groupes monogènes ; $(\mathbf{R}, +)$ n'est pas un groupe monogène. □
Exercice 12
Démontrez les assertions précédentes.

Remarque 2.38 : Il est facile de fabriquer des groupes monogènes : si G est un groupe (noté multiplicativement), à partir de n'importe quel élément g de G on peut fabriquer un sous-groupe monogène de G, à savoir le sous-groupe de G engendré par g ! □

2.4.2 Ordre d'un élément d'un groupe

Définition 2.39 *Soit G un groupe noté multiplicativement. Un élément g de G est* d'ordre fini *s'il existe un entier* STRICTEMENT *positif n tel que $g^n = e$.*

Remarque 2.40 : Si G est noté additivement (rappelons que cela n'est possible que si G est commutatif) la condition s'écrit : il existe un entier STRICTEMENT positif tel que $n.g = 0$. □

Exemple 2.41 : Dans n'importe quel groupe, l'élément neutre e est d'ordre fini. On l'appellera l'élément d'ordre fini trivial.

$(\mathbf{Z}, +)$ et $(\mathbf{R}, +)$ n'ont aucun élément d'ordre fini non trivial.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est un élément d'ordre fini du groupe $\mathrm{GL}_2(\mathbf{R})$. □

Exercice 13

Démontrez le !

Définition 2.42 *Soit G un groupe noté multiplicativement. Soit $g \in G$ un élément d'ordre fini. Son* ordre *est le plus petit entier* STRICTEMENT *positif vérifiant $g^n = e$.*

Exercice 14

Montrer que l'élément neutre e est d'ordre 1, et que c'est l'unique élément d'ordre 1.

Montrer que $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 2.

Proposition 2.43 *Soit $N \geqslant 1$. Alors tous les éléments du groupe $(\{0, 1, \ldots, N-1\}, \oplus)$ sont d'ordre fini. L'ordre d'un élément m de $\{0, 1, \ldots, N-1\}$ est $\frac{N}{\mathrm{pgcd}(N,m)}$.*

Démonstration : On utilise la notation additive, et pour éviter les confusions, pour $m \in \{0, 1, \ldots, N-1\}$ on notera $[m]$ l'entier m « vu comme élément du groupe $(\{0, 1, \ldots, N-1\}, \oplus)$ ». Ainsi $n.[m] = [r]$ où r est le reste de la division euclidienne de $n.m$ par N, et l'élément neutre de $(\{0, 1, \ldots, N-1\}, \oplus)$ est $[0]$.

Soit $m \in \{0, 1, \ldots, N-1\}$. Comme N divise $N.m$, on a $N.[m] = [0]$ donc $[m]$ est d'ordre fini (rappelons que $N \geqslant 1$).

Plus généralement, pour $n \in \mathbf{Z}$, on a les équivalences

$$n.[m] = [0] \iff N \text{ divise } n.m \iff \frac{N}{\mathrm{pgcd}(N,m)} \text{ divise } n.$$

Ainsi le plus petit entier strictement positif vérifiant $n.[m] = 0$ est $\frac{N}{\mathrm{pgcd}(N,m)}$. □

Exercice 15

Montrer la validité de la chaîne d'équivalences de la démonstration.

Proposition 2.44 *Soit G un groupe noté multiplicativement. Soit g un élément de G, et n un entier* STRICTEMENT *positif. Sont équivalents :*

1. *on a $g^n = e$;*
2. *g est d'ordre fini et son ordre* DIVISE *n.*

Démonstration : Supposons $g^n = e$. Comme n est supposé strictement positif, g est d'ordre fini. Soit m l'ordre de g. Comme m est par définition un entier strictement positif, on peut considérer $n = m\,q + r$ la division euclidienne de n par m. Rappelons qu'en particulier on a $0 \leqslant r < m$. En utilisant les règles de calcul des puissances, on obtient

$$e = g^n = g^{m\,q+r} = g^{m\,q}\,g^r = (g^m)^q\,g^r.$$

Comme m est l'ordre de g, on a $g^m = e$. Ainsi

$$e = e^q\,g^r = e\,g^r = g^r.$$

Donc $g^r = e$. Or m est par définition le plus petit entier μ strictement positif vérifiant $g^\mu = e$. Comme on a en outre $0 \leqslant r < m$, nécessairement $r = 0$. Ainsi m divise n.

Supposons que g est d'ordre fini m, et que m divise n. Ainsi $n = qm$ avec $q \in \mathbf{Z}$. Toujours d'après les règles de calcul des puissances on a

$$g^n = g^{m\,q} = (g^m)^q = e^q = e.$$

□

Proposition 2.45 *Tout élément d'un groupe fini est d'ordre fini.*

Démonstration : Soit G un groupe fini, noté multiplicativement. On considère, pour $g \in G$, l'application

$$\begin{array}{ccc} \mathbf{N} \setminus \{0\} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}.$$

Comme $\mathbf{N} \setminus \{0\}$ est infini et G est fini, cette application n'est pas injective. On peut donc trouver des entiers $1 \leqslant n_1 < n_2$ vérifiant $g^{n_1} = g^{n_2}$. En multipliant par g^{-n_1}, on obtient $g^{n_2-n_1} = 0$. Or $n_2 - n_1 \geqslant 1$, donc g est d'ordre fini. □

Remarque 2.46 : Le théorème de Lagrange ci-dessous renforcera considérablement ce résultat. □

2.4.3 Groupes cycliques

Définition 2.47 *Un groupe est cyclique s'il est engendré par un élément d'ordre fini.*

Un groupe cyclique est donc en particulier monogène.

Exemple 2.48 : $(\mathbf{Z}, +)$ est monogène non cyclique.

$(\{0, 1, \ldots, N-1\}, \oplus)$ est cyclique. □

Exercice 16

Montrer au moins la deuxième assertion ; la non cyclicité de $\mathbf{Z}$ découlera aussitôt de la proposition ci-dessous.

Un chapitre spécifique du cours sera dédié aux propriétés importantes des groupes cycliques. On se contente ici de la proposition suivante.

Désormais, sauf mention expresse du contraire, les groupes sont notés multiplicativement.

Proposition 2.49 *Soit G un groupe cyclique, engendré par un élément g d'ordre n. Alors G est fini, de cardinal n.*

Plus généralement, soit G un groupe et g un élément d'ordre fini de G. Alors le sous-groupe de G engendré par g est fini, de cardinal l'ordre de g.

Démonstration : Soit H un sous-groupe de G engendré par un élément g d'ordre fini N. Pour montrer la proposition, il suffit de montrer que l'application

$$\begin{array}{ccc} \{0,\dots,N-1\} & \longrightarrow & H \\ n & \longmapsto & g^n \end{array}$$

est bijective.

Montrons l'injectivité. Soit $0 \leqslant n_1 \leqslant n_2 \leqslant N-1$ vérifiant $g^{n_1} = g^{n_2}$. En multipliant par g^{-n_1}, on obtient $g^{n_2-n_1} = e$. Or on a $0 \leqslant n_2 - n_1 \leqslant N-1$. Comme N est l'ordre de g, on en déduit $n_2 - n_1 = 0$ soit $n_2 = n_1$.

Montrons la surjectivité. On sait qu'on a $H = \{g^n \quad n \in \mathbf{Z}\}$. Il suffit donc de montrer

$$\forall n \in \mathbf{Z}, \exists r \in \{0,\dots,N-1\}, \quad g^n = g^k.$$

Pour $n \in \mathbf{Z}$, soit $n = N\,q + r$ la division euclidienne de n par N. Par un calcul similaire à celui de la démonstration de la proposition 2.44, on a $g^n = g^r$ (vérifiez-le !), d'où le résultat voulu. □

En théorie des groupes, le cardinal d'un groupe fini est appelé son *ordre*. Il ne faut pas confondre les notions d'ordre d'un groupe fini et d'ordre d'un élément ! (même si la proposition précédente montre qu'elle ne sont pas sans rapport).

2.4.4 Théorème de Lagrange

Théorème 2.50 (Théorème de Lagrange) *Soit G un groupe fini. L'ordre de tout sous-groupe de G divise l'ordre de G.*

Comme corollaire immédiat du théorème, on obtient ce qui suit.

Corollaire 2.51 *Soit G un groupe fini. L'ordre d'un élément g de G divise l'ordre de G.*

En particulier si d désigne l'ordre de G on a $g^d = e$ pour tout élément de g de G.

Il suffit en effet d'appliquer le théorème de Lagrange au sous-groupe de G engendré par g et d'utiliser les propositions 2.49 et 2.44.

Corollaire 2.52 *La table de la question 3 de l'exercice 6 du TD 1 ne représente pas une loi de groupe.*

En effet si on avait affaire à un groupe, a serait l'élément neutre, donc b serait d'ordre 2, or le groupe serait d'ordre 3. Cette résolution élégante (qui évite d'avoir à chercher un contre-exemple à l'associativité, ce qui est possible mais laborieux) est déjà une jolie illustration de la puissance du théorème. Ce théorème donne des renseignements absolument non triviaux sur les sous-groupes des groupes finis, et donc sur la structure des groupes finis. Pour une illustration frappante, *cf.* l'exercice 7.1 du TD 2.

Démonstration : (du théorème de Lagrange) On donne les idées fondamentales de la démonstration. Le lecteur intéressé devrait pouvoir sans trop de peine rédiger les détails.

Soit H un sous-groupe de G. Pour tout g élément de G, on définit

$$g\,H \stackrel{\text{déf}}{=} \{g.h, \quad h \in H\}.$$

Ainsi $g.H$ est une parties de G, et par ailleurs l'application $h \mapsto g\,h$ induit une bijection de H sur $g\,H$. En particulier on a $\mathrm{card}(g\,H) = \mathrm{card}(H)$.

Soit maintenant g_1, g_2 deux éléments de G. Alors soit $g_1H = g_2H$, soit $g_1H \cap g_2H = \varnothing$. G étant fini, on peut ainsi trouver des éléments $g_1, \ldots, g_r$ tels que les ensembles $\{g_i\,H\}_{1 \leqslant i \leqslant r}$ forment une partition de H. Ainsi on a

$$\mathrm{card}(G) = \sum_{i=1}^{r} \mathrm{card}(g_i\,H) = \sum_{i=1}^{r} \mathrm{card}(H) = r\,\mathrm{card}(H),$$

d'où le résultat. □

3 Le groupe $(\mathbf{Z}, +)$. L'anneau $(\mathbf{Z}, +, \times)$. Structure d'anneau. Introduction à la notion de structure quotient. Les anneaux $\mathbf{Z}/N\mathbf{Z}$.

3.1 Le groupe $(\mathbf{Z}, +)$

3.1.1 Propriétés connues en tant que groupe

C'est un groupe monogène (il est engendré, au choix, par 1 ou -1), en particulier commutatif, et infini.

3.1.2 Les sous-groupes de Z

Notre objectif est de décrire l'ensemble des sous-groupes de $\mathbf{Z}$. Bien évidemment, $\mathbf{Z}$ et $\{0\}$ en font partie. Plus généralement, si $a \in \mathbf{Z}$, le sous-groupe engendré par a en fait partie. Rappelons que ce sous-groupe est $\{a\,n, \quad n \in \mathbf{Z}\}$ (en d'autres termes c'est l'ensemble des multiples de a). On le note $a\mathbf{Z}$. Notons que $\mathbf{Z} = 1.\mathbf{Z}$ et $\{0\} = 0.\mathbf{Z}$.

On peut a priori essayer de construire d'autres sous-groupes de $\mathbf{Z}$ en considérant par exemple des sous-groupes engendrés par deux éléments ou plus. Mais en fait on a le théorème fondamental suivant.

Théorème 3.1 *Tous les sous-groupes de $\mathbf{Z}$ sont monogènes. En d'autres termes, si G est un sous-groupe de $\mathbf{Z}$, alors il existe $a \in \mathbf{Z}$ tel qu'on ait $G = a\,\mathbf{Z}$.*

Remarquons encore une fois que la réciproque est vraie : pour $a \in \mathbf{Z}$, $a\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ (*cf.* ci-dessus).

La démonstration du théorème est donnée ci-dessous. Commençons d'abord par expliciter une application à l'existence du pgcd. On a besoin de la proposition suivante qui montre que la notion de divisibilité dans $\mathbf{Z}$ peut se traduire en termes d'inclusion de sous-groupes (la démonstration est un exercice du TD 1).

Proposition 3.2 *Soit $a, b \in \mathbf{Z}$.*

Alors

$$b \text{ divise } a \iff a \in b\,\mathbf{Z} \iff a\mathbf{Z} \subset b\,\mathbf{Z}.$$

En particulier on a $a\,\mathbf{Z} = b\,\mathbf{Z}$ si et seulement si $|a| = |b|$.

Corollaire 3.3 *Soit $a, b \in \mathbf{Z}$. Il existe un unique $\delta \geqslant 0$ vérifiant :*

1. *δ divise a et δ divise b ;*
2. *pour tout entier relatif d qui divise a et b, d divise δ.*

δ est appelé le pgcd de a et b.

Démonstration : On ne donne que les grandes lignes, on se reportera à l'exercice 8 du TD 1 pour les détails. Les conditions sur δ, compte tenu de la proposition 3.2 se réécrivent : « $\delta\mathbf{Z}$ contient $a\mathbf{Z}$ et $b\mathbf{Z}$ et pour tout entier relatif d tel que $d\,\mathbf{Z}$ contient $a\mathbf{Z}$ et $b\mathbf{Z}$, $d\,\mathbf{Z}$ contient $\delta\mathbf{Z}$ ». Ceci équivaut à « $\delta\mathbf{Z}$ contient $a\mathbf{Z} + b\mathbf{Z}$ et pour tout entier relatif d tel que $d\,\mathbf{Z}$ contient $a\mathbf{Z} + b\mathbf{Z}$, $d\,\mathbf{Z}$ contient $\delta\mathbf{Z}$ ». Compte tenu du théorème, la condition sur δ est vérifiée si et seulement si $\delta\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$, ce qui permet de conclure. □

Cette approche du pgcd, en plus d'être plus agréable que l'approche élémentaire [11], est également a priori intéressante en vue d'une généralisation de la notion de pgcd à d'autres ensembles « arithmétiquement intéressants » que $\mathbf{Z}$. Essentiellement, on a en fait montré que sur tout groupe dont tout sous-groupe est monogène, on peut définir un pgcd. On peut donc imaginer étendre la notion de pgcd à n'importe quel groupe vérifiant cette propriété. Le problème est que le seul groupe (infini) vérifiant la propriété que tous ses sous-groupes sont monogènes est $\mathbf{Z}$ lui-même (en toute rigueur, tout tel groupe est isomorphe au groupe $\mathbf{Z}$). Pour que cette approche par structure algébrique du pgcd se généralise bien, il faut en fait

11. celle qui consiste à définir le pgcd de a et b comme étant le plus grand diviseur positif commun de a et b ; elle ne fonctionne pas si $a = b = 0$ et la propriété fondamentale « tout diviseur commun est un diviseur du pgcd » n'en découle pas immédiatement.

faire intervenir une sructure « plus riche » que la structure de groupe, à savoir la structure *d'anneau*, et remplacer la notion de sous-groupe par la notion *d'idéal*[12]. Si on se limite à l'étude de $\mathbf{Z}$, la nécessité de la structure d'anneau n'apparaît pas clairement, car en un sens la structure d'anneau de $\mathbf{Z}$ est entièrement déterminée par sa structure de groupe [13] et les notions d'idéal et de sous-groupe coïncident. C'est une situation tout à fait exceptionnelle. $\mathbf{Z}$ est (à isomorphisme près) le seul anneau (infini) vérifiant cette propriété.

Démonstration : (du théorème) L'outil crucial de la démonstration est la division euclidienne. Pour en comprendre le principe, il est utile de constater ce qui suit : si $G = a\mathbf{Z}$ avec $a \neq 0$, alors quitte à changer a en $-a$ on peut supposer a strictement positif. Alors a peut-être caractérisé comme étant le plus petit élément de $G \cap (\mathbf{N} \setminus \{0\})$. En d'autres termes : si a est un entier strictement positif, le plus petit multiple strictement positif de a est a lui-même.

Soit à présent G un sous-groupe de $\mathbf{Z}$. Si $G = \{0\}$, on a $G = 0.\mathbf{Z}$ et on a terminé. Supposons donc $G \neq \{0\}$. Au vu de ce que nous avons constaté précédemment, il est naturel de poser

$$a = \mathrm{Min}[G \cap (\mathbf{N} \setminus \{0\})]$$

et d'essayer de montrer qu'on a $G = a\mathbf{Z}$. Il faut d'abord montrer que a est bien défini ! Comme on sait que toute partie *non vide* de $\mathbf{N}$ admet un plus petit élément, il suffit pour cela de montrer que $G \cap (\mathbf{N} \setminus \{0\})$ est non vide, en d'autres termes que G contient un élément strictement positif. Mais par hypothèse G contient un élément b non nul. Si $b > 0$, on a terminé, sinon, comme G est un sous-groupe, on a $-b \in G$, et $-b > 0$.

Ainsi a est bien défini. C'est un entier strictement positif élément de G. Comme G est un sous-groupe de $\mathbf{Z}$ contenant a et que $a\mathbf{Z}$ est le sous-groupe engendré par a, on a $a\mathbf{Z} \subset G$. Montrons à présent l'inclusion inverse $G \subset a\mathbf{Z}$, ce qui terminera la démonstration du théorème.

Soit donc $b \in G$. Il faut montrer que b est un multiple de a. Il est naturel de considérer la division euclidienne $b = a\,q + r$ de b par a (rappelons que a est non nul). En particulier on a $0 \leqslant r < a$. Comme G est un sous-groupe de $\mathbf{Z}$ contenant b et $a\mathbf{Z}$, G contient $b - q.a$, c'est-à-dire G contient r. Or on a

$$r < \mathrm{Min}\, G \cap (\mathbf{N} \setminus \{0\})$$

donc $r \notin G \cap (\mathbf{N} \setminus \{0\})$. Comme $r \in G$, nécessairement on a $r \leqslant 0$. Comme on a également $r \geqslant 0$, r est nul et on a terminé. □

3.2 L'anneau $(\mathbf{Z}, +, \times)$

Sur $\mathbf{Z}$, en plus de la loi de composition interne donnée par l'addition, qui est commutative, associative, possède un élément neutre, et pour laquelle tout élément possède un symétrique,

12. Attention, la notion de *sous-anneau* aura aussi un sens, et sera différente de la notion d'idéal

13. Plus prosaïquement : la multiplication dans $\mathbf{Z}$ peut se retrouver à partir de l'addition ; en effet, calculer le produit $n \times m$ (si n est positif, disons), c'est additioner m « n fois de suite ».

existe une autre loi de composition interne que, tout comme l'addition, vous connaissez bien : c'est la multiplication $(m, n) \mapsto m \times n$, souvent notée $m.n$ voire $m\,n$. La loi $\times$ est commutative, associative, distributive par rapport à $+$, et possède un élément neutre. Ces propriétés de $+$ et de $\times$ vont plus généralement caractériser les anneaux (commutatifs).

Remarque 3.4 : Bien évidemment, muni de la seule loi $\times$, $\mathbf{Z}$ n'est pas un groupe : il n'est pas vrai que tout élément de $\mathbf{Z}$ admet un symétrique pour la loi $\times$. Insistons sur le fait que la définition demande l'existence d'un symétrique dans $\mathbf{Z}$, et pas éventuellement dans un ensemble plus gros. Les seuls éléments de $\mathbf{Z}$ qui admettent un symétrique pour $\times$ sont 1 et -1. Notez bien que $(\mathbf{Z} \setminus \{0\}, \times)$ n'est pas non plus un groupe. □

3.3 Définition générale d'un anneau, premières propriétés

3.3.1 Définitions, exemples

Un anneau est un ensemble muni d'un *couple* de lois de composition interne qui ont les mêmes propriétés que celles qu'on a soulignées pour le couple $(+, \times)$ dans la section précédente.

Définition 3.5 *Un anneau est un triplet $(A, \star, \perp)$ où A est un ensemble et $\star$ et $\perp$ sont deux lois de composition interne sur A, qui vérifient les propriétés suivantes :*

1. *$(A, \star)$ est un groupe commutatif ;*
2. *la loi $\perp$ possède un élément neutre, est associative et commutative ;*
3. *la loi $\perp$ est distributive par rapport à la loi $\star$; ceci signifie que pour tout triplet (a, b, c) d'éléments de A, on a*
$$a \perp (b \star c) = (a \perp b) \star (a \perp c)$$

Exemple 3.6 : $(\mathbf{Z}, +, \times)$, $(\mathbf{R}, +, \times)$, $(\mathbf{C}, +, \times)$, $(\mathbf{K}[X], +, \times)$ où $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$ sont des exemples d'anneaux.

Pour $N \geqslant 1$, on définit une loi de composition interne sur $\{0, \ldots, N-1\}$ en prenant pour $m \otimes n$ le reste de la division euclidienne de $m\,n$ par N. Alors $(\{0, \ldots, N-1\}, \oplus, \otimes)$ est un anneau. □

Exercice 17

Montrer que les exemples précédents sont bien des exemples d'anneaux.

Remarque 3.7 : Ce qu'on a définit ici sera pour d'autres auteurs un « anneau commutatif avec unité ». On peut notamment [14] relâcher la définition en ne demandant pas que la seconde loi, notée $\perp$ dans la définition, soit commutative (anneaux non commutatifs) [15] et/ou en ne demandant pas qu'elle admette un élément neutre (anneaux sans unité). Attention, la

14. C'est utile dans certains contextes qui dépassent le cadre de ce cours.
15. Il faut alors demander la distributivité « à droite et à gauche »

première loi, notée $\star$ dans la définition, est toujours commutative, même pour un anneau non commutatif. La théorie des anneaux non commutatifs est assez différente de celles des anneaux commutatifs. On se contentera ici de donner un exemple d'anneau non commutatif (mais avec unité) : le triplet $(M_n(\mathbf{K}), +, \times)$ où $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$, $M_n(\mathbf{K})$ est l'ensemble des matrices carrées de taille n (avec $n \geqslant 2$) à coefficients dans $\mathbf{K}$, $+$ est l'addition matricielle et $\times$ la multiplication matricielle. □

Remarque 3.8 : En ce qui concerne les usages en termes de notations (usages auxquels je me conformerai en général), la première loi d'un anneau est quasi-systématiquement notée additivement, et la seconde loi est très souvent notée multiplicativement. L'élément neutre de la première loi est ainsi noté 0 et l'élément neutre de la seconde loi 1. L'élément neutre de la seconde loi est souvent appelé *l'unité* de l'anneau. Pour des raisons pédagogiques, il m'arrivera d'écrire 0_A et 1_A, où A est l'anneau considéré. □

Remarque 3.9 : Soit $(A, +, \times)$ un anneau. Pour tout élément a de A et pour n entier *naturel* il est alors possible, et la démarche est strictement similaire à celle de la définition 2.19, de définir la puissance itérée n-ème de A, noté a^n. On a alors les mêmes règles de calcul de puissances que pour les lois de groupes, en se limitant toutefois aux exposants positifs.

Rappelons qu'il y a bien sûr aussi une notion de « puissance itérée » pour la première loi mais que vu la notation adoptée on parlera ici plutôt de somme itérée ; on se reportera à la section suivante pour une petite subtilité à ce sujet. □

Remarque 3.10 : Les abus d'écriture traditionnels sont essentiellement de la même nature que ceux pratiqués pour les groupes. Ainsi on dira souvent « soit A un anneau… » plutôt que « soit $(A, \star, \perp)$ un anneau… » (et si on pratique cet abus, il est alors implicite que les notations pour les lois de A sont la notation additive pour la première loi et la notation multiplicative pour la seconde). □

Remarque 3.11 : Les règles de priorité d'écriture sont aussi les mêmes que celles appliquées traditionnellement sur $\mathbf{Z}$, à savoir : la deuxième loi est prioritaire sur la première. Ainsi, si $(A, +, \times)$ est un anneau, l'écriture $a \times b + c$ signifie $(a \times b) + c$ (ou $(a\,b) + c$ en pure notation multiplicative) et désigne donc un élément a priori différent de $a \times (b + c)$. □

3.3.2 Une particularité de l'anneau $(\mathbf{Z}, +, \times)$ et une subtilité concernant les sommes itérées dans un anneau

Nous disons ici quelque mots d'un point un peu subtil dont la compréhension, il faut bien le dire, n'est pas vraiment facilitée par les usages traditionnels de notation. Soit $n \in \mathbf{Z}$. Alors pour tout élément x de $\mathbf{Z}$, $n\,x$ ou $n.x$ désignent a priori deux éléments différents : soit la « somme itérée n-ème » de x, soit le produit de n par x. Bien évidemment, et c'est heureux, ces deux éléments coïncident.

Conservons à présent notre $n \in \mathbf{Z}$ et considérons un élément x d'un anneau $(A, +, \times)$ quelconque. Alors l'expression $n\,x$ (ou $n.x$) a toujours un sens, à savoir la « somme itérée n-ème » de x. Mais il n'est plus question en général de l'interpéter comme une multiplication.

Ce n'est même pas que l'égalité

$$n\,x = n \times x$$

soit fausse, c'est que son second membre n'a pas de sens en général, car $\times$ est par définition une application $A \times A \to A$, et (n, x) ne fait a priori pas partie du domaine de définition de cette application. En particulier, l'égalité

$$n\,1_A = n$$

n'a pas non plus de sens en général. Une exception importante se produit lorsque A contient $\mathbf{Z}$ comme sous-anneau (*cf.* plus loin pour la définition précise d'un sous-anneau), par exemple $A = \mathbf{Q}$ ou $A = \mathbf{R}[X]$. Dans ce cas les égalités ci-dessus ont un sens et... elles sont vraies (heureusement, d'ailleurs...). Notamment 1_A n'est autre que le 1 « traditionnel ».

Mais il existe des anneaux très intéressants qui ne contiennent pas $\mathbf{Z}$ comme sous-anneau et pour lesquels il faut faire attention. C'est le cas des anneaux $\mathbf{Z}/N\mathbf{Z}$ que nous rencontrerons bientôt (que nous avons en fait déjà rencontrés, sous une forme un peu cachée).

3.3.3 Premières propriétés : quelques règles de calcul dans les anneaux commutatifs

Proposition 3.12 *Soit $(A, +, \times)$ un anneau. On a alors les propriétés suivantes :*

$$\forall x \in A, \quad x \times 0_A = 0_A \times x = 0_A$$

$$\forall (x, y) \in A^2, \quad x \times (-y) = (-x) \times y = -(x \times y)$$

$$\forall (x, y) \in A^2, \quad (-x) \times (-y) = x \times y$$

$$\forall (x, y) \in A^2, \forall m \in \mathbf{Z}, \quad x \times (m.y) = (m.x) \times y = m.(x \times y)$$

Démonstration : Pour $x \in A$, on a, en utilisant la distributivité

$$x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A.$$

En ajoutant $-(x \times 0_A)$ à chaque membre, on obtient $x \times 0_A = 0_A$.

Les autres propriétés sont laissées à titre d'exercice. La dernière propriété N'EST PAS une conséquence directe de l'associativité de la loi $\times$ (*cf.* la section précédente). □

Proposition 3.13 (Formule du binôme de Newton) *Soit A un anneau, x et y des éléments de A. On a alors, pour tout $n \in \mathbf{N}$,*

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k\, y^{n-k}.$$

Démonstration : C'est exactement la même que pour $A = \mathbf{C}$. Elle se fait par récurrence sur n, refaites-là à titre d'exercice, ça ne peut pas faire de mal. □

3.3.4 Morphisme d'anneaux

Définition 3.14 *Soit A et B des anneaux. Un morphisme d'anneaux est une application $\varphi : A \to B$ vérifiant les propriétés suivantes :*

1. *φ est un morphisme de groupes de $(A, +)$ vers $(B, +)$; pour mémoire cela signifie qu'on a*
$$\forall (x, y) \in A^2, \quad \varphi(x + y) = \varphi(x) + \varphi(y).$$
2. *On a*
$$\forall (x, y) \in A^2, \quad \varphi(x\, y) = \varphi(x)\varphi(y)$$
3. *On a $\varphi(1_A) = 1_B$.*

Remarque 3.15 : La dernière condition est essentiellement là pour éviter les morphismes inintéressants du genre [16] $\varphi(x) = 0_B$ pour tout $x \in A$. □

Exemple 3.16 : L'application $\mathbf{Z} \to \mathbf{R}$ déduite de l'inclusion naturelle $\mathbf{Z} \subset \mathbf{R}$ est un morphisme d'anneaux. Pour $N \geqslant 1$ l'application $\mathbf{Z} \to \{0, \ldots, N-1\}$ qui à $n \in \mathbf{Z}$ associe le reste de la division euclidienne de n par N est un morphisme de l'anneau $\mathbf{Z}$ vers l'anneau $(\{0, \ldots, N-1\}, \oplus, \otimes)$. □

Exercice 18

Vous aurez deviné... Convenons de toute façon désormais que, sauf mention expresse du contraire, toute assertion non entièrement démontrée de ce texte (typiquement, les exemples illustrant les définitions) fournit implicitement le sujet d'un exercice.

Proposition 3.17 *Si φ est un morphisme d'anneaux bijectif, alors l'application réciproque de φ est encore un morphisme d'anneaux.*

La composée de deux morphismes d'anneaux en est un.

Si $\varphi : A \to B$ est un morphisme d'anneaux, alors pour tout $a \in A$ et tout $n \in \mathbf{Z}$, on a $\varphi(n\, a) = n\, \varphi(a)$ et pour tout $n \in \mathbf{N}$, on a $\varphi\,(a^n) = \varphi(a)^n$.

Démonstration : laissée en exercice (*cf.* la proposition 2.28). □

Définition 3.18 *Le noyau d'un morphisme d'anneaux est son noyau en tant que morphisme de groupes. C'est donc pour mémoire l'ensemble des éléments de l'anneau de départ qui s'envoient sur le 0 de l'anneau d'arrivée.*

Proposition 3.19 *Un morphisme d'anneaux est injectif si et seulement si son noyau est $\{0\}$.*

C'est une conséquence directe de la proposition 2.34.

16. On peut quand même noter que l'application constante égale à 0_B sera un morphisme d'anneaux dans un cas très particulier (et uniquement dans ce cas) : celui où l'anneau d'arrivée est l'anneau nul, *cf.* plus loin.

3.3.5 Anneau produit

Proposition 3.20 *Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ des anneaux. On définit sur $A \times B$ les lois de composition interne $\widetilde{+}$ et $\widetilde{\times}$ par $(a,b)\widetilde{+}(a',b') = (a + a', b \oplus b')$ et $(a,b)\widetilde{\times}(a',b') = (a \times a', b \otimes b')$. Alors $(A \times B, \widetilde{+}, \widetilde{\times})$ est un anneau, appelé* anneau produit *de A par B, et les deux applications de projections $A \times B \to A$ et $A \times B \to B$ (définies pour mémoire par $(a,b) \mapsto a$ et $(a,b) \mapsto b$) sont des morphismes d'anneaux.*

Démonstration : Exercice. Il n'y a aucune astuce, c'est un peu laborieux, mais essentiellement il « suffit d'écrire ». □

Remarque 3.21 : Il existe aussi une notion similaire de groupe produit, dont on ne parle pas ici essentiellement pour garder au contenu de ce cours une longueur raisonnable (*cf.* l'exercice 16 de la feuille de TD 1). □

3.3.6 Sous-anneaux

Définition 3.22 *Soit A un anneau. Un* sous-anneau *de A est une partie B de A vérifiant les propriétés suivantes :*

- *B est un sous-groupe de $(A, +)$*
- *pour tout $(x, y) \in B^2$, $x \times y$ est dans B*
- *1_A est dans B.*

Exemple 3.23 : Toute inclusion déduite de la chaîne d'inclusions ci-dessous

$$\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

fait du « petit ensemble » un sous-anneau du « grand ensemble ».

R est un sous-anneau de $\mathbf{R}[X]$.

Pour tout anneau A, l'ensemble $\{n.1_A\}_{n \in \mathbf{Z}}$ est un sous-anneau de A. □

De façon similaire à ce qui se passe pour les groupes, les lois de composition interne sur un anneau induisent des lois de composition interne sur chacun de ses sous-anneaux. Ces lois induites munissent tout sous-anneau d'une structure d'anneau. La situation est alors similaire à celle décrite dans la section 2.2.7 : pour montrer qu'un triplet $(A, +\times)$ est un anneau, il est souvent plus commode, quand c'est possible, de montrer que A s'identifie à un sous-anneau d'un anneau « connu » plutôt que d'appliquer directement la définition 3.5.

Au niveau de ce module, les anneaux réputés « connus » seront les suivants : l'anneau nul, $(\mathbf{Z}, +, \times)$, $(\mathbf{Q}, +, \times)$, $(\mathbf{R}, +, \times)$, $(\mathbf{C}, +, \times)$, $(\mathbf{K}[X], +, \times)$ où **K** est un anneau connu qui est un corps et (en anticipant un peu) les anneaux $\mathbf{Z}/N\mathbf{Z}$ pour $N \geqslant 1$.

3.3.7 Idéal d'un anneau

De façon peut-être un peu surprenante au premier abord, le bon analogue de la notion de sous-groupe pour un anneau n'est en fait pas la notion de sous-anneau (même si elle a son utilité), mais la notion d'idéal.

Définition 3.24 *Soit A un anneau. Un* idéal *de A est une partie B de A vérifiant les propriétés suivantes :*

- *B est un sous-groupe de $(A, +)$*
- *pour tout $(x, y) \in A \times B$, $x \times y$ est dans B*

Remarque 3.25 : Attention aux confusions possibles ! La définition est techniquement assez proche de celle d'un sous-anneau. □

Exemple 3.26 : $\{0\}$, A, et pour $a \in A$, $a.A = \{a\,b, \quad b \in A\}$ sont des idéaux de A.

Soit $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$. Pour $x \in \mathbf{K}$, $\{P \in \mathbf{K}[X], \quad P(x) = 0\}$ est un idéal de $\mathbf{K}[X]$.

Les idéaux de $\mathbf{Z}$ sont exactement les $a\mathbf{Z}$ pour $a \in \mathbf{Z}$ (noter qu'un idéal est en particulier un sous-groupe, et qu'on connaît tous les sous-groupes de $\mathbf{Z}$; il reste à constater que ce sont en fait des idéaux).

$\mathbf{Z}$ est un sous-anneau de $\mathbf{Q}$ mais n'est pas un idéal de $\mathbf{Q}$; d'ailleurs les seuls idéaux de $\mathbf{Q}$ sont $\{0\}$ et $\mathbf{Q}$. □

La proposition suivante, dont la démonstration est un petit exercice, est un début d'explication au fait que le bon analogue de la notion de sous-groupe est la notion d'idéal (comparer avec la proposition 2.30).

Proposition 3.27 *Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.*

3.3.8 Diviseurs de zéro

Définition 3.28 *Soit A un anneau. Un* diviseur de zéro *dans A est un élément a de A tel qu'il existe un élément b* non nul *de A vérifiant $a \times b = 0_A$.*

Remarque 3.29 : Attention, cette terminologie, bien qu'usuelle, est un peu dangereuse. Par exemple, dans $\mathbf{Z}$, n'importe quel entier divise 0, mais seul 0 est un diviseur de zéro au sens ci-dessus. □

Exemple 3.30 : Si A est un anneau non réduit à un élément, 0_A est un diviseur de zéro. On l'appelle le diviseur de zéro *trivial*.

La quasi-totalité des anneaux que vous « connaissez déjà » n'ont pas de diviseurs de zéro *non-triviaux*. C'est le cas par exemple de $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{R}[X]$, $\mathbf{C}[X]\ldots$

Soit p et q deux nombres premiers et $N = p.q$. Alors p et q sont des diviseurs de zéro non triviaux de l'anneau $(\{0, \ldots, N-1\}, \oplus, \otimes)$. □

Remarque 3.31 : Attention encore, on peut parfois trouver dans d'autres références une définition de diviseur de zéro similaire à celle donnée ici sauf qu'on impose en outre que a soit non nul. Dans ce cas la notion de diviseur de zéro trivial n'a plus lieu d'être et certains des énoncés s'adaptent en conséquence. Il faut bien penser à vérifier la définition employée dans la référence consultée. □

Remarque 3.32 : Un anneau est dit nul s'il vérifie l'égalité $0_A = 1_A$. Un anneau A est nul si et seulement si on a $A = \{0_A\}$ si et seulement si A est réduit à un élément ; ainsi tous les anneaux nuls sont « les mêmes », on parlera de l'anneau nul avec un article défini. L'anneau nul n'a pas de diviseur de zéro. C'est d'ailleurs le seul anneau vérifiant cette propriété. □

Définition 3.33 *Un anneau est dit* intègre *s'il est* non nul *et ne possède pas de diviseurs de zéro* non-triviaux.

Remarque 3.34 : Ainsi A est intègre si et seulement si on a $A \neq \{0_A\}$ et la propriété

$$\forall (x, y) \in A^2, \quad x \times y = 0 \Rightarrow (x = 0_A \text{ ou } y = 0_A).$$

C'est sous cette forme en général qu'on exploite l'intégrité d'un anneau. □

Exemple 3.35 : Les exemples d'anneaux sans diviseurs de zéro non triviaux donnés ci-dessus fournissent donc des exemples d'anneaux intègres. Pouvez vous citer des exemples d'utilisation de l'intégrité de $\mathbf{Z}$, $\mathbf{R}$, ou $\mathbf{C}$, vus dans votre scolarité antérieure ? □

3.3.9 Groupes des éléments inversibles d'un anneau

Soit $(A, +, \times)$ un anneau. Alors $(A, \times)$ n'est presque jamais un groupe, car 0_A n'aura en général pas de symétrique x pour $\times$. En fait si un tel symétrique existe, on aura $1_A = 0_A \times x$ mais par ailleurs $0_A \times x = 0_A$ et donc on voit facilement que $(A, \times)$ est un groupe si et seulement si A est l'anneau nul.

En général, 0_A n'est pas le seul élément à ne pas admettre de symétrique et pour cette raison, si A est intègre [17], $(A \setminus \{0\}, \times)$ ne sera en général pas un groupe (exemple : $A = \mathbf{Z}$). Il existe cependant toujours une structure de groupe que l'on peut définir à partir de la seconde loi sur un anneau, à condition de se restreindre aux éléments dit inversibles.

Définition 3.36 *Soit A un anneau. Un élément $a \in A$ est dit* inversible *s'il admet un symétrique pour la seconde loi, c'est-à-dire qu'il existe $b \in A$ vérifiant $a \times b = 1_A$.*

L'ensemble des éléments inversibles de l'anneau A est noté $A^\times$.

Remarque 3.37 : La notation $A^\times$ NE DÉSIGNE PAS, en général, $A \setminus \{0_A\}$. Ainsi $\mathbf{Z}^\times = \{1, -1\}$. □

Remarque 3.38 : $A^\times$ n'est jamais vide, il contient toujours au moins 1_A.

Un élément inversible n'est jamais diviseur de zéro. □

Proposition 3.39 *Soit A un anneau. Alors $A^\times$ est stable par $\times$, en d'autres termes si $a, b \in A^\times$ alors $a\,b \in A^\times$. Ainsi $\times$ induit une loi de composition interne sur $A^\times$. Muni de cette loi, $A^\times$ est un groupe.*

De manière un peu plus informelle, cette proposition dit : « l'ensemble des éléments inversibles d'un anneau est un groupe pour la multiplication ».

Démonstration : On peut en donner une démonstration directe, à partir de la définition 2.14, laborieuse mais sans difficulté essentielle (je la ferai sans doute en amphi).

Une démonstration un peu plus jolie consiste à identifier $A^\times$ à un sous-ensemble de $\mathfrak{S}_A$ via l'application $a \mapsto (x \mapsto a.x)$ On vérifie alors que la composition sur $\mathfrak{S}_A$ induit la

17. Question un peu subtile : si A n'est pas intègre, pourquoi $(A \setminus \{0\}, \times)$ n'est-il pas un groupe ?

multiplication sur $A^\times$, puis que $A^\times$ est un sous-groupe de $\mathfrak{S}_A$. Le lecteur intéressé rédigera les détails. □

Exemple 3.40 : $\mathbf{Z}^\times = \{1, -1\}$, $\mathbf{R}^\times = \mathbf{R} \setminus \{0\}$, $\mathbf{R}[X]^\times = \mathbf{R}^\times$ (ensemble des polynômes constants non nuls). □

La démonstration de la proposition suivante est l'exercice 13 de la feuille de TD 3.

Proposition 3.41 *Soit A et B des anneaux. Alors $(A \times B)^\times = A^\times \times B^\times$.*

Définition 3.42 *Un corps est un anneau A tel que $A^\times = A \setminus \{0_A\}$, en d'autres termes c'est un anneau non nul tel que tout élément non nul est inversible.*

Remarque 3.43 : Un corps est en particulier un anneau intègre. □

Exemple 3.44 : $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ sont des corps. Voici un exemple moins évident : on considère l'ensemble

$$A = \{a + b\sqrt{2}, \quad (a, b) \in \mathbf{Q}^2\} \subset \mathbf{R}.$$

Alors A est un sous-anneau de $\mathbf{R}$. Il est donc naturellement muni d'une structure d'anneau. Et c'est un corps pour cette structure.

Si N est un nombre premier $(\{0, 1, \ldots, N-1\}, \oplus, \otimes)$ est un corps ; c'est un exemple de corps fini.

Il existe des anneaux intègres qui ne sont pas des corps, par exemple $\mathbf{Z}$, $\mathbf{K}[X]$ où $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$. □

Exercice 19

Un anneau non nul A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

3.4 Quotient d'un groupe commutatif par un sous-groupe, d'un anneau par un idéal

3.4.1 Quotient d'un groupe commutatif par un sous-groupe

Théorème 3.45 *Soit G un groupe commutatif, H un sous-groupe de G. Il existe un groupe commutatif K et un morphisme de groupes surjectif $\pi : G \to K$ de noyau H.*

Le couple (K, π) est « unique à isomorphisme unique près ».

K est appelé *groupe quotient* (de G par H) et noté G/H. Le morphisme π est appelé *morphisme quotient*. L'« unicité à isomorphisme unique près » nous servira uniquement moralement (c'est pour cela notamment que je ne précise pas ce qu'elle signifie formellement). Ce qu'il faut retenir, c'est qu'elle nous assure qu'on peut parler « du » groupe quotient de G par H et « du » morphisme quotient. Ce théorème est admis, non pas parce que les techniques mises en oeuvre pour sa démonstration sont hors de notre portée, mais parce que, selon du moins l'opinion de l'auteur de ce texte, la connaissance de la démonstration n'apporte strictement aucun éclairage utile sur la façon dont il faut « penser » la notion de

quotient. Rappelez vous, par exemple, que vous avez manipulé des nombres réels bien avant de savoir comment on construisait rigoureusement $\mathbf{R}$. Ce qui importait n'était pas de savoir comment on construisait les réels mais les propriétés qu'ils vérifiaient. C'est exactement la même chose pour les quotients de groupes (et d'anneaux, voire plus loin).

Exemple 3.46 : Voici quelques exemples.

- $H = G$, $G/H \xrightarrow{\sim} \{e\}$, $\pi : G \to \{e\}$
- $H = \{e\}$, $G/H \xrightarrow{\sim} G$, $\pi : G \to G$ avec $\pi = \mathrm{Id}_G$
- $G = G_1 \times G_2$, $H = G_1 \times \{e\}$, $G/H \xrightarrow{\sim} G_2$, $\pi : G_1 \times G_2 \to G_2$ est la projection sur G_2
- $G = \mathbf{R}$, $H = \mathbf{Z}$, $G/H \xrightarrow{\sim} \mathbf{U}$ (le groupe des nombres complexes de module 1), $\pi : \mathbf{R} \to \mathbf{U}$ est l'application $t \mapsto \exp(2\,i\,\pi\,t)$
- $G = E$ où E est un espace vectoriel, $H = F$ un sous-espace vectoriel de E. Pour tout supplémentaire F' de F dans E, on a $E/F \xrightarrow{\sim} F'$ et $\pi : E \to F'$ est la deuxième projection $E = F \oplus F' \to F'$

□

3.4.2 Quotient d'un anneau par un idéal

Théorème 3.47 *Soit A un anneau et $\mathcal{I}$ un idéal de A. Il existe un anneau B et un morphisme d'anneaux surjectif $\pi : A \to B$ de noyau $\mathcal{I}$.*

Le couple (B, π) est unique à isomorphisme unique près.

B est appelé anneau quotient (de A par $\mathcal{I}$) et π morphisme quotient. Les commentaires qui suivaient le théorème sur l'existence des quotients de groupes s'appliquent *mutatis mutandi*.

Exercice 20

Soit A un anneau. En vous inspirant des exemples donnés ci-dessus pour les quotients de groupes, décrire l'anneau quotient et le morphisme quotient lorsque $\mathcal{I} = \{0\}$ puis $\mathcal{I} = A$. Même question si A est un produit $A_1 \times A_2$ et $\mathcal{I} = A_1 \times \{0\}$.

Remarque 3.48 : Une bonne façon de se faire une intuition de l'anneau quotient $A/\mathcal{I}$ est de le voir comme « l'anneau A dans lequel on a tué tous les éléments de $\mathcal{I}$ » (on les a « forcés » à être nuls). Une remarque similaire vaut pour un groupe quotient. □

3.5 L'anneau $\mathbf{Z}/N\mathbf{Z}$

3.5.1 Préliminaires

Pour $N \in \mathbf{Z}$, on va considérer l'anneau quotient de $\mathbf{Z}$ par l'idéal $N\,\mathbf{Z}$. Noter qu'on peut toujours supposer $N \geqslant 0$ (*cf.* la proposition 3.2). Si $N = 0$, $\mathbf{Z}/N\mathbf{Z}$ n'est autre que $\mathbf{Z}$ (et le morphisme quotient est l'identité). Ce cas sera écarté par la suite. Un autre cas un peu extrême est le cas où $N = 1$. Dans ce cas $N\,\mathbf{Z} = \mathbf{Z}$ et le quotient est l'anneau nul. Même si ce cas présente un intérêt limité, il n'y aura en général pas lieu de l'écarter par la suite.

On va donner une démonstration de l'existence de l'anneau quotient de $\mathbf{Z}$ par $N\,\mathbf{Z}$ pour tout $N \geqslant 1$. En d'autres termes, on va démontrer une partie du théorème 3.47 dans le cas particulier $A = \mathbf{Z}$ et $\mathcal{I} = N\mathbf{Z}$.

En fait, notre construction consiste simplement à reprendre le morphisme d'anneaux π_N : $(\mathbf{Z}, +, \times) \to (\{0, \ldots, N-1\}, \oplus, \otimes)$ déjà considéré précédemment, qui envoie $n \in \mathbf{Z}$ sur le reste de la division euclidienne de n par N. Rappelons pour mémoire que pour $(m, n) \in \{0, \ldots, N-1\}^2$, $m \oplus n$ (respectivement $m \otimes n$) désigne le reste de la division euclidienne de $m + n$ (respectivement mn) par N. Ceci étant dit, on vérifie facilement que π_N est un morphisme surjectif de noyau $N\,\mathbf{Z}$ (faites le !).

Ailleurs on pourra trouver d'autres constructions de l'anneau $\mathbf{Z}/N\mathbf{Z}$, une des plus répandues consistant à utiliser les classes d'équivalence de la relation « être congru modulo N ».

Insistons de nouveau sur le fait que la façon de construire $\mathbf{Z}/N\mathbf{Z}$ (plus généralement l'anneau quotient) nous importera peu dans la pratique et ne nous sera d'aucune utilité pour manipuler $\mathbf{Z}/N\mathbf{Z}$. Au contraire, cela n'apporte pas nécessairement une très bonne intuition de voir les éléments de $\mathbf{Z}/N\mathbf{Z}$ comme des classes d'équivalence ou comme des éléments de $\{0, \ldots, N-1\}$.

L'unique propriété fondamentale à retenir pour travailler avec l'anneau $\mathbf{Z}/N\mathbf{Z}$ est celle donnée par le théorème 3.47 ci-dessus : il existe un morphisme d'anneaux surjectif $\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}$, de noyau $N\,\mathbf{Z}$. Ce morphisme sera noté, dans le cadre de ce cours, $n \mapsto [n]_N$. Ce n'est aucunement une notation standard mais pour des raisons pédagogiques je m'y tiendrai strictement [18]. La raison est que la seule notation suffisamment répandue que je connaisse consiste tout simplement à n'adopter aucune notation, en d'autres termes à noter les éléments de $\mathbf{Z}/N\mathbf{Z}$ « comme si c'étaient des éléments de $\mathbf{Z}$ ». Cette convention est bien pratique et évite beaucoup de lourdeurs d'écriture *à condition qu'on ait bien compris ce qu'était* $\mathbf{Z}/N\mathbf{Z}$. À notre niveau, cette convention me semble antipédagogique au possible et elle sera bannie de ce cours. Si cela vous semble inutilement lourd et ennuyeux d'utiliser la notation $[\,.\,]_N$, soit vous avez une excellente compréhension en profondeur des concepts introduits dans ce cours (et ce cours n'a pas grand chose à vous apprendre), soit vous n'avez en fait pas bien compris ce qu'était $\mathbf{Z}/N\mathbf{Z}$. Le deuxième cas se produit plus souvent que le premier.

3.5.2 Quelques conséquences du fait que $[\,.\,]_N$ est un morphisme d'anneaux

Toujours pour des raisons pédagogiques, les lois sur l'anneau $\mathbf{Z}/N\mathbf{Z}$ sont notées dans ce paragraphe $\oplus$ et $\otimes$. Traditionnellement, elles sont en général simplement notées additivement et multiplicativement. Assez rapidement, pour des raisons de commodités d'écriture, nous nous plierons à la tradition, même si l'auteur de cet texte n'est pas persuadé que ce soit nécessairement pédagogiquement très rentable. La définition d'un morphisme

18. sauf rares exceptions...

d'anneaux entraîne aussitôt les propriétés suivantes.

$$\forall (a,b) \in \mathbf{Z}^2, \quad [a+b]_N = [a]_N \oplus [b]_N$$

$$\forall (a,b) \in \mathbf{Z}^2, \quad [a \times b]_N = [a]_N \otimes [b]_N$$

$$[1]_N = 1_{\mathbf{Z}/N\mathbf{Z}}$$

Il découle de la proposition 3.17 qu'on a

$$\forall a \in \mathbf{Z}, \forall n \in \mathbf{Z}, \quad [n.a]_N = n.[a]_N$$

$$\forall a \in \mathbf{Z}, \forall n \in \mathbf{N}, \quad [a^n]_N = [a]_N^{\otimes n}.$$

Il découle de ce qui précède qu'on a notamment pour tout $a, b \in \mathbf{Z}$ les relations

$$a.[b]_N = [a.b]_N = [a \times b]_N = [a]_N \otimes [b]_N = b.[a]_N.$$

3.5.3 Conséquences du fait que le noyau de $[\,.\,]_N$ est $N\,\mathbf{Z}$

Soit $N \geqslant 1$. Pour $a \in \mathbf{Z}$, on a

$$[a]_N = 0_{\mathbf{Z}/N\mathbf{Z}} \Longleftrightarrow a \in N\,\mathbf{Z} \Leftrightarrow a \equiv 0 \mod N \Leftrightarrow N|a.$$

Par conséquent, $[\,.\,]_N$ étant un morphisme d'anneaux, on a pour tout $(a,b) \in \mathbf{Z}^2$ les équivalences

$$[a]_N = [b]_N \Longleftrightarrow [a-b]_N = 0_{\mathbf{Z}/N\mathbf{Z}} \Longleftrightarrow a \equiv b \mod N.$$

Plus généralement, ceci montre que toute relation entre des éléments de $\mathbf{Z}/N\mathbf{Z}$ construite à partir des lois d'anneaux $\oplus$, $\otimes$ est équivalente à une relation de congruence modulo N. Donnons simplement un exemple pour illustrer ce fait général. Soit $(x,y,z) \in (\mathbf{Z}/N\mathbf{Z})^3$. Soit $(a,b,c) \in \mathbf{Z}^3$ tel que $x = [a]_N$ $y = [b]_N$ et $z = [c]_N$ (rappelons que $[\,.\,]_N$ est surjective !). Alors on a

$$x \otimes y \oplus z = [1]_N \Longleftrightarrow a \times b + c \equiv 1 \mod N$$

« Calculer dans $\mathbf{Z}/N\,\mathbf{Z}$, c'est comme calculer modulo N. La différence est au niveau du langage et des notations. »

3.5.4 Système de représentants de $\mathbf{Z}/N\mathbf{Z}$

Définition 3.49 *Soit $N \geqslant 1$. Un* système de représentants *de $\mathbf{Z}/N\mathbf{Z}$ est une partie A de $\mathbf{Z}$ telle que $[\,.\,]_N$ induit une bijection de A sur $\mathbf{Z}/N\mathbf{Z}$, en d'autres termes telle que l'application*

$$\begin{array}{ccc} A & \longrightarrow & \mathbf{Z}/N\mathbf{Z} \\ a & \longmapsto & [a]_N \end{array}$$

est bijective.

Proposition 3.50 *Soit $N \geqslant 1$. Alors $\{0, \ldots, N-1\}$ est un système de représentants de $\mathbf{Z}/N\mathbf{Z}$*

Démonstration : Montrons que

$$\begin{array}{ccc} \{0, \ldots, N-1\} & \longrightarrow & \mathbf{Z}/N\mathbf{Z} \\ a & \longmapsto & [a]_N \end{array}$$

est surjective. Soit $x \in \mathbf{Z}/N\mathbf{Z}$. On sait que l'application

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/N\mathbf{Z} \\ a & \longmapsto & [a]_N \end{array}$$

est surjective. Il existe donc $a \in \mathbf{Z}$ tel que $x = [a]_N$. Soit $a = q\,N + r$ la division euclidienne de a par N. On a donc en particulier $0 \leqslant r \leqslant N-1$ et $r \equiv a \mod N$. D'après la section précédente, la dernière propriété entraîne $[a]_N = [r]_N$ d'où $x = [r]_N$. Conclusion : il existe bien un élément de $\{0, \ldots, N-1\}$ qui s'envoie sur x par $[\,.\,]_N$.

Montrons à présent que l'application

$$\begin{array}{ccc} \{0, \ldots, N-1\} & \longrightarrow & \mathbf{Z}/N\mathbf{Z} \\ a & \longmapsto & [a]_N \end{array}$$

est injective. Soit $n, m \in \{0, \ldots, N-1\}$ vérifiant $[n]_N = [m]_N$. On peut supposer $n \leqslant m$. D'après la section précédente, N divise $m - n$. Or les hypothèse entraînent qu'on a $0 \leqslant m - n \leqslant N-1$. Or le plus petit multiple strictement positif de N est N. Ainsi $m - n = 0$, ce qu'il fallait démontrer. □

Ceci montre en particulier que $\mathbf{Z}/N\mathbf{Z}$ est en bijection avec l'ensemble $\{0, \ldots, N-1\}$, d'où le corollaire qui suit.

Corollaire 3.51 *Pour $N \geqslant 1$, $\mathbf{Z}/N\mathbf{Z}$ est fini, de cardinal N.*

Remarque 3.52 : Cela découlait aussi de la construction de $\mathbf{Z}/N\mathbf{Z}$ décrite ci-dessus. □

Plus généralement, on montre assez facilement que A est un système de représentants de $\mathbf{Z}/N\mathbf{Z}$ si et seulement si pour $a, b \in A$, N ne divise pas $a-b$ et pour tout $x \in \{0, \ldots, N-1\}$ il existe $a \in A$ tel que $a \equiv x \mod N$ si et seulement si pour tout $x \in \{0, \ldots, N-1\}$ il existe un unique $a \in A$ tel que $a \equiv x \mod N$.

Exemple 3.53 : $\{0, 1, \ldots, N-1\}$, $\{1, 2, \ldots, N\}$ plus généralement $\mathcal{S}_k = \{k, k+1, \ldots, N+k-1\}$ où $k \in \mathbf{Z}$, sont des systèmes de représentants de $\mathbf{Z}/N\mathbf{Z}$. On peut en imaginer de plus biscornus, par exemple

$$\{k + k\,N\}_{0 \leqslant k \leqslant N-1}.$$

□

Attention ! Un système de représentants de $\mathbf{Z}/N\,\mathbf{Z}$ est une partie de $\mathbf{Z}$ en bijection avec $\mathbf{Z}/N\,\mathbf{Z}$. L'existence de tels systèmes montre en particulier que $\mathbf{Z}/N\,\mathbf{Z}$, en tant

qu'*ensemble*, s'identifie à une partie de $\mathbf{Z}$ (et de beaucoup de façons différentes). Mais il n'existe aucune identification de $\mathbf{Z}/N\mathbf{Z}$ à une partie de $\mathbf{Z}$ qui respecte les structure d'anneau (ni même les structures de groupe), c'est-à-dire qui fasse de $\mathbf{Z}/N\mathbf{Z}$ un sous-anneau de $\mathbf{Z}$.

Un système de représentants est pratique pour fixer une notation biunivoque des éléments de $\mathbf{Z}/N\mathbf{Z}$, mais ne sert *en aucun cas* à « calculer dans $\mathbf{Z}/N\mathbf{Z}$ comme si c'était une partie de $\mathbf{Z}$ ».

Les systèmes de représentants les plus utilisés sont sans doute les $\mathcal{S}_k$ avec $k = 0$, $k = -(N-2)/2$ si N pair et $k = -(N-1)/2$ N impair.

3.5.5 Ordre des éléments du groupe additif de $\mathbf{Z}/N\mathbf{Z}$

Proposition 3.54 *Soit $N \geqslant 1$. Soit $x \in \mathbf{Z}/N\mathbf{Z}$ et $m \in \mathbf{Z}$ tel que $x = [m]_N$. Alors l'ordre additif de x (c'est à dire l'ordre de x en tant qu'élément du groupe $(\mathbf{Z}/N\mathbf{Z}, +)$) est $\frac{N}{\mathrm{pgcd}(m,N)}$.*

Démonstration : Notons que comme $\mathbf{Z}/N\mathbf{Z}$ est fini, on sait d'avance que tous ses éléments sont d'ordre fini (proposition 2.45). Soit $n \in \mathbf{Z}$ tel que $n.x = 0$. Comme $n.x = n\,[m]_N = [n\,m]_N$, on a $n.x = [0]_N$ si et seulement si N divise $n\,m$ si et seulement si $\frac{N}{\mathrm{pgcd}(m,N)}$ divise n (oui, on a déjà vu ça quelque part...). Le plus petit n strictement positif vérifiant $n.x = 0$ est donc le plus petit multiple strictement positif de $\frac{N}{\mathrm{pgcd}(m,N)}$, à savoir lui-même. □

3.5.6 Diviseurs de zéro et élément inversibles de $\mathbf{Z}/N\mathbf{Z}$

Proposition 3.55 *Soit $N \geqslant 1$. Soit $x \in \mathbf{Z}/N\mathbf{Z}$ et $m \in \mathbf{Z}$ tel que $x = [m]_N$. Les trois assertions suivantes sont équivalentes.*

1. *x est un élément inversible de $\mathbf{Z}/N\mathbf{Z}$;*
2. *on a $pgcd(m, N) = 1$;*
3. *x n'est pas diviseur de zéro.*

Démonstration : On a les équivalences

$$x \in (\mathbf{Z}/N\mathbf{Z})^\times \Leftrightarrow \exists y \in \mathbf{Z}/N\mathbf{Z},\, x\,y = [1]_N \Leftrightarrow \exists n \in \mathbf{Z}/N\mathbf{Z},\, [m]_N\,[n]_N = [1]_N$$

$$\Leftrightarrow \exists n \in \mathbf{Z}/N\mathbf{Z},\, [m\,n]_N = [1]_N \Leftrightarrow N|(m\,n-1) \Leftrightarrow \exists k \in \mathbf{Z}, m\,n - 1 = k\,N.$$

D'après ce qui a été vu en AR1 (théorème de Bézout), la dernière condition équivaut à $\mathrm{pgcd}(m, N) = 1$.

Sur n'importe quel anneau, un élément inversible n'est pas diviseur de zéro.

Pour conclure, il suffit de montrer qu'un élément non inversible de $\mathbf{Z}/N\mathbf{Z}$ est diviseur de zéro. D'après ce qu'on a démontré ci-dessus, dire que $x = [m]_N$ n'est pas inversible équivaut

à dire qu'on a $\mathrm{pgcd}(m, N) \geqslant 2$ (en particulier l'existence d'un tel élément impose $N \geqslant 1$). On peut supposer $m \geqslant 0$. On a

$$m \frac{N}{\mathrm{pgcd}(m, N)} = N \frac{m}{\mathrm{pgcd}(m, N)}.$$

Or $\frac{N}{\mathrm{pgcd}(m,N)}$ et $\frac{m}{\mathrm{pgcd}(m,N)}$ sont entiers. Donc en particulier N divise $m \frac{N}{\mathrm{pgcd}(m,N)}$ et on a

$$x \left[\frac{N}{\mathrm{pgcd}(m, N)}\right]_N = [0]_N.$$

Par ailleurs, comme $\mathrm{pgcd}(m, N) \geqslant 2$, on a $1 \leqslant \frac{N}{\mathrm{pgcd}(m,N)} \leqslant N - 1$; d'où $\left[\frac{N}{\mathrm{pgcd}(m,N)}\right]_N \neq 0$.

Donc x est diviseur de zéro. □

Exercice 21

Soit A un anneau. Pour $a \in A$ soit $\mu_a : A \to A$ l'application qui à $x \in A$ associe $x \mapsto a\,x$. Montrer que μ_a est un morphisme de groupes. Montrer que μ_a est injective si et seulement si a n'est pas un diviseur de zéro. Montrer que μ_a est surjective si et seulement si $a \in A^\times$. En déduire que si A est fini, un élément de A est inversible si et seulement s'il n'est pas diviseur de zéro. Comme cas particulier, on retrouve une partie du théorème précédent.

Corollaire 3.56 *Soit $N \geqslant 1$. Alors le cardinal de $(\mathbf{Z}/N\mathbf{Z})^\times$ est $\varphi(N)$.*

Démonstration : Rappelons que $\varphi(N)$ est le nombre d'entiers compris entre 1 et N qui sont premiers avec N. Comme $[\,.\,]_N$ induit une bijection de $\{1, \ldots, N\}$ sur $\mathbf{Z}/N\mathbf{Z}$, le théorème précédent montre qu'on a une bijection de $\{m \in \{1, \ldots, N\}, \mathrm{pgcd}(m, N) = 1\}$ sur $(\mathbf{Z}/N\mathbf{Z})^\times$. □

Corollaire 3.57 (Théorème d'Euler) *Soit $N \geqslant 1$ et $n \in \mathbf{Z}$. Si $\mathrm{pgcd}(n, N) = 1$ alors $n^{\varphi(N)} \equiv 1 \mod N$.*

Démonstration : D'après le théorème, on a $[n]_N \in (\mathbf{Z}/N\mathbf{Z})^\times$. D'après la proposition 2.51 et le corollaire précédent, on a $[n]_N^{\varphi(N)} = [1]_N$, d'où $n^{\varphi(N)} \equiv 1 \mod N$. □

Remarque 3.58 : Pour N premier on retrouve le petit théorème de Fermat. Rappelons en effet que dans ce cas on a $\varphi(N) = N - 1$ et $\mathrm{pgcd}(n, N) = 1$ si et seulement si n n'est pas multiple de N. □

Remarque 3.59 : Ainsi, si $x \in (\mathbf{Z}/N\mathbf{Z})^\times$, l'ordre de x comme élément du groupe des éléments inversibles, appelé *ordre multiplicatif*, divise $\varphi(N)$. Il ne faut surtout pas le confondre avec l'ordre additif considéré ci-dessus ! Notez par exemple que $[1]_N$ est d'ordre additif N et d'ordre multiplicatif 1. En ce qui concerne l'ordre additif, nous avions donné une formule qui permet de calculer très facilement l'ordre additif d'un élément de $\mathbf{Z}/N\mathbf{Z}$. Le calcul de l'ordre multiplicatif d'un élément inversible est par contre un problème difficile. □

Proposition 3.60 *Soit $N \geqslant 1$. Alors $\mathbf{Z}/N\mathbf{Z}$ est intègre si et seulement si N est premier si et seulement si $\mathbf{Z}/N\mathbf{Z}$ est un corps.*

Démonstration : D'après le théorème ci-dessus, un élément non nul de $\mathbf{Z}/N\mathbf{Z}$ est inversible si et seulement s'il n'est pas diviseur de zéro. Donc $\mathbf{Z}/N\mathbf{Z}$ est intègre si et seulement si $\mathbf{Z}/N\mathbf{Z}$ est un corps.

Toujours d'après le théorème, tout élément non nul de $\mathbf{Z}/N\mathbf{Z}$ est inversible si et seulement si pour tout $n \in \{1, \ldots, N-1\}$ on a $\mathrm{pgcd}(n, N) = 1$. On sait que ceci équivaut à N est premier. □

Si $N = p$ est un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. C'est un exemple de corps fini. On verra plus tard dans le cours comment construire d'autres exemples de corps finis.

3.5.7 Théorème de factorisation, application au théorème chinois

Théorème 3.61 (Théorème de factorisation) *Soit A un anneau, $\mathcal{I}$ un idéal de A, $\pi : A \to A/\mathcal{I}$ le morphisme quotient. Soit C un anneau.*

Pour tout morphisme $\psi : A/\mathcal{I} \to C$, $\psi \circ \pi$ est un morphisme dont le noyau contient $\mathcal{I}$.

Réciproquement, pour tout morphisme $\varphi : A \to C$ de noyau contenant $\mathcal{I}$, il existe un unique morphisme $\widetilde{\varphi} : A/\mathcal{I} \to C$ tel que $\widetilde{\varphi} \circ \pi = \varphi$. On dit que φ se factorise de manière unique par π.

$\widetilde{\varphi}$ est surjectif si et seulement si φ est surjectif.

$\widetilde{\varphi}$ est injectif si et seulement si $\mathrm{Ker}(\varphi) = \mathcal{I}$. Plus généralement on a $\mathrm{Ker}(\widetilde{\varphi}) = \pi(\mathrm{Ker}(\varphi))$.

En particulier si $\varphi : A \to C$ est surjectif, de noyau $\mathcal{I}$, alors φ induit un isomorphisme $\widetilde{\varphi} : A/\mathcal{I} \xrightarrow{\sim} C$.

Ce théorème est admis (sa démonstration est à la portée d'un étudiant motivé).

Corollaire 3.62 (Lemme chinois) *Soient N et M deux entiers strictement positifs tels que $\mathrm{pgcd}(N, M) = 1$.*

Alors l'anneau $\mathbf{Z}/NM\,\mathbf{Z}$ est isomorphe à l'anneau produit $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z}$.

Démonstration : C'est une esquisse, on demande au lecteur de compléter les détails. On regarde l'application

$$\varphi : \begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z} \\ n & \longmapsto & ([n]_N, [n]_M) \end{array} .$$

Alors φ est un morphisme d'anneaux de noyau $NM\,\mathbf{Z}$, donc il se se factorise en un morphisme injectif

$$\widetilde{\varphi} : \mathbf{Z}/NM\,\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z}.$$

Or $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z}$ et $\mathbf{Z}/NM\,\mathbf{Z}$ ont même cardinal, à savoir $N\,M$. Donc $\widetilde{\varphi}$, étant injectif, est aussi surjectif. Donc $\widetilde{\varphi}$ est un isomorphisme. □

Remarque 3.63 : Expliquons le lien de ce résultat avec la résolution des systèmes de congruences vue en AR1. Conservons les mêmes notations et hypothèses que ci-dessus. Soit $(a, b) \in \mathbf{Z}^2$. On souhaite résoudre le système de congruences

$$\begin{cases} n & \equiv a \mod N \\ n & \equiv b \mod M \end{cases} \qquad n \in \mathbf{Z}.$$

Posons $x = [a]_M$ et $y = [b]_N$. Alors résoudre le système revient à décrire l'ensemble

$$\{n \in \mathbf{Z}, \quad \varphi(n) = (x, y)\}.$$

D'après le corollaire, il existe un unique $z \in \mathbf{Z}/NM\mathbf{Z}$ tel que $(x, y) = \widetilde{\varphi}(z)$. Sachant que $\varphi = \widetilde{\varphi} \circ [\,.\,]_{NM}$, on a alors l'équivalence

$$\forall n \in \mathbf{Z}, \quad \varphi(n) = (x, y) \Longleftrightarrow [n]_{NM} = z.$$

Soit $n_0 \in \mathbf{Z}$ tel que $[n_0]_{NM} = z$. L'ensemble des solutions du système de congruence est alors l'ensemble

$$\{n \in \mathbf{Z}, \quad n \equiv n_0 \mod NM\}.$$

Ici la résolution n'est pas complètement effective, car on ne connaît pas explicitement l'inverse de $\widetilde{\varphi}$, et donc on n'a pas a priori de moyen efficace de calculer z (ou, ce qui revient au même, n_0) à partir de a et b. Pour une description effective de $\widetilde{\varphi}^{-1}$, on se reportera à l'exercice 12 du TD 2. □

Remarque 3.64 : Le lemme chinois est faux si M et N ne sont pas premiers entre eux. Par exemple $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/4\,\mathbf{Z}$ ne sont pas isomorphes (ni en tant qu'anneaux, ni même en tant que groupes ; regarder les ordres des éléments). □

Corollaire 3.65 *Soient N et M deux entiers strictement positifs tels que* $\operatorname{pgcd}(N, M) = 1$. *Alors $\varphi(N\,M) = \varphi(N)\,\varphi(M)$.*

Démonstration : Comme $\mathbf{Z}/N\,M\mathbf{Z}$ et $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z}$ sont isomorphes, $(\mathbf{Z}/N\,M\mathbf{Z})^\times$ et $(\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z})^\times$ sont en bijection [19]. D'après la proposition 3.41 on a

$$(\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z})^\times = (\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/M\mathbf{Z})^\times.$$

Ainsi $(\mathbf{Z}/N\,M\mathbf{Z})^\times$ et $(\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/M\mathbf{Z})^\times$ ont le même cardinal. D'après le corollaire 3.56, le premier est de cardinal $\varphi(NM)$ et le second de cardinal $\varphi(N)\varphi(M)$. □

19. Plus précisément, si $f : A \to B$ est un morphisme d'anneaux, alors $f(A^\times)$ est inclus dans $B^\times$ et le morphisme $g : A^\times \to B^\times$ induit par f est un morphisme de groupes. Si en outre f est un isomorphisme, g également.

4 L'anneau des polynômes en une variable à coefficients dans un corps. Application à la construction de corps finis.

4.1 Propriétés élémentaires de l'anneau des polynôme en une variable à coefficients dans un corps

Cette section expose, la plupart du temps sans démonstration, les propriétés de base de l'anneau des polynômes en une variable à coefficients dans un corps $\mathbf{K}$. Ces propriétés, au moins lorsque $\mathbf{K}$ est $\mathbf{R}$ ou $\mathbf{C}$, ont été vues dans le module AR2. Dans tout ce qui suit, on se fixe un corps $\mathbf{K}$ (par exemple $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{F}_p \ldots$).

4.1.1 Premières propriétés

Lemme 4.1 *Soit $(E, +, \times)$ un anneau qui contient un sous-anneau isomorphe à $\mathbf{K}$ (en d'autres termes, il existe un morphisme d'anneaux injectif $\mathbf{K} \to E$) ; on identifie alors $\mathbf{K}$ à ce sous-anneau.*

Pour $\alpha \in \mathbf{K}$ et $v \in E$ on pose $\alpha.v = \alpha \times v$. On définit ainsi une loi de composition externe $\mathbf{K} \times E \to E$.

Alors le triplet $(E, +, .)$ est un $\mathbf{K}$-espace vectoriel.

Noter que la démonstration est immédiate si on se rappelle les définitions d'un espace vectoriel et d'un anneau. Par la suite tout anneau contenant (un sous-anneau isomorphe à) $\mathbf{K}$ sera automatiquement muni, outre sa structure d'anneau, de la structure de $\mathbf{K}$-espace vectoriel définie par le lemme ci-dessus [20].

La démonstration du théorème suivant occupe une annexe du présent chapitre.

Théorème 4.2 *Il existe un anneau $(E, +, \times)$ vérifiant les propriétés suivantes :*

1. *E contient un sous-anneau isomorphe à $\mathbf{K}$;*
2. *E possède un élément X tel que la famille $\{X^n\}_{n \in \mathbf{N}}$ est une base du $\mathbf{K}$-espace vectoriel E.*

Un tel élément X est appelée *indéterminée* de E. Rappelons que par définition $X^0 = 1_E = 1_K$. Les éléments de E sont appelés *polynômes en une indéterminée à coefficients dans* $\mathbf{K}$, en abrégé *polynômes à coefficients dans* $\mathbf{K}$ voire *polynômes* quand le corps $\mathbf{K}$ est clairement indiqué par le contexte. L'élément neutre de l'addition est souvent appelé *le polynôme nul*. Les éléments de $\mathbf{K}$ sont appelés *polynômes constants*. Si X est une indéterminée de E, toute autre indéterminée s'écrit $X + \alpha$ où $\alpha \in \mathbf{K}$. Dans ce qui suit on fixe une indéterminéee X de E et on note $E = \mathbf{K}[X]$.

20. Le nom savant pour de telles structures est $\mathbf{K}$-*algèbre*.

Pour tout élément P de $\mathbf{K}[X]$, il existe une unique suite presque nulle[21] $(a_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{K}$ telle qu'on a :

$$P = \sum_{n\in\mathbf{N}} a_n X^n$$

(il s'agit en fait d'une somme finie !). Cette suite est appelée *suite des coefficients* du polynômes P. Pour $n \in \mathbf{N}$, a_n est appelée *coefficient de degré* n de P. Un polynôme est nul si et seulement si tous ses coefficients sont nuls ; plus généralement deux polynômes sont égaux si et seulement s'ils ont les mêmes coefficients.

Soient P et Q des polynômes, (a_n) la suite des coefficients de P et (b_n) celle de Q. Alors la suite (c_n) de terme général $c_n = \sum_{\ell=0}^{n} a_\ell b_{n-\ell}$ est presque nulle, et c'est la suite des coefficients du produit $P.Q$.

4.1.2 Degré, éléments inversibles, division euclidienne

Soit P un polynôme et (a_n) sa suite de coefficients. L'ensemble $\{n \in \mathbf{N}, \quad a_n \neq 0\}$ est une partie majorée de $\mathbf{N}$, vide si et seulement si P est le polynôme nul. Si P n'est pas nul, cet ensemble a donc un plus grand élément, appelé *degré de* P, et noté $\deg(P)$. Le *coefficient dominant* de P est alors $a_{\deg(P)}$.

Le degré du polynôme nul est $-\infty$. On a

$$\{P \in \mathbf{K}[X], \quad \deg(P) = 0\} = \mathbf{K}^\times.$$

En d'autre termes on a $\deg(P) \leqslant 0$ si et seulement si P est constant.

Si P et Q sont des polynômes, on a

$$\deg(P+Q) \leqslant \mathrm{Max}(\deg(P), \deg(Q))$$

et

$$\deg(P.Q) = \deg(P) + \deg(Q)$$

avec la convention $(-\infty) + n = n + (-\infty) = -\infty$ pour tout $n \in \{-\infty\} \cup \mathbf{N}$. On déduit de la deuxième propriété que $\mathbf{K}[X]$ est un anneau intègre. On en déduit également la détermination de $\mathbf{K}[X]^\times$.

Proposition 4.3 *Les éléments inversibles de* $\mathbf{K}[X]$ *sont les polynômes constants non nuls.*

Démonstration : Si $P = a$ est constant non nul, P est inversible d'inverse le polynôme constant non nul a^{-1} (l'inverse de a dans $\mathbf{K}$).

Réciproquement, soit $P \in \mathbf{K}[X]^\times$. Il existe $Q \in \mathbf{K}[X]$ tel que $PQ = 1$. En prenant les degrés, on obtient $\deg(P) + \deg(Q) = 0$. Comme $\deg(P)$ et $\deg(Q)$ sont des éléments de $\mathbf{N} \cup \{-\infty\}$ on en déduit aussitôt qu'on a $\deg(P) = \deg(Q) = 0$. Ainsi P est constant non nul. □

On a sur $\mathbf{K}[X]$ une division euclidienne analogue à celle qui existe sur $\mathbf{Z}$ (pour la démonstration, *cf.* l'annexe du présent chapitre).

21. dont tous les termes sont nuls sauf un nombre fini

Théorème 4.4 *Soient A et B des éléments de $\mathbf{K}[X]$, avec B* non nul*. Il existe alors un unique couple (Q, R) d'éléments de $\mathbf{K}[X]$ vérifiant $A = B.Q + R$ et $\deg(R) < \deg(B)$*

Noter que comme B est non nul, on a $\deg(B) \geqslant 0$. Si $\deg(B) = 0$, la condition sur le degré de R impose $R = 0$.

4.1.3 Fonction polynôme, évaluation, racines d'un polynômes, corps algébriquement clos

À tout élément P de $\mathbf{K}[X]$, on associe une application $\mathbf{K} \to \mathbf{K}$ définie de la façon suivante : soit (a_n) la suite des coefficients de P ; pour $x \in \mathbf{K}$, on pose

$$P(x) \stackrel{\text{déf}}{=} \sum_{n \in \mathbf{N}} a_n \, x^n$$

(il s'agit en fait d'une somme finie). L'application $x \mapsto P(x)$ est appelée fonction polynôme associée à P.

Si on fixe à présent $a \in \mathbf{K}$, on a une application

$$\begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathbf{K} \\ P & \longmapsto & P(a) \end{array}$$

qui est un morphisme d'anneaux et qui est appelée *évaluation en a*.

Définition 4.5 *Soit $P \in \mathbf{K}[X]$. Une* racine *de P est un élément a de $\mathbf{K}$ vérifiant $P(a) = 0$.*

Exemple 4.6 : Si P est nul, tout élément de $\mathbf{K}$ est racine de P. Si P est constant non nul, P n'a pas de racine. Si $a \in \mathbf{K}$, le polynôme $X - a$ a pour unique racine a. Si $\mathbf{K} = \mathbf{R}$, le polynôme $X^2 + 1$ n'a pas de racine. □

Remarque 4.7 : Très souvent, on se trouve dans la situation où plusieurs corps sont mis en jeux : typiquement deux corps $\mathbf{K}$ et $\mathbf{L}$ tels que $\mathbf{K}$ est un sous-corps de $\mathbf{L}$ (par exemple $\mathbf{K} = \mathbf{R}$ et $\mathbf{L} = \mathbf{C}$). Alors $\mathbf{K}[X]$ s'identifie naturellement à un sous-anneau de $\mathbf{L}[X]$ et tout élément de $\mathbf{K}[X]$ peut donc être « vu » comme un élément de $\mathbf{L}[X]$. Il est crucial de comprendre qu'alors l'expression « racine de P » est ambigue ; ainsi si $X^2 + 1$ est vu comme un élément de $\mathbf{R}[X]$, l'ensemble de ses racines est vide, mais ce n'est pas le cas s'il est vu comme un élément de $\mathbf{C}[X]$. Pour éviter la confusion, il est indispensable de préciser dans ce genre de situation si on considère les racines « dans $\mathbf{K}$ » ou « dans $\mathbf{L}$ ». □

Proposition 4.8 *Soit $P \in \mathbf{K}[X]$ et $a \in \mathbf{K}$. Alors a est une racine de P (dans $\mathbf{K}$) si et seulement s'il existe $Q \in \mathbf{K}[X]$ tel que $P = (X - a).Q$.*

Démonstration : Si $P = (X - a).Q$, alors en évaluant en a, on obtient $P(a) = (a - a).Q(a) = 0$.

Supposons à présent $P(a) = 0$. Comme $X - a$ est non nul, on peut considérer $P = (X - a).Q + R$ la division euclidienne de P par $X - a$. En particulier on a $\deg(R) \leqslant 0$. En évaluant en a on obtient

$$0 = P(a) = (a - a).Q(a) + R(a) = R(a)$$

donc $R(a) = 0$. Donc R est un polynôme constant qui a au moins une racine ; ainsi $R = 0$, d'où le résultat. □

Corollaire 4.9 *Soit $P \in \mathbf{K}[X]$ un polynôme non nul. Alors l'ensemble des racines de P est de cardinal au plus* $\deg(P)$.

Démonstration : On montre par récurrence sur $n \in \mathbf{N}$ l'assertion $\mathcal{H}_n$ suivante : « tout polynôme de degré n a au plus n racines ».

$\mathcal{H}_0$ est vraie car les polynômes de degré 0 sont les polynômes constants non nuls, qui n'ont pas de racine.

Supposons $\mathcal{H}_n$ vraie pour un $n \in \mathbf{N}$. Soit P un polynôme de degré $n + 1$. Si P n'a pas de racine, l'assertion « P a au plus $n + 1$ racines est vraie ». Supposons à présent que P a une racine a. D'après la proposition précédente, il existe $Q \in \mathbf{K}[X]$ tel que $P = (X - a)Q$. On a en particulier

$$n + 1 = \deg(P) = \deg(X - a) + \deg(Q) = 1 + \deg(Q)$$

donc $\deg(Q) = n$. Soit $\mathcal{R}$ l'ensemble des racines de P distinctes de a. Soit $b \in \mathcal{R}$. On a, en évaluant en b,

$$0 = P(b) = (b - a).Q(b)$$

soit comme $b - a \neq 0$ et $\mathbf{K}$ est intègre, $Q(b) = 0$. Ainsi $\mathcal{R}$ est inclus dans l'ensemble des racines de Q. D'après $\mathcal{H}_n$, $\mathcal{R}$ est de cardinal au plus n. L'ensemble des racines de P, étant la réunion de $\{a\}$ et de $\mathcal{R}$, est alors bien de cardinal au plus $n + 1$. Ainsi $\mathcal{H}_{n+1}$ est vraie, ce qui conclut la démonstration. □

Définition 4.10 *Le corps $\mathbf{K}$ est dit* algébriquement clos *si tout polynôme non constant de $\mathbf{K}[X]$ admet une racine (dans $\mathbf{K}$).*

Exemple 4.11 : $\mathbf{R}$ n'est pas algébriquement clos.

Si p est un nombre premier, $\mathbf{F}_p$ n'est pas algébriquement clos (considérer le polynôme $X^p - X + [1]_p$). □

Théorème 4.12 (Théorème fondamental de l'algèbre) *Le corps $\mathbf{C}$ est algébriquement clos.*

Remarque 4.13 : En dépit de son nom, toutes les démonstrations connues de ce théorème font appel, au moins en partie, à des arguments d'analyse. □

4.2 Arithmétique de $\mathbf{K}[X]$

Dans cette partie, on va en fait considérer un anneau *intègre* A quelconque. Les notions et résultats développés s'appliqueront en particulier à $\mathbf{K}[X]$ (pour $\mathbf{K}$ corps quelconque) et à $\mathbf{Z}$. Un autre exemple de terrain d'application sera vu au dernier chapitre de ce cours : celui de l'anneau des entiers de Gauss. L'hypothèse « abstraite » cruciale commune vérifiée par ces trois anneaux est celle d'être principal [22] (*cf.* la définition 4.28).

Dans tout ce qui suit, A est un anneau *intègre* fixé.

Lemme 4.14 *[Rappel] Pour tout $a \in A$, l'ensemble $a\,A \overset{déf}{=} \{ab, \quad b \in A\}$ est un idéal de A ; tout idéal de A contenant a contient également aA.*

Définition 4.15 *Un idéal I de A est dit* principal *s'il existe $a \in A$ tel que $I = a\,A$.*

Définition 4.16 *Soit a et b des éléments de A. On dit que a divise b, ou encore que b est un multiple de a, et on note $a|b$, s'il existe $c \in A$ tel que $b = c\,a$.*

Remarque 4.17 : Attention ! Tout élément de A divise 0_A, mais n'est pas nécessairement un « diviseur de zéro » au sens de la définition 3.28. D'ailleurs, comme l'anneau A est ici supposé intègre, 0_A est le seul diviseur de zéro au sens de la définition 3.28. □
Remarque 4.18 : Si a est un élément inversible de A, a divise n'importe quel élément de A. □

Lemme 4.19 *Soient $a, b \in A$.*
Alors a divise b si et seulement si on a l'inclusion $b\,A \subset a\,A$.
Par ailleurs les propriétés suivantes sont équivalentes :

1. *a divise b et b divise a ;*
2. *on a $b\,A = a\,A$;*
3. *il existe $c \in A^\times$ tel que $b = c\,a$;*
4. *il existe $c \in A^\times$ tel que $a = c\,b$.*

Démonstration : La première propriété se démontre exactement comme dans le cas particulier $A = \mathbf{Z}$ (*cf.* la proposition 3.2). L'équivalence 1. $\Leftrightarrow$ 2. en découle aussitôt. L'équivalence 3. $\Leftrightarrow$ 4. est facile et laissée au lecteur. On en déduit alors 3. $\Rightarrow$ 1. Il reste à montrer 1. $\Rightarrow$ 3.. Si $b = 0$, on a $a = 0$ et 3. est vraie avec $c = 1$. Supposons $b \neq 0$. Par hypothèse, il existe $c \in A$ tel que $b = c\,a$ et $d \in A$ tel que $a = d\,b$. En particulier on a $b = c\,d\,b$ soit $b\,(1 - c\,d) = 0$. Comme A est supposé intègre et b est non nul, on en déduit $c\,d = 1$. En particulier $c \in A^\times$. □

22. En fait, on a mieux que ça, car ces trois anneaux admettent chacun une division euclidienne, et sont donc « euclidiens » dans un sens abstrait qu'on ne développera pas dans ce cours ; tout anneau euclidien est principal.

Définition 4.20 *Soit $a, b \in A$. On dit que a et b sont des éléments* associés *si l'une des quatre conditions équivalentes de la proposition précédente est vérifiée.*

Remarque 4.21 : Noter que si a, a' et b sont des éléments de A, avec a et a' d'une part, b, b' d'autre part, associés, alors a divise b si et seulement a' divise b'. □

Définition 4.22 *Un élément a de A est dit* irréductible *s'il est non nul, non inversible, et toute écriture $a = bc$ avec $b, c \in A$ entraîne que $b \in A^\times$* ou *$c \in A^\times$.*

Exemple 4.23 : Les éléments irréductibles de $\mathbf{Z}$ sont les nombres premiers et leurs opposés.

Le cas où $A = \mathbf{K}[X]$ sera examiné plus en détail au paragraphe suivant. □

Remarque 4.24 : Un élément a de A est irréductible si et seulement s'il est non nul, non inversible, et tout élément qui divise a est soit inversible soit associé à a. □

Lemme 4.25 *Soit $a \in A$. Alors a est irréductible si et seulement si tout élément associé à a est irréductible.*

Définition 4.26 *Deux éléments a et b de A sont dit* premiers entre eux *si les seuls éléments de A qui divisent à la fois a et b sont les inversibles de A.*

Proposition 4.27 *Soit a un élément irréductible de A et $b \in A$. Alors a et b ne sont pas premiers entre eux si et seulement si a divise b.*

Démonstration : Si a divise b, a est un diviseur commun de a et b qui est non inversible (car irréductible), donc a et b ne sont pas premiers entre eux.

Si a et b ne sont pas premier entre eux, il existe un diviseur commun c de a et b qui n'est pas inversible. Comme a est irréductible, c et a sont associés. Comme c divise b, a également. □

Définition 4.28 *Un anneau* principal *est un anneau intègre dont tous les idéaux sont principaux (cf. pour mémoire la définition 4.15).*

Exemple 4.29 : Tous les corps fournissent des exemples (peu intéressants dans la pratique) d'anneaux principaux. Rappelons en effet que si A est un corps les seuls idéaux de A sont $\{0\} = 0.A$ et $A = 1.A$.

$\mathbf{Z}$ est un anneau principal d'après le théorème 3.1.

Si $\mathbf{K}$ est un corps, $\mathbf{K}[X]$ est un anneau principal : c'est le contenu du théorème 4.30 ci-dessous.

On verra dans le dernier chapitre du cours un autre exemple d'anneau principal : l'anneau des entiers de Gauss.

Il n'est pas facile, à notre niveau, d'exhiber des exemples d'anneaux intègres qui ne soient pas principaux. L'anneau $\mathbf{K}[X, Y]$ des polynômes en *deux* indéterminées à coefficients dans un corps $\mathbf{K}$ est un tel exemple. □

Théorème 4.30 *Soit* $\mathbf{K}$ *un corps. Alors l'anneau* $\mathbf{K}[X]$ *est principal.*

Démonstration : Il est intéressant de comparer cette démonstration à celle du théorème 3.1.

On sait que $\mathbf{K}[X]$ est intègre.

Soit I un idéal de $\mathbf{K}[X]$. Il s'agit de montrer qu'il existe $P \in \mathbf{K}[X]$ tel que $I = P\mathbf{K}[X]$. Si $I = \{0\}$, c'est vrai. Supposons donc $I \neq 0$. Alors l'ensemble

$$\{\deg(P), \quad P \in I \setminus \{0\}\}$$

est une partie non vide de $\mathbf{N}$, qui admet donc un plus petit élément d. Soit $P \in I \setminus \{0\}$ vérifiant $\deg(P) = d$. Montrons que $I = P\,\mathbf{K}[X]$. Tout d'abord, comme $P \in I$, on a $P\,\mathbf{K}[X] \subset I$ d'après le lemme 4.14.

Soit à présent $A \in I$. Il s'agit de montrer que P divise A. Comme P est non nul, on peut considérer $A = P.Q + R$ la division euclidienne de A par P. On a ainsi d'une part $\deg(R) < \deg(P) = d$ et d'autre part $R = A - P\,Q$ d'où, comme A et P sont dans I, $R \in I$. Ainsi $R \neq 0$ contredirait la définition de d. Donc $R = 0$ et on a terminé. □

Théorème 4.31 *Soit* A *un anneau principal.*

1. *Toute paire d'élément de* A *admet un pgcd. Plus précisément, pour tous* $a, b \in A$*, il existe* $\delta \in A$ *tel que* $\delta|a$*,* $\delta|b$ *et pour tout* $d \in A$ *tel que* $d|a$ *et* $d|b$ *alors* d *divise* δ*. Un tel* δ *est appelé un* pgcd *de* a *et* b*.*

   Si δ' *est un autre pgcd de* a *et* b*, alors* δ *et* δ' *sont associés et réciproquement.*

   a *et* b *sont premiers entre eux si et seulement si* 1 *est un pgcd de* a *et* b *si et seulement si tout pgcd de* a *et* b *est un inversible de* A*.*

2. A *vérifie le* théorème de Bézout*. Plus précisément, pour tous* $a, b \in A$*, si* δ *est un pgcd de* a *et* b*, alors il existe* $\alpha, \beta \in A$ *tel que*

   $$\alpha\, a + \beta\, b = \delta.$$

   Par ailleurs a *et* b *sont premiers entre eux si et seulement s'il existe* $\alpha, \beta \in A$ *tel que*

   $$\alpha\, a + \beta\, b = 1.$$

3. A *vérifie les «* lemmes de Gauss *». Plus précisément, soient* a*,* b *et* c *des éléments de* A*. Alors :*

   (a) *Si* a *et* b *divise* c *et si* a *et* b *sont premiers entre eux alors* $a\,b$ *divise* c*.*

   (b) *Si* a *divise* $b\,c$ *et si* a *et* b *sont premiers entre eux alors* a *divise* c*.*

   En particulier A *vérifie le* lemme d'Euclide*. Plus précisément, soit* a*,* b *et* c *des éléments de* A *tel que* a *est* irréductible *et* a *divise* $b\,c$*; alors* a *divise* b *ou* a *divise* c*.*

4. *A est un anneau* factoriel*, autrement dit tout élément non nul et non inversible se décompose en un produit d'éléments irréductibles, et la décomposition est unique « à l'ordre et aux inversibles près ».*

   Plus précisément, si $a \in A$ est non nul et non inversible, il existe un entier strictement positif n et des éléments irréductibles $\pi_1, \ldots, \pi_n$ de A tels que

$$a = \prod_{i=1}^{n} \pi_i \ ;$$

   en outre, si m un entier strictement positif et $\tau_1, \ldots, \tau_m$ sont m éléments irréductibles de A tels que

$$a = \prod_{i=1}^{m} \tau_i \ ;$$

   alors $n = m$ et quitte à renuméroter les τ_i, pour tout $1 \leqslant i \leqslant n$, π_i et τ_i sont associés.

Remarque 4.32 : Même si l'abus est couramment pratiqué, il est incorrect en toute rigueur de parler *du* pgcd de deux éléments de A et de noter $\mathrm{pgcd}(a, b)$. « Le » pgcd n'est défini qu'à multiplication par un inversible près.

Cependant dans certains cas il est possible de choisir de manière « canonique » un pgcd parmi tous ceux existant. Si $A = \mathbf{Z}$, on peut choisir parmi les pgcd celui qui est positif ; on retrouve ainsi la définition classique. Si $A = \mathbf{K}[X]$, on peut choisir parmi les pgcd celui qui est de coefficient dominant égal à 1 (sauf bien sûr si 0 est un pgcd, mais dans ce cas c'est le seul). □

Remarque 4.33 : Cette remarque est intimement liée à la remarque précédente. Dans certains cas, lorsqu'il existe un choix « canonique » des irréductibles, on peut remplacer la conclusion « π_i et τ_i sont associés » dans le 4. par $\pi_i = \tau_i$, quitte à rajouter un facteur inversible dans la décomposition. Par exemple si $A = \mathbf{Z}$ on peut, quitte à rajouter un signe dans la décomposition, ne considérer que les irréductibles qui sont positifs (c'est-à-dire les nombres premiers) et si $A = \mathbf{Z}[X]$ on peut, quitte à rajouter un scalaire non nul dans la décomposition, ne considérer que les polynômes irréductibles qui sont unitaires. □

Démonstration : Hormis l'*existence* d'une décomposition en produit d'irréductibles, un peu délicate techniquement (et traitée dans le DM donné en 2012-2013), le reste de la démonstration de ce théorème est une copie presque conforme des arguments utilisés pour la démonstration dans le cas où $A = \mathbf{Z}$ et que vous connaissez déjà (pour le 1., il s'agit des arguments « à la sauce sous-groupes », *cf.* le corollaire 3.3). On se permettra ainsi d'être assez succinct.

Pour le 1. (en gardant constamment en tête le lemme 4.19), $a\,A + b\,A$ est un idéal contenant $a\,A$ et $b\,A$, donc, comme A est principal, de la forme $\delta\,A$ pour un $\delta \in A$. Comme $\delta\,A$ contient $a\,A$ (respectivement $b\,A$), δ divise a (respectivement b). Soit d tel que $d\,A$ contient $a\,A$ et $b\,A$. Alors d contient $a\,A + b\,A$ donc $\delta\,A$. Et δ' est un pgcd de a et b si et seulement si $\delta'\,A = \delta\,A$.

On en déduit aussitôt le théorème de Bézout.

Supposons qu'il existe $\alpha, \beta \in A$ tel que $\alpha\, a + \beta\, b = 1$.

Supposons en outre que a et b divisent c. Écrivons $c = k\, a = \ell\, b$ avec $k, \ell \in A$. On a

$$c = c.1 = \alpha\, a\, c + \beta b\, c = \alpha\, a\, \ell\, b + \beta b\, k\, a = (\alpha\, \ell + \beta\, k)\, a\, b.$$

Ainsi $a\, b$ divise c.

Supposons à présent que a divise $b\, c$. Comme a divise $b\, c$, a divise

$$\alpha\, a\, c + \beta b\, c = c.1 = c.$$

Le lemme d'Euclide découle aussitôt du second lemme de Gauss, compte tenu de 4.27.

L'« unicité » de la décomposition en produit d'irréductibles est alors conséquence de ce lemme d'Euclide. □

4.3 Polynômes irréductibles

Il est à noter que l'expérience montre que cette notion, notamment son lien avec la notion de racine, pose traditionnellement de gros problèmes aux étudiants ; n'hésitez donc pas à la travailler soigneusement.

4.3.1 Rappel de la définition et premières remarques

Si on particularise la définition 4.22 dans le cas où $A = \mathbf{K}[X]$, on obtient, compte tenu de la connaissance de $\mathbf{K}[X]^\times$:

Proposition 4.34 *Un polynôme P est irréductible si et seulement s'il est non constant, et toute écriture $P = Q\, R$ entraîne que Q ou R est constant.*

Remarque 4.35 : Un polynôme non constant P n'est pas irréductible si et seulement s'il admet un diviseur de degré strictement positif, et strictement inférieur à $\deg(P)$. □

Exemple 4.36 : Tout polynôme de degré 1 est irréductible.

Un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine. □

Remarque 4.37 : Dans la continuation de la remarque 4.7, si $\mathbf{K}$ est un sous-corps de $\mathbf{L}$, un élément irréductible de $\mathbf{K}[X]$ n'est pas nécessairement irréductible dans $\mathbf{L}[X]$ (la réciproque est vraie cependant). Par exemple $X^2 + 1$ est irréductible comme élément de $\mathbf{R}[X]$ mais pas comme élément de $\mathbf{C}[X]$. On aura donc intérêt à préciser, dans ce genre de situation, « irréductible dans $\mathbf{K}[X]$ (respectivement dans $\mathbf{L}[X]$) », souvent abrégé en « irréductible sur $\mathbf{K}$ (respectivement sur $\mathbf{L}$) ».

Par contre, « le pgcd est invariant par extension du corps de base ». Plus précisément, si P et Q sont des éléments de $\mathbf{K}[X]$ et Δ est un pgcd de P et Q (vus comme éléments de $\mathbf{K}[X]$), alors Δ est un pgcd de P et Q vus comme éléments de $\mathbf{L}[X]$. Voyez-vous pourquoi ? En particulier, lorsqu'on parle de polynômes premiers entre eux, on n'a pas besoin de préciser le « corps de base ». □

4.3.2 Lien entre irréductibilité et racine

Proposition 4.38 *Un polynôme de degré au moins* 2 *irréductible n'a pas de racine.*

Remarque 4.39 : La réciproque est vraie si le degré est 2 ou 3, et fausse dès que le degré est au moins 4. Par exemple, si $\mathbf{K} = \mathbf{R}$, le polynôme $(X^2+1)^2$ n'a pas de racine mais n'est pas irréductible. □

Démonstration : Montrons la contraposée. Si P polynôme de degré 2 admet une racine a, alors P est divisible par $X - a$, donc admet un diviseur de degré strictement positif et strictement inférieur à $\deg(P)$. Ainsi P n'est pas irréductible. □

4.3.3 Cas des corps algébriquement clos

Les polynômes irréductibles sont les polynômes de degré 1. En effet, on sait que ces derniers sont toujours irréductibles, et par ailleurs tout polynôme de degré au moins 2 possède une racine, donc un diviseur de degré 1.

4.3.4 Cas de R

Proposition 4.40 *Les polynômes de* $\mathbf{R}[X]$ *irréductibles sont les polynômes de degré* 1 *et les polynômes de degré* 2 *sans racines réelles.*

Démonstration : On sait déjà que les polynômes de degré 1 et de degré 2 sans racines réelles sont irréductibles, et qu'un polynôme de degré 2 admettant une racine réelle n'est pas irréductible.

Il reste donc à montrer qu'un polynôme réel P de degré au moins 3 n'est pas irréductible. Comme $\mathbf{C}$ est algébriquement clos, P possède une racine complexe a. Si $a \in \mathbf{R}$, P n'est pas irréductible. Supposons $a \in \mathbf{C}\setminus\mathbf{R}$. Alors en conjuguant la relation $P(a) = 0$, compte tenu du fait que les coefficients de P sont réels, on obtient $P(\overline{a}) = 0$. Ainsi $X - a$ et $X - \overline{a}$ divisent P (dans $\mathbf{C}[X]$). Or ces deux polynômes sont premiers entre eux (exercice : le démontrer), donc par le lemme de Gauss le polynôme $Q = (X-a)(X-\overline{a})$ divise P (dans $\mathbf{C}[X]$). Notons que $\deg(Q) = 2$ et $Q \in \mathbf{R}[X]$. Pour conclure il suffit de montrer que Q divise P dans $\mathbf{R}[X]$. Plus précisément, on sait qu'il existe $R \in \mathbf{C}[X]$ qui satisfait $P = Q\,R$ et il s'agit de montrer qu'en fait $R \in \mathbf{R}[X]$. Mais en conjuguant on obtient

$$P = \overline{P} = Q\,\overline{R} = Q\,R$$

d'où, par intégrité de $\mathbf{C}[X]$, $R = \overline{R}$, ce qui conclut. □

Exercice 22

Soit $\mathbf{L}$ un corps et $\mathbf{K}$ un sous-corps de $\mathbf{K}$. Soient P, Q des éléments de $\mathbf{K}[X]$. On suppose qu'il existe $R \in \mathbf{L}[X]$ tel que $P = Q\,R$. Montrer qu'alors on a $R \in \mathbf{K}[X]$.

4.3.5 Cas de Q

Nous nous contentons de signaler le résultat suivant : il existe des polynômes à coefficients dans $\mathbf{Q}$ irréductibles (sur $\mathbf{Q}$) de n'importe quel degré strictement positif. Par exemple pour tout $n \geqslant 1$, le polynôme $X^n - 2$ est irréductible sur $\mathbf{Q}$ (difficile, *cf.* l'exercice 1 du DM de 2012-2013).

4.3.6 Cas de $\mathbf{F}_p$

Il y a également des polynômes irréductibles de n'importe quel degré strictement positif. On peut les énumérer par récurrence sur le degré (noter qu'il n'y a qu'un nombre fini de polynômes de degré donné à coefficients dans $\mathbf{F}_p$).

Exercice 23

Déterminer tous les polynômes irréductibles de degrés 1, 2, 3 et 4 sur $\mathbf{F}_2$.

4.4 Description du quotient de $\mathbf{K}[X]$ par un idéal, corps finis

4.4.1 Description du quotient

Soit $\mathbf{K}$ un corps. Pour tout élément P de $\mathbf{K}[X]$, on note $\langle P\rangle$ l'idéal $P\,\mathbf{K}[X]$. On note π_P (voire π lorsque le polynôme P est clairement indiqué par le contexte) le morphisme quotient $\mathbf{K}[X] \to \mathbf{K}[X]/\langle P\rangle$.

Théorème 4.41 *Soit $P \in \mathbf{K}[X]$ un polynôme de degré $n \geqslant 1$. Soit $t \overset{déf}{=} \pi_P(X)$.*

La restriction de π_P à $\mathbf{K} \subset \mathbf{K}[X]$ est injective. En particulier $\mathbf{K}$ s'identifie à un sous-anneau du quotient $\mathbf{K}[X]/\langle P\rangle$, donc $\mathbf{K}[X]/\langle P\rangle$ est naturellement muni d'une structure de $\mathbf{K}$-espace vectoriel (cf. le lemme 4.1).

Alors π_P est un morphisme de $\mathbf{K}$-espace vectoriel (une application linéaire) et $\{t^r\}_{0\leqslant r\leqslant n-1}$ est une base de $\mathbf{K}[X]/\langle P\rangle$.

Démonstration : Que π_P soit une application linéaire découle aussitôt du fait que c'est un morphisme d'anneaux et de la façon dont on définit la multiplication par un scalaire dans cette situation (*cf.* encore une fois le lemme 4.1).

Soit $(a_0, \ldots, a_{n-1}) \in \mathbf{K}^n$. Pour $\Pi \in \mathbf{K}[X]$, montrons l'équivalence des assertions suivantes.

1. On a $\pi_P(\Pi) = \sum_{r=0}^{n-1} a_r\, t^r$.
2. Le polynôme $\sum_{r=0}^{n-1} a_r\, X^r$ est le reste de la division euclidienne de Π par P.

Ceci permettra de conclure, compte tenu de l'existence et de l'unicité de la division euclidienne.

On a, compte tenu du fait que π_P est un morphisme d'anneaux,

$$\pi_P(\Pi) = \sum_{r=0}^{n-1} a_r\, t^r \iff \pi_P(\Pi) = \pi_P\left(\sum_{r=0}^{n-1} a_r\, X^r\right) \iff \Pi - \sum_{r=0}^{n-1} a_r\, X^r \in P\,\mathbf{K}[X] = \mathrm{Ker}(\pi_P)$$

$$\iff \exists Q \in \mathbf{K}[X], \quad \Pi - \sum_{r=0}^{n-1} a_r\, X^r = Q\, P \iff \exists Q \in \mathbf{K}[X], \quad \Pi = Q\, P + \sum_{r=0}^{n-1} a_r\, X^r$$

d'où le résultat, compte tenu de

$$\deg\left(\sum_{r=0}^{n-1} a_r\, X^r\right) \leqslant n-1 < \deg(P).$$

□

L'addition dans le quotient $\mathbf{K}[X]/\langle P\rangle$ se décrit facilement en termes des décompositions dans la base $\{1,\dots,t^{n-1}\}$. Pour $(a_r)_{0\leqslant r\leqslant n-1}$ et $(b_r)_{0\leqslant r\leqslant n-1}$, on a en effet

$$\left(\sum_{r=0}^{n-1} a_r\, t^r\right) + \left(\sum_{r=0}^{n-1} b_r\, t^r\right) = \sum_{r=0}^{n-1} (a_r + b_r)\, t^r. \tag{4.4.1}$$

Pour la multiplication, c'est un peu plus compliqué. Comme π_P est un morphisme d'anneaux, on a évidemment la formule

$$\left(\sum_{r=0}^{n-1} a_r\, t^r\right)\, \left(\sum_{r=0}^{n-1} b_r\, t^r\right) = \sum_{r=0}^{2\,n-2} \left(\sum_{\ell+\ell'=r} a_\ell b_{\ell'}\right)\, t^r \tag{4.4.2}$$

mais l'expression de droite n'est pas une décomposition dans la base $\{1,\dots,t^{n-1}\}$, à cause de l'apparition des expressions t^r avec $n \leqslant r \leqslant 2\,n-2$. Pour résoudre ce problème, on peut calculer le reste de la division euclidienne du polynôme

$$\left(\sum_{r=0}^{n-1} a_r\, X^r\right)\, \left(\sum_{r=0}^{n-1} b_r\, X^r\right)$$

par P : ses coefficients donneront la décomposition cherchée pour le produit.

Si ce type de calcul doit être répété un grand nombre de fois (par exemple pour établir la table de multiplication du quotient) il sera plus intéressant de calculer au préalable la décomposition des éléments $t^n,\dots,t^{2\,n-2}$ dans la base $\{1,\dots,t^{n-1}\}$, en effectuant les divisions euclidiennes de $X^n,\dots,X^{2\,n-1}$ par P (voire plus directement, en exploitant notamment la relation $\pi_P(P)=0$, *cf.* les exemples plus loin). Ceci étant fait, il est alors aisé d'écrire la décomposition d'une expression du type du membre de droite de (4.4.2).

Exemple 4.42 : Prenons $\mathbf{K}=\mathbf{R}$ et $P=X^2+1$. Ainsi $\{1,t\}$ est une base du $\mathbf{R}$-espace vectoriel $\mathbf{R}[X]/\langle X^2+1\rangle$. Comme $\pi_P(P)=0=\pi_P(X^2+1)$, on a $t^2+1=0$ soit $t^2=-1$. Ceci détermine entièrement la multiplication dans $\mathbf{R}[X]/\langle X^2+1\rangle$ en termes des décompositions dans la base $\{1,t\}$. On a pour $(a,b,c,d)\in\mathbf{R}^2$

$$(a+b\,t)(c+d\,t) = a\,c + (a\,d+b\,c)\,t + b\,d\,t^2 = (a\,c-b\,d) + (a\,d+b\,c)\,t.$$

□

Exercice 24

$\mathbf{R}[X]/\langle X^2+1\rangle$ est en fait beaucoup plus connu sous le nom de...

De manière similaire au cas des anneaux quotients $\mathbf{Z}/N\mathbf{Z}$, on détermine à présent les éléments inversibles des quotients $\mathbf{K}[X]/\langle P\rangle$, ce qui permettra de caractériser lesquels de ces quotients sont des corps.

Théorème 4.43 *Soit* $\mathbf{K}$ *un corps et* $P \in \mathbf{K}[X]$ *un polynôme non constant. Pour tout* $Q \in \mathbf{K}[X]$*, les assertions suivantes sont équivalentes :*

1. $\pi_P(Q)$ *est inversible ;*
2. $\pi_P(Q)$ *n'est pas diviseur de zéro ;*
3. P *et* Q *sont premiers entre eux.*

En particulier $\mathbf{K}[X]/\langle P\rangle$ *est un corps si et seulement si* $\mathbf{K}[X]/\langle P\rangle$ *est intègre si et seulement si* P *est irréductible.*

Démonstration : Elle est très semblable au cas de $\mathbf{Z}/N\mathbf{Z}$ (proposition 3.55). Ce n'est pas étonnant si l'on considère l'exercice 25 ci-dessous.

On a les équivalences

$$\pi_P(Q) \in (\mathbf{K}[X]/\langle P\rangle)^\times \Leftrightarrow \exists y \in \mathbf{K}[X]/\langle P\rangle,\, \pi_P(Q)\, y = 1 \Leftrightarrow \exists R \in \mathbf{K}[X],\, \pi_P(Q)\,\pi_P(R) = \pi_P(1)$$

$$\Leftrightarrow \exists R \in \mathbf{K}[X],\, \pi_P(Q\,R) = \pi_P(1) \Leftrightarrow P \text{ divise } Q\,R - 1 \Leftrightarrow \exists T \in \mathbf{K}[X], Q\,R - 1 = T\,N.$$

D'après le théorème de Bézout, la dernière condition équivaut au fait que Q et P sont premiers entre eux.

Sur n'importe quel anneau, un élément inversible n'est pas diviseur de zéro (bis repetita).

La fin de la démonstration est laissée à titre d'exercice. □

Exercice 25

Soit A un anneau principal et $a \in A$. Soit $\pi : A \to A/a\,A$ le morphisme quotient.

Montrer que pour tout $b \in A$, $\pi(b)$ est inversible si et seulement si $\pi(b)$ n'est pas diviseur de zéro si et seulement si a et b sont premiers entre eux.

En déduire que A/aA est un corps si et seulement si A/aA est intègre si et seulement si a est irréductible.

Remarque 4.44 : Si P est un polynôme de degré 1, P est irréductible ; ainsi $\mathbf{K}[X]/\langle P\rangle$ est un corps. Mais on n'a pas construit ainsi un « nouveau » corps ; on vérifie en effet que $\mathbf{K}[X]/\langle P\rangle$ est isomorphe à $\mathbf{K}$.

Les constructions intéressantes interviennent quand on quotiente $\mathbf{K}[X]$ par un idéal engendré par un polynôme irréductible de degré au moins 2 ; on obtient alors un corps qui contient $\mathbf{K}$ comme sous-corps strict. On a déjà vu l'exemple de $\mathbf{R}[X]/\langle X^2+1\rangle$.

Dans la fin de ce chapitre on va regarder de plus près le cas où $\mathbf{K}$ est le corps $\mathbf{F}_p$, p étant un nombre premier. Cela va nous permettre de construire de nouveaux corps finis. □

4.4.2 Construction de nouveaux corps finis

Par « nouveau corps fini », on entend des corps finis qui ne sont pas isomorphes à un corps de la forme $\mathbf{F}_p$ où p est un nombre premier.

Proposition 4.45 *Soit p un nombre premier, $n \geqslant 1$, et P un polynôme de degré n à coefficients dans $\mathbf{F}_p$ et irréductible sur $\mathbf{F}_p$. Alors $\mathbf{F}_p[X]/\langle P\rangle$ est fini, de cardinal p^n. En particulier si $n \geqslant 2$ et P est irréductible, $\mathbf{F}_p[X]/\langle P\rangle$ est un nouveau corps fini.*

Démonstration : On a vu que $\mathbf{F}_p[X]/\langle P\rangle$ est un $\mathbf{F}_p$-espace vectoriel de dimension finie égale à n. En tant que $\mathbf{F}_p$-espace vectoriel, il est donc isomorphe à $\mathbf{F}_p^n$, d'où le résultat pour le cardinal.

En particulier si $n \geqslant 2$ et P est irréductible, $\mathbf{F}_p[X]/\langle P\rangle$ est un corps de cardinal p^n ; notamment son cardinal n'est pas premier, donc il n'est isomorphe à aucun corps fini de la forme $\mathbf{F}_q$ où q est un nombre premier. □

Pour exhiber de nouveaux corps finis, il suffit donc d'exhiber des polynômes irréductibles de degré au moins égal à 2 à coefficients dans un corps $\mathbf{F}_p$ où p est un nombre premier. Nous avons déjà signalé que pour tout entier $n \geqslant 1$, il existe des polynômes irréductibles de degré n à coefficients dans $\mathbf{F}_p$. En particulier pour tout premier p et tout entier $n \geqslant 1$ il existe au moins un corps fini de cardinal p^n. On peut montrer par ailleurs que tout corps fini a un cardinal de cette forme, et que p et n étant fixés, tous les corps de cardinal p^n sont deux à deux isomorphes.

Au niveau de ce cours, nous nous contenterons de donner quelques exemples de construction lorsque n et p sont petits.

Proposition 4.46 *Le seul polynôme irréductible de degré 2 sur $\mathbf{F}_2$ est*

$$[1]_2X^2 + [1]_2X + [1]_2$$

Les polynômes irréductibles de degré 3 sur $\mathbf{F}_2$ sont

$$[1]_2X^3 + [1]_2X + [1]_2 \text{ et } [1]_2X^3 + [1]_2X^2 + [1]_2.$$

Les polynômes irréductibles de degré 2 sur $\mathbf{F}_3$ sont

$$[1]_3X^2 + [1]_3, \quad [1]_3X^2 + [1]_3X + [2]_3 \text{ et } [1]_3X^2 + [2]_3X + [2]_3.$$

Démonstration : Remarquons tout d'abord que pour un premier p donné et un entier d donné, on peut écrire la liste de tous les polynômes de degré d à coefficients dans $\mathbf{F}_p$: ces polynômes sont exactement ceux qui s'écrivent

$$\sum_{r=0}^{d}[a_r]_pX^r$$

avec $1 \leqslant a_d \leqslant p-1$ et $0 \leqslant a_r \leqslant p-1$ pour $0 \leqslant r \leqslant d-1$. En particulier il y a $p^{d+1} - p^d$ tels polynômes. Ainsi les deux polynômes de degré 1 sur $\mathbf{F}_2$ sont

$$[1]_2X, [1]_2X + [1]_2$$

les quatre polynômes de degré 2 sur $\mathbf{F}_2$ sont

$$[1]_2X^2, [1]_2X^2 + [1]_2, [1]_2X^2 + [1]_2X, [1]_2X^2 + [1]_2X + [1]_2,$$

et les huit polynômes de degré 3 sur $\mathbf{F}_2$ sont

$$[1]_2X^3, [1]_2X^3 + [1]_2, [1]_2X^3 + [1]_2X, [1]_2X^3 + [1]_2X + [1]_2, [1]_2X^3 + [1]_2X^2,$$

$$[1]_2X^3 + [1]_2X^2 + [1]_2, [1]_2X^3 + [1]_2X^2 + [1]_2X, [1]_2X^3 + [1]_2X^2 + [1]_2X + [1]_2.$$

On utilise ensuite la caractérisation déjà vue : un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine. On regarde alors pour chacun des polynômes de la liste si $[1]_2$ ou $[0]_2$ est racine. Si ça n'est pas le cas, c'est que le polynôme n'a pas de racine dans $\mathbf{F}_2$ et est donc irréductible. □

Pour clore le chapitre, détaillons le calcul des tables d'addition et de multiplication du corps à quatre éléments $\mathbf{K} \stackrel{\text{déf}}{=} \mathbf{F}_2[X]/\langle [1]_2X^2 + [1]_2X + [1]_2\rangle$. Pour alléger la notation, on écrira 1 et 0 en lieu et place de $[1]_2$ et $[0]_2$. Soit $\pi : \mathbf{F}_2[X] \to \mathbf{K}$ le morphisme quotient et $t = \pi(X)$. Alors $\mathbf{K}$ est un $\mathbf{F}_2$-espace vectoriel de base $\{1, t\}$. L'ensemble des éléments de $\mathbf{K}$ est donc

$$\{a + b\,t, \quad (a, b) \in \mathbf{F}_2^2\} = \{0, 1, t, 1 + t\}.$$

La table d'addition découle aussitôt de (4.4.1).

$+$	0	1	t	$1+t$
0	0	1	t	$1+t$
1	1	0	$1+t$	t
t	t	$1+t$	0	1
$1+t$	$1+t$	t	1	0

Pour la table de multiplication, calculons les coordonnées de t^2 dans la base $\{1, t\}$ en remarquant que $0 = \pi(X^2 + X + 1) = t^2 + t + 1$, soit $t^2 = t + 1$. On en déduit alors le calcul de $t.(1 + t) = t + t^2 = 1 + 2\,t = 1$ et de $(1 + t)^2 = 1 + 2\,t + t^2 = 1 + 1 + t = t$.

$\times$	0	1	t	$1+t$
0	0	0	0	0
1	0	1	t	$1+t$
t	0	t	$1+t$	1
$1+t$	0	$1+t$	1	t

Remarque 4.47 : Comme l'addition et la multiplication sont commutatives, il suffit pour déterminer les tables de remplir la diagonale et la partie située au-dessus. Le reste s'en déduit par symétrie. □

Remarque 4.48 : L'anneau $\mathbf{Z}/4\mathbf{Z}$ possède quatre éléments, mais ça n'est pas un corps car 4 n'est pas premier. L'assertion « $\mathbf{Z}/4\mathbf{Z}$ est un corps à quatre éléments » est certainement l'une des « erreurs standards » sur les corps finis commises par les candidats à l'agrégation. □

4.5 Construction de l'anneau des polynômes en une variable à coefficients dans un corps K

Ce paragraphe consacré à la démonstration des théorèmes 4.2 et 4.4. doit être considéré comme une annexe au chapitre et réservé à une seconde lecture. Le schéma général des démonstrations est donné, et les détails sont laissés au lecteur.

Commençons par la démonstration du théorème 4.2. Soit $\mathbf{K}$ un corps. Soit E l'ensemble des suites à coefficients dans $\mathbf{K}$ qui sont presque nulles (c'est-à-dire que tous leurs termes sauf un nombre fini sont nuls). On vérifie que E est un sous-espace vectoriel du $\mathbf{K}$-espace vectoriel des suites à coefficients dans $\mathbf{K}$, et est donc naturellement muni d'une structure de $\mathbf{K}$-espace vectoriel. Pour $d \in \mathbf{N}$ on note $u(d)$ la suite dont tous les termes sont nuls sauf le terme d'indice d qui vaut 1. On vérifie que $\{u(d)\}_{d\in\mathbf{N}}$ est une base du $\mathbf{K}$-espace vectoriel E.

On définit sur E une loi de composition interne $\times$ en posant

$$(a_n) \times (b_n) = (\sum_{k=0}^{n} a_k\, b_{n-k})$$

Il faut vérifier qu'il s'agit bien d'une loi de composition interne, en d'autres termes que si (a_n) et (b_n) sont des suites presque nulles, alors la suite de terme général $(\sum_{k=0}^{n} a_k\, b_{n-k})$ est encore une suite presque nulle. Il est immédiat que $\times$ est commutative et que pour toute suite presque nulle (a_n) on a $(a_n) \times u(0) = (a_n)$. Il découle de calculs un peu techniques que $\times$ est également associative et distributive par rapport à l'addition. Ainsi $(E, +, \times)$ est un anneau (rappelons que la loi $+$ provient de la structure d'espace vectoriel).

On vérifie par ailleurs par récurrence qu'on a pour tout $d \in \mathbf{N}$ la relation $u(1)^d = u(d)$ et que l'application $\alpha \mapsto \alpha.u(0)$ est un morphisme injectif du corps $\mathbf{K}$ vers l'anneau $(E, +, \times)$

Notant $X = u(1)$, on voit donc que $\{X^d\}_{d\in\mathbf{N}}$ est une base du $\mathbf{K}$-espace vectoriel E.

Pour conclure, il suffit de vérifier que pour $u \in E$ et $\alpha \in \mathbf{K}$, on a l'égalité

$$\alpha.u = (\alpha.u(0)) \times u.$$

Passons à la démonstration du théorème 4.4 (division euclidienne dans $\mathbf{K}[X]$). Il s'agit en fait de la mise en forme de la technique consistant à calculer la division euclidienne « en la posant ».

Lemme 4.49 *Soit B un polynôme non nul. Soit $d \geqslant \deg(B)$ et T un polynôme tel que $\deg(T) \leqslant d$. Il existe alors $\alpha \in \mathbf{K}$ tel que*

$$\deg(T - \alpha.X^{d-\deg(B)}B) \leqslant d-1$$

Démonstration : On prend $\alpha = \frac{a}{b}$ où a est le coefficient de degré d de T et b le coefficient dominant de B. On « tue » ainsi le coefficient de degré d de T. □

Démontrons à présent le théorème 4.4. Soient A et B des éléments de $k[X]$, avec B non nul. Montrons d'abord l'existence du couple (Q, R) de l'énoncé. Si $\deg(A) < \deg(B)$, on peut prendre $Q = 0$ et $R = A$.

Sinon montrons par récurrence finie sur n tel que $0 \leqslant n \leqslant \deg(A) - \deg(B)$ l'assertion $\mathcal{H}_n$ suivante : il existe un polynôme Q_n vérifiant

$$\deg(A - X^{\deg(A)-\deg(B)-n}Q_n.B) \leqslant \deg(A) - n - 1.$$

Pour démontrer $\mathcal{H}_0$, on applique le lemme ci-dessus avec $T = A$, $d = \deg(A)$, et on prend $Q_0 = \alpha$.

Pour passer de $\mathcal{H}_n$ à $\mathcal{H}_{n+1}$ (où $0 \leqslant n \leqslant \deg(A) - \deg(B) - 1$) on applique le lemme ci-dessus avec $T = A - X^{\deg(A)-\deg(B)-n}Q_n.B$ et $d = \deg(A) - n - 1$. On obtient $\alpha \in \mathbf{K}$ vérifiant

$$\deg(A - X^{\deg(A)-\deg(B)-n}Q_nB - \alpha.X^{\deg(A)-\deg(B)-n-1}B) \leqslant \deg(A) - n - 2$$

soit en posant $Q_{n+1} = X.Q_n + \alpha$

$$\deg(A - X^{\deg(A)-\deg(B)-n-1}Q_{n+1}\,B) \leqslant \deg(A) - n - 2.$$

Par récurrence, $\mathcal{H}_{\deg(A)-\deg(B)}$ est vraie. Ceci montre l'existence de la division euclidienne.

L'unicité est laissée à titre d'exercice.

5 Groupes cycliques

Ce court chapitre est consacré à quelques propriétés des groupes cycliques. Son point d'orgue est la démonstration de la propriété que le groupe multiplicatif d'un corps fini est cyclique.

Rappelons tout d'abord quelques propriétés importantes vues dans le premier chapitre. Soit G un groupe, $g \in G$ et H le sous-groupe de G engendré par g. Alors g est d'ordre fini si et seulement si H est fini, et dans ce cas l'ordre de H coïncide avec l'ordre de g. En particulier un groupe fini G d'ordre N est cyclique (c'est-à-dire monogène et engendré par un élément d'ordre fini) si et seulement si G possède un élément d'ordre N, et alors tout élément de G d'ordre N est un générateur de G.

Théorème 5.1 *Soit $N \geqslant 1$. Alors tout groupe cyclique d'ordre N est isomorphe à $\mathbf{Z}/N\mathbf{Z}$.*

Démonstration : Soit $g \in G$ un élément d'ordre N. On considère l'application

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & G \\ k & \longmapsto & g^k \end{array} .$$

Les règles de calcul des puissances montrent que c'est un morphisme de groupes. Comme g engendre G, ce morphisme est surjectif. D'après la proposition 2.44, le noyau de ce morphisme est $N\,\mathbf{Z}$. D'après la dernière assertion du théorème 3.61, ce morphisme induit un isomorphisme de $\mathbf{Z}/N\,\mathbf{Z}$ sur G. □

Lemme 5.2 *Soit G un groupe et g un élément d'ordre fini m. Alors pour tout entier relatif k, g^k est d'ordre fini, et cet ordre est $\frac{m}{\mathrm{pgcd}(m,k)}$.*

Démonstration : Pour $d \in \mathbf{Z}$, on a

$$(g^k)^d = e \Leftrightarrow g^{k\,d} = e \Leftrightarrow m \text{ divise } k\,d \Leftrightarrow \frac{m}{\mathrm{pgcd}(m,k)} \text{ divise } d$$

d'où le résultat. □

Corollaire 5.3 *Un groupe cyclique G d'ordre N a exactement $\varphi(N)$ générateurs.*

Démonstration : Soit g un élément d'ordre N. Alors

$$\begin{array}{ccc} \{0, \ldots, N-1\} & \longrightarrow & G \\ k & \longmapsto & g^k \end{array}$$

est bijective, et pour $0 \leqslant k \leqslant N-1$, g^k est générateur si et seulement si g^k est d'ordre N si et seulement si $\frac{N}{\mathrm{pgcd}(k,N)} = N$ si et seulement si k et N sont premiers entre eux. □
Exemple 5.4 : Tout groupe fini d'ordre premier p est cyclique et possède $p-1$ générateurs.
□

Notation 5.5 *Soit G un groupe fini.*
Pour $d \geqslant 1$, on note $\Delta_G(d) = \{x \in G, \quad x^d = e\}$ l'ensemble des éléments de G dont l'ordre divise d, $\Omega_G(d)$ l'ensemble des éléments de G dont l'ordre est exactement d et $\omega_G(d)$ le cardinal de $\Omega_G(d)$.

Remarque 5.6 : D'après le théorème de Lagrange, si d ne divise pas l'ordre de G, $\Omega_G(d)$ est vide. Par ailleurs les ensembles $\{\Omega_G(d)\}_{d \geqslant 1}$ forment visiblement une partition de G.
On a donc la relation $\sum_{d|\mathrm{card}(G)} \omega_G(d) = \mathrm{card}(G)$. □

Proposition 5.7 *Soit G un groupe cyclique d'ordre N.*
Si d divise N, $\Delta_G(d)$ est un sous-groupe de G ; il est cyclique d'ordre d.

Démonstration : Soit g un générateur de G. Pour $k \in \mathbf{Z}$ et $x = g^k$, on a $x^d = e$ si et seulement si N divise $k\,d$ si et seulement si $\frac{N}{d}$ divise k. Ainsi $\Delta_G(d)$ est l'ensemble des éléments de G qui sont des puissances de $g^{\frac{N}{d}}$, en d'autres termes c'est le sous-groupe de G engendré par $g^{\frac{N}{d}}$. Il est donc d'ordre $\frac{N}{\mathrm{pgcd}(N, \frac{N}{d})} = N/(N/d) = d$. □

Corollaire 5.8 *Si G est un groupe cyclique d'ordre N, pour tout d diviseur de N, on a $\omega_G(d) = \varphi(d)$.*

En particulier on a $\sum_{d|N} \varphi(d) = N$.

Démonstration : On sait que $\Delta_G(d)$ est un sous-groupe cyclique d'ordre d, Or tout élément d'ordre d est dans $\Delta_G(d)$, donc est un générateur de G_d. Réciproquement tout générateur de G_d est un élément d'ordre d de G.

Ainsi l'ensemble des éléments d'ordre d de G est l'ensemble des générateurs du groupe cyclique d'ordre d $\Delta_G(d)$, d'où le résultat d'après le corollaire 5.3. □

Théorème 5.9 (Un critère de cyclicité) *Soit G un groupe fini d'ordre N. Sont équivalents :*

1. *G est cyclique ;*
2. *$\forall d|N$, $card(\Delta_G(d)) \leqslant d$;*
3. *$\forall d|N$, $\omega_G(d) \leqslant \varphi(d)$.*

Démonstration : Si G est cyclique d'ordre N et d divise N, on a déjà vu l'égalité $\mathrm{card}(\Delta_G(d)) = d$.

Supposons que pour tout diviseur d de N, on a $\mathrm{card}(\Delta_G(d)) = d$. Montrons qu'on a $\omega_G(d) \leqslant \varphi(d)$. C'est évidemment vrai si $\Omega_G(d)$ est vide. Sinon, on prend un élément d'ordre d et le groupe H qu'il engendre. H est de cardinal d et est contenu dans $\Delta_G(d)$ qui est de cardinal au plus d, donc on a $H = \Delta_G(d)$. En particulier $\Delta_G(d)$ est un sous-groupe cyclique d'ordre d, et les éléments d'ordre d de G sont exactement les générateurs de $\Delta_G(d)$. Ainsi $\omega_G(d) = \varphi(d)$.

Supposons que pour tout diviseur d de N, on a $\omega_G(d) \leqslant \varphi(d)$. Mais on a par ailleurs

$$\sum_{d|N} \omega_G(d) = N = \sum_{d|N} \varphi(d).$$

Ainsi aucune des inégalités $\omega_G(d) \leqslant \varphi(d)$ ne peut être stricte. En particulier on a $\Omega_G(N) = \varphi(N) \neq 0$ et G possède un élément d'ordre N. □

Corollaire 5.10 *Le groupe multiplicatif d'un corps fini $\mathbf{K}$ est cyclique.*

Démonstration : En effet dans ce cas $\Delta_G(d)$ est l'ensemble des racines du polynôme $X^d - 1$. D'après le corollaire 4.9, cet ensemble est de cardinal au plus d. □

Exemple 5.11 : Pour tout nombre premier p, $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique de cardinal $p-1$. Noter que la démonstration ci-dessus ne fournit aucun moyen effectif efficace pour déterminer un générateur de ce groupe. □

Exercice 26

Le théorème montre que le résultat suivant est vrai :
« Les assertions

1. G est cyclique
2. $\forall d|N$, $\mathrm{card}(\Delta_G(d)) = d$
3. $\forall d|N$, $\omega_G(d) = \varphi(d)$

sont équivalentes. »
Il en est de même du résultat
« Les assertions

1. G est cyclique
2. $\forall d|N$, $\mathrm{card}(\Delta_G(d)) \leqslant d$
3. $\forall d|N$, $\omega_G(d) = \varphi(d)$

sont équivalentes ».
Voyez vous pourquoi le théorème n'a pas été énoncé directement sous l'une des deux formes précédentes ?

Citons pour information le théorème suivant, qui montre l'importance des groupes cycliques dans la classification des groupes finis commutatifs.

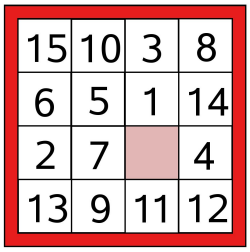
Théorème 5.12 *Tout groupe fini commutatif est isomorphe à un produit de groupes cycliques.*

Ce théorème est admis et nous ne n'utiliserons pas dans ce cours.

6 Le groupe des permutations d'un ensemble fini

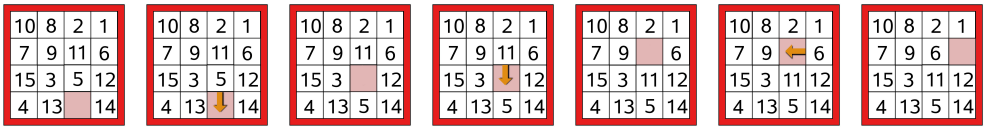
6.1 Une motivation ludique : résolution du taquin

Le *jeu de taquin* est un célèbre « casse-tête » se composant d'un damier de dimension 4x4 sur lequel se trouvent 15 petites plaques carrées numérotée de 1 à 15, la seizième case restant vide. Voici un exemple de configuration possible.



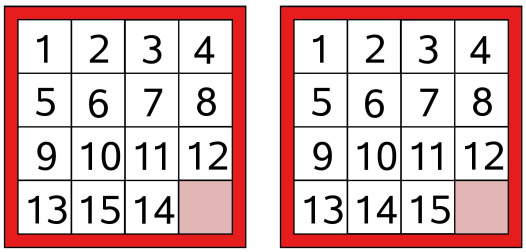
La case vide sert à changer la configuration des plaques, en poussant l'une des plaques adjacentes dessus ; cette plaque laisse à son tour une case vide à son ancien emplacement et on peut itérer le processus.

Voici un exemple d'une succession de trois tels modifications.



De telles modifications de la configuration sont appelées *modifications élémentaires*.

Le problème posé est de passer, à l'aide d'une succession de modifications élémentaires, d'une position où les plaques sont rangées dans l'ordre de leur numérotation, à l'exception des plaques 14 et 15 qui sont échangées (position de gauche ci-dessous), à une position où les plaques sont rangées dans l'ordre (position de droite ci-dessous).



L'étude du groupe des permutations d'un ensemble fini va nous permettre de montrer que ce problème n'est pas résoluble : il n'existe aucune suite de mouvements tels que décrits ci-dessus qui permet de passer de la position de gauche à la position de droite.

6.2 Définition, quelques remarques

Pour n entier strictement positif, on note $\mathbf{N}_n$ l'ensemble $\{1, \ldots, n\}$.

Définition 6.1 *Pour n entier strictement positif*[23]*, on note $\mathfrak{S}_n = \mathfrak{S}_{\mathbf{N}_n}$ le groupe des permutations de l'ensemble $\mathbf{N}_n$. On l'appelle le* groupe symétrique d'indice n.

23. La stricte positivité n'est là que pour des raisons psychologiques ; on peut tout aussi bien étudier le groupe des permutations de l'ensemble vide, même si l'étude ne sera pas très longue…

Remarque 6.2 : La loi de groupe est bien sûr la composition ; elle sera en général notée multiplicativement. □

Remarque 6.3 : Si E est un ensemble fini de cardinal n, alors les groupes $\mathfrak{S}_E$ et $\mathfrak{S}_n$ sont isomorphes (*cf.* l'exercice 13 du TD 4). Ainsi, pour étudier $\mathfrak{S}_E$ pour E ensemble fini non vide quelconque, il suffit d'étudier $\mathfrak{S}_n$ pour tout entier strictement positif n. □

Remarque 6.4 : Vous avez vu en AR1 que pour tout n entier strictement positif, $\mathfrak{S}_n$ est fini, de cardinal $n!$. □

Remarque 6.5 : Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}_G$ (théorème 2.23) donc si G est fini et n est l'ordre de G, G s'identifie à un sous-groupe de $\mathfrak{S}_n$. Ainsi, en un sens, la connaissance de la structure de groupe de tous les groupes $\mathfrak{S}_n$ pour $n \geqslant 1$ contient la connaissance de tous les groupes finis. Ceci montre en fait que l'étude fine des groupes $\mathfrak{S}_n$ est particulièrement délicate. Nous ne ferons ici que l'effleurer ! □

Notation 6.6 *Pour travailler de manière concrète avec les éléments de $\mathfrak{S}_n$, il est préférable de fixer une notation. Un élément σ de $\mathfrak{S}_n$ est noté comme un tableau à 2 lignes et n colonnes. La première ligne contient les entiers de 1 à n rangés dans l'ordre croissant. Sous l'entier i figure la valeur de $\sigma(i)$. Par exemple la notation*

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

représente l'élément σ de $\mathfrak{S}_6$ qui envoie 1 sur 2, 2 sur 4, etc...

ATTENTION ! ! *Une autre notation va être introduite pour des éléments distingués de $\mathfrak{S}_n$, appelés cycles. Il convient tout particulièrement de ne pas confondre ces deux notations ! !*

Exemple 6.7 : Avec la notation ci-dessus, on a $\mathfrak{S}_1 = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$, $\mathfrak{S}_2 = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$, et

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

□

Exercice 27

Dresser la table du groupe $\mathfrak{S}_3$ et montrer que $\mathfrak{S}_3$ n'est pas commutatif.

6.3 Cycles, décomposition en cycles à supports disjoints

Pour comprendre un peu mieux un élément général de $\mathfrak{S}_n$, plus précisément pour comprendre un peu mieux la « façon dont il agit » sur $\mathbf{N}_n$, on va s'intéresser à une certaine famille d'éléments de $\mathfrak{S}_n$ qui « agissent » de manière particulièrement simple : les cycles.

Définition 6.8 *Soit $n \geqslant 1$. Un* cycle *de $\mathfrak{S}_n$ est un élément σ de $\mathfrak{S}_n$ vérifiant la propriété suivante : il existe une partie $\mathcal{P}$ de $\mathbf{N}_n$ de cardinal $r \geqslant 2$ et une numérotation $\{d_1, \ldots, d_r\}$ de $\mathcal{P}$ telle qu'on ait*

$$\forall i \in \{1, \ldots, r-1\}, \quad \sigma(d_i) = d_{i+1}$$

$$\sigma(d_r) = d_1$$

$$\forall d \in \mathbf{N}_n \setminus \mathcal{P}, \quad \sigma(d) = d$$

Le support *d'un cycle σ est l'ensemble $\{d \in \mathbf{N}_n, \quad \sigma(d) \neq d\}$.*

Remarque 6.9 : En dépit de cette définition sans doute un peu technique, les cycles sont vraiment en un sens les permutations les plus simples qu'on puisse imaginer, et les exemples plus que la définition elle-même contribueront, on l'espère, à l'illustrer.

Il est sans doute plus facile de comprendre la simplicité de la notion de cycle si l'on maîtrise un peu le langage des actions de groupes. En effet, un cycle n'est rien d'autres qu'une permutation ayant une seule orbite non triviale (une orbite est triviale si elle est réduite à un élément). □

Remarque 6.10 : La définition d'un cycle demande l'existence d'une certaine partie $\mathcal{P}$ vérifiant certaines conditions. A priori une telle partie n'est pas nécessairement unique. Mais c'est bien le cas : une telle partie coïncide nécessairement avec le support de σ, qui lui est uniquement déterminé par le cycle σ. La numérotation du support, elle, n'est par contre jamais unique. □

Remarque 6.11 : Si σ est un cycle de support $\mathcal{P}$, $\mathcal{P}$ est stable par σ, plus précisément on a $\sigma(\mathcal{P}) = \mathcal{P}$. □

Définition 6.12 *La longueur d'un cycle est le cardinal de son support. Un cycle de longueur r est aussi appelée un r-cycle. Les 2-cycles sont aussi appelés transpositions.*

Exemple 6.13 : Noter que l'identité n'est jamais un cycle.

L'élément de $\mathfrak{S}_2$ distinct de l'identité, à savoir $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ est un cycle, et c'est une transposition.

Tous les éléments de $\mathfrak{S}_3$ distincts de l'identité sont des cycles.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

sont des transpositions,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

sont des 3-cycles. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ n'est pas un cycle de $\mathfrak{S}_4$. Si c'en était un, son support serait $\{1,2,3,4\}$, donc il serait de longueur 4 ; en particulier il serait d'ordre 4 (*cf.* ci-dessous) ; mais son carré est égal à l'identité. □

Exercice 28

Déterminer tous les cycles de $\mathfrak{S}_4$ (il y a six transpositions, huit 3-cycles, et six 4-cycles).

Notation 6.14 *Soit $n \geqslant 1$, $r \geqslant 2$ et $\sigma \in \mathfrak{S}_n$ un r-cycle de support $\mathcal{P}$. Soit $\mathcal{P} = \{d_1, \ldots, d_r\}$ une numérotation de $\mathcal{P}$ vérifiant les conditions de la définition 6.8. On* note *alors*

$$\sigma = (d_1, \ldots, d_r).$$

Exemple 6.15 : Avec la notation ci-dessus, on a

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1,2) = (2,1)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2) = (2,1), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3) = (3,1)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3) = (2,3,1) = (3,1,2), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2) = (3,2,1) = (2,1,3).$$

□

Remarque 6.16 : Il est bon de garder en tête deux particularités importantes de cette notation, qui sont clairement illustrées par les exemples ci-dessus.

Tout d'abord, plusieurs notations valent pour un même cycle. En fait, il y a autant de notations disponibles pour un cycle donné qu'il y a de choix pour l'élément du support que l'on va écrire en premier ; ainsi pour un r-cycle il y a r notations disponibles.

Ensuite, la notation est a priori ambigue. On voit par exemple que $(1,2)$ peut désigner soit un élément de $\mathfrak{S}_2$, soit un élément de $\mathfrak{S}_3$ (en fait $(1,2)$ pourrait aussi désigner un élément de $\mathfrak{S}_n$ pour n'importe quel $n \geqslant 2$). De manière un peu surprenante au premier abord, cette ambiguité n'est que très rarement gênante dans la pratique. Pour une explication théorique de ce constat, voir l'exercice 14 du TD 4. □

Théorème 6.17 *Soit $n \geqslant 1$ et $r \geqslant 2$. Tout r-cycle de $\mathfrak{S}_n$ est d'ordre r.*

Pour la démonstration, on se reportera à l'exercice 10 du TD 4.

Remarque 6.18 : L'inverse d'un r-cycle est un r-cycle de même support. Plus précisément on a la formule $(d_1, \ldots, d_r)^{-1} = (d_r, d_{r-1}, \ldots, d_2, d_1)$. □

Proposition 6.19 *Deux cycles dont les supports sont disjoints commutent.*

Démonstration : Soit σ et τ deux tels cycles. Soit $\mathcal{P}$ le support de σ et $\mathcal{Q}$ celui de τ. Par hypothèse $\mathcal{P} \cap \mathcal{Q} = \varnothing$.

Il s'agit de montrer que $\sigma\tau = \tau\sigma$, en d'autres termes il s'agit de montrer que pour tout $d \in \mathbf{N}_n$ on a

$$\sigma(\tau(d)) = \tau(\sigma(d)). \tag{6.3.1}$$

Distinguons trois cas.

1. *Le cas où $d \notin \mathcal{P}$ et $d \notin \mathcal{Q}$.* Alors, par définition du support, $\sigma(d) = \tau(d) = d$. On vérifie alors facilement que (6.3.1) est vraie.
2. *Le cas où $d \in \mathcal{P}$.* Alors par hypothèse $d \notin \mathcal{Q}$ et $\tau(d) = d$ et le membre de gauche de (6.3.1) vaut $\sigma(d)$. Par ailleurs, d'après la remarque 6.11, on a $\sigma(d) \in \mathcal{P}$. Donc par hypothèse $\sigma(d) \notin \mathcal{Q}$, d'où par définition du support $\tau(\sigma(d)) = \sigma(d)$. Ainsi (6.3.1) est vérifiée.
3. *Le cas où $d \in \mathcal{Q}$.* Les couples de données $(\sigma, \mathcal{P})$ et $(\tau, \mathcal{Q})$ jouant des rôles symétriques dans l'énoncé à démontrer, ce cas découle du cas précédent.

□

Remarque 6.20 : Soit $r \geqslant 1$ et $\{c_i\}_{1 \leqslant i \leqslant r}$ des cycles à supports 2 à 2 disjoints. Soit $\sigma = \prod_{i=1}^{r} c_i$. Alors un élément de $\mathbf{N}_n$ est point fixe [24] de σ si et seulement s'il n'est pas dans le support de l'un des c_i. □

Théorème 6.21 *Soit $n \geqslant 1$. Toute permutation de $\mathfrak{S}_n$ s'écrit comme produit de cycles dont les supports sont deux à deux disjoints, et cette décomposition est unique à l'ordre des cycles près.*

En d'autres termes, pour tout élément σ de $\mathfrak{S}_n$, il existe un entier $r \geqslant 0$ et des cycles $\{c_i\}_{1 \leqslant i \leqslant r}$ tels que pour tout couple $(i, j) \in \{1, \ldots, r\}$ avec $i \neq j$, les supports de c_i et c_j sont disjoints et on a [25]

$$\sigma = \prod_{i=1}^{r} c_i \ ;$$

et s'il existe $s \geqslant 0$ et des cycles $\{c'_i\}_{1 \leqslant i \leqslant s}$ tels que pour tout couple $(i, j) \in \{1, \ldots, s\}$ avec $i \neq j$, les supports de c'_i et c'_j sont disjoints et on a

$$\sigma = \prod_{i=1}^{s} c'_i,$$

alors on a $r = s$ et quitte à renuméroter les c'_i, on a $c_i = c'_i$ pour tout $i \in \{1, \ldots, r\}$.

24. Un *point fixe* d'un élément σ de $\mathfrak{S}_n$ est un élément d de $\mathbf{N}_n$ vérifiant $\sigma(d) = d$.

25. Si $r = 0$, l'ensemble $\{c_i\}_{1 \leqslant i \leqslant r}$ est vide et le produit $\prod_{i=1}^{r} c_i$ vaut $\mathrm{Id}_{\mathbf{N}_n}$; bien entendu cela ne peut se produire que si $\sigma = \mathrm{Id}_{\mathbf{N}_n}$.

Démonstration : Montrons l'existence par récurrence descendante sur le nombre de points fixes de σ. Nous travaillerons avec l'hypothèse de récurrence $\mathcal{H}_r$ (pour $0 \leqslant r \leqslant n$) donnée par « Tout élément σ de $\mathbf{N}_n$ ayant au moins $n-r$ points fixes s'écrit comme un produit de cycles à supports deux à deux disjoints ».

$\mathcal{H}_0$ est vraie. En effet le seul éléments de $\mathfrak{S}_n$ ayant n points fixe est l'identité, pour laquelle le résultat d'existence est clair.

Supposons $\mathcal{H}_r$ vérifiée pour $0 \leqslant r \leqslant n-1$ et montrons que $\mathcal{H}_{r+1}$ l'est encore.

Soit $\sigma \in \mathfrak{S}_n$ ayant au moins $n-r-1$ points fixes. Si σ a en fait au moins $n-r$ points fixes, on peut appliquer $\mathcal{H}_r$ et σ s'écrit comme un produit de cycles à supports deux à deux disjoints. Regardons à présent le cas où σ a exactement $n-r-1$ points fixes. Comme $n-r-1 < n$, il existe au moins un élément d de $\mathbf{N}_n$ qui n'est pas un point fixe de d. L'application $\mathbf{N} \to \mathbf{N}_n$ qui à k associe $\sigma^k(d)$ n'est pas injective. En effet un ensemble infini ne peut pas s'injecter dans un ensemble fini. Il existe donc $k \in \mathbf{N}$ et $l > 0$ tel que $\sigma^{k+l}(d) = \sigma^k(d)$. En prenant l'image de cette égalité par σ^{-k}, on obtient $\sigma^l(d) = d$.

Ainsi on peut considérer ℓ minimal parmi les $l > 0$ vérifiant $\sigma^l(d) = d$. Nécessairement on a $\ell \geqslant 2$ car d n'est pas un point fixe de σ. Soit c le ℓ-cycle donné par

$$c = (d, \sigma(d), \ldots, \sigma^{\ell-1}(d)).$$

Soit $\mathcal{P}$ le support de c. Notons que pour tout $e \in \mathcal{P}$, on a $c(e) = \sigma(e)$. Par ailleurs on a $\sigma(\mathcal{P}) = \mathcal{P}$.

Montrons que $c^{-1}\sigma$ a au moins $n-r+1$ points fixes.

Si $e \notin \mathcal{P}$, comme $\sigma(\mathcal{P}) = \mathcal{P}$, nécessairement on a $\sigma(e) \notin \mathcal{P}$. Ainsi $c(\sigma(e)) = \sigma(e)$ d'où $c^{-1}\sigma(e) = \sigma(e)$

Pour $e \notin \mathcal{P}$, on a $c^{-1}\sigma(e) = c^{-1}(c(e)) = e$.

Ainsi l'ensemble des points fixes de $c^{-1}\sigma$ est la réunion de $\mathcal{P}$ et de l'ensemble des éléments de $\mathbf{N}_n \setminus \mathcal{P}$ qui sont points fixes de σ. En particulier cet ensemble contient d (qui n'est pas un point fixe de σ) et l'ensemble des points fixes de σ. Ainsi $c^{-1}\sigma$ a au moins un point fixe de plus que σ. D'après $\mathcal{H}_r$, soit $c^{-1}\sigma = \mathrm{Id}_{\mathbf{N}_n}$, soit il existe $s \geqslant 1$ et des cycles $\{c_i\}_{1 \leqslant i \leqslant s}$ à supports 2 à 2 disjoints tels que

$$c^{-1}\sigma = \prod_{i=1}^{s} c_i.$$

Si $c^{-1}\sigma = \mathrm{Id}_{\mathbf{N}_n}$, on a $\sigma = c$ et donc la décomposition voulue pour σ.

Dans le deuxième cas, pour tout $i \in \{1, \ldots, s\}$, le support de c_i est disjoint du support de c ; en effet tout élément du support de c est un point fixe de $c^{-1}\sigma$, donc n'est pas dans le support de c_i d'après la remarque 6.20 ; d'où la conclusion voulue.

L'unicité sera vue en exercice (exercice 10 du TD 4). □

Remarque 6.22 : La pratique effective de la décomposition en produit de cycles à supports disjoints d'un élément de $\mathfrak{S}_n$ est donnée par la démonstration ci-dessus On prend d qui n'est pas un point fixe, on calcule $\sigma(d)$, $\sigma^2(d)$,... jusqu'à ce qu'on trouve ℓ tel que $\sigma^\ell(d) = d$

Le ℓ-cycle $(d, \sigma(d), \ldots, \sigma^{\ell-1}(d))$ est alors l'un des cycles intervenant dans la décomposition de σ. On recommence avec un d qui n'est pas un point fixe et qui n'est pas dans le support des cycles déjà calculés. S'il n'en existe pas, on a terminé. □

Exemple 6.23 : Soit à décomposer en produit de cycles à supports disjoints

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 5 & 8 & 10 & 7 & 9 & 2 & 4 & 6 & 3 \end{pmatrix}$$

L'unique point fixe de σ est 1. Prenons un point non fixe de σ, par exemple 2 comme premier point non fixe. On a $\sigma(2) = 5$, $\sigma^2(2) = \sigma(5) = 7$ et $\sigma^3(2) = \sigma(7) = 2$. Ainsi $(2, 5, 7)$ apparaît dans la décomposition. Choisissons à présent un élément de $\mathbf{N}_{10} \setminus \{1, 2, 5, 7\}$, par exemple 8. On a $\sigma(8) = 4$, $\sigma^2(8) = 10$, $\sigma^3(8) = 3$, $\sigma^4(8) = 8$. Ainsi $(8, 4, 10, 3)$ apparaît dans la décomposition.

On poursuit de la sorte pour obtenir finalement la décomposition

$$\sigma = (2, 5, 7)(8, 4, 10, 3)(6, 9).$$

□

Exercice 29

Décomposer

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 5 & 6 & 3 & 2 & 4 & 7 & 8 & 1 & 10 \end{pmatrix}$$

en produit de cycles à support disjoints.

Corollaire 6.24 *Pour $n \geqslant 1$, les cycles engendrent $\mathfrak{S}_n$.*

Démonstration : Formellement, l'énoncé doit se lire : le sous-groupe de $\mathfrak{S}_n$ engendré par l'ensemble des cycles est $\mathfrak{S}_n$ lui-même. Et en effet, comme c'est un sous-groupe et qu'il contient les cycles, il contient tous les produits de cycles (en toute rigueur, il y a une récurrence à rédiger ici). D'après le théorème précédent, il contient donc $\mathfrak{S}_n$, donc il lui est égal. □

Corollaire 6.25 *Pour $n \geqslant 1$, les transpositions engendrent $\mathfrak{S}_n$.*

Démonstration : D'après le corollaire précédent, il suffit de montrer que tout cycle est un produit de transpositions. Mais on a par exemple, pour $r \geqslant 1$ et $d_1, \ldots, d_r$ des entiers 2 à 2 distincts la formule

$$(d_1, \ldots, d_r) = (d_1, d_r)(d_1, d_{r-1}) \ldots (d_1, d_3)(d_1, d_2).$$

Sa vérification est un exercice de TD. □

Une autre application de la décomposition en support à cycles disjoints sera vue en TD : le calcul de l'ordre d'une permutation en fonction de la longueur des cycles intervenant dans la décomposition. Une application supplémentaire est donnée dans la partie suivante : la définition de la signature d'une permutation

6.4 La signature et le groupe alterné

Il existe de nombreuses définitions possibles de la signature d'une permutation. Nous utilisons ici celle basée sur la décomposition en cycles à supports disjoints.

Définition 6.26 *Soit $\sigma \in \mathfrak{S}_n$. Soit $\sigma = \prod_{i=1}^{s} c_i$ la décomposition de σ en produit de cycles à supports disjoints, Pour $1 \leqslant i \leqslant s$, soit r_i la longueur de c_i. Alors on pose*[26]

$$\varepsilon(\sigma) \stackrel{déf}{=} (-1)^{\sum_{i=1}^{s}(r_i+1)}.$$

Cette quantité est appelée la signature *de σ.*

Remarque 6.27 : Le fait que ε soit bien définie est dû à l'unicité de la décomposition en produit de cycles à supports disjoints. □

Remarque 6.28 : Pour $r \geqslant 2$, si σ est un r-cycle, on a $\varepsilon(\sigma) = (-1)^{1+r}$. En d'autre termes la signature d'un cycle est 1 si sa longueur est impaire et -1 si sa longueur est paire. En particulier une transposition est de signature -1. Ainsi si $n \geqslant 2$, $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est une application surjective. □

Théorème 6.29 *Soit $n \geqslant 1$. Alors l'application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un morphisme de groupes.*

Démonstration : On a admet la proposition suivante, démontrée dans l'exercice 11 du TD 4 : pour toute permutation σ et toute transposition τ, on a $\varepsilon(\sigma.\tau) = -\varepsilon(\sigma)$. En particulier, pour tout entier $r \geqslant 1$ et toute famille $\{\tau_i\}_{1 \leqslant i \leqslant r}$ de transpositions on a

$$\varepsilon(\tau_1 \dots \tau_r) = (-1)^r$$

(faire une récurrence...)

Si σ, σ' sont des éléments de $\mathfrak{S}_n$, d'après le corollaire 6.25, σ' s'écrit $\tau_1 \dots \tau_r$ pour $r \geqslant 1$ et $\{\tau_i\}_{1 \leqslant i \leqslant r}$ une famille de transpositions, et on a

$$\varepsilon(\sigma\, \sigma') = \varepsilon(\sigma\, \tau_1 \dots \tau_r) = \varepsilon(\sigma).(-1)^r$$

(là encore, récurrence...) et d'après le calcul ci-dessus on a donc

$$\varepsilon(\sigma\, \sigma') = \varepsilon(\sigma\, \tau_1 \dots \tau_r) = \varepsilon(\sigma)\varepsilon(\sigma').$$

□

Remarque 6.30 : Si σ est une permutation, il existe une infinité de décomposition possible de σ comme produit de transpositions. Cependant le résultat précédent montre que la parité du nombre de transpositions intervenant dans la décomposition est indépendante de la décomposition choisie. □

26. Si $s = 0$, c'est-à-dire si σ est l'identité, $\sum_{i=1}^{s}$ est la somme indexée par l'ensemble vide, qui vaut 0, et $\varepsilon(\mathrm{Id}) = 1$.

Définition 6.31 *Pour $n \geqslant 1$, le* groupe alterné d'indice n *est le noyau de $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$. On le note $\mathfrak{A}_n$.*

Remarque 6.32 : D'après la proposition 2.30, $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$, ce qui justifie la dénomination.

Les éléments de $\mathfrak{A}_n$ sont exactement les permutations qui s'écrivent comme le produit d'un nombre pair de transpositions. □

Théorème 6.33 *Pour $n \geqslant 1$, $\mathfrak{A}_n$ engendré par les 3-cycles.*

Démonstration : [esquisse] Elle est basée sur la remarque précédente et les identités suivantes : si $\#\{i, j, k\} = 3$, on a

$$(i, j)(j, k) = (i, j, k)$$

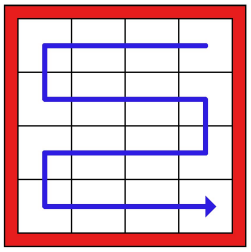
et si $\#\{i, j, k, l\} = 4$

$$(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l).$$

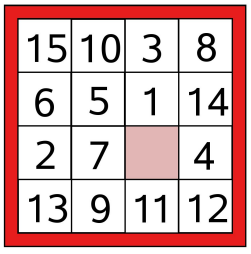
□

6.5 Application à la résolution du problème du taquin

À toute configuration du taquin, on associe l'élément de $\mathfrak{S}_{15}$ obtenu en lisant les numéros des plaques dans l'ordre indiqué par la flèche ci-dessous (et en oubliant la case vide).



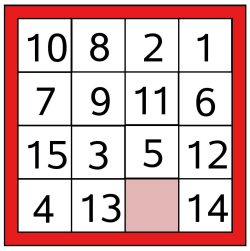
Ainsi, à la configuration



est associée la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 8 & 3 & 10 & 15 & 6 & 5 & 1 & 14 & 4 & 7 & 2 & 13 & 9 & 11 & 12 \end{pmatrix}$$

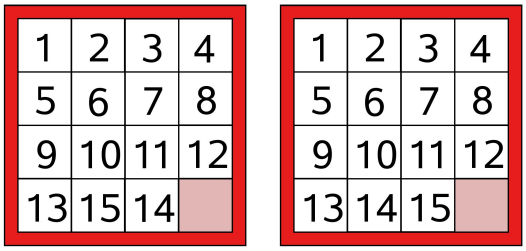
et à la configuration



la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 8 & 10 & 7 & 9 & 11 & 6 & 12 & 5 & 3 & 15 & 4 & 13 & 14. \end{pmatrix}$$

Si on note $\mathcal{T}$ l'ensemble des configurations du taquin, on définit ainsi une application $\Sigma : \mathcal{T} \to \mathfrak{S}_{15}$. Si $\mathscr{C}_1$ (respectivement $\mathscr{C}_2$) désigne la configuration de gauche (respectivement de droite) ci-dessous



on vérifie facilement que $\Sigma(\mathscr{C}_1)\Sigma(\mathscr{C}_2)^{-1}$ est la transposition $(14, 15)$ qui est de signature -1.

Le résultat suivant montre alors qu'il n'est pas possible de passer de $\mathscr{C}_1$ à $\mathscr{C}_2$ par une succession de modifications élémentaires, en d'autres termes résout le problème du taquin.

Théorème 6.34 *Soit $\mathscr{C}_1$ et $\mathscr{C}_2$ deux configurations du taquin. Si on peut passer de $\mathscr{C}_1$ à $\mathscr{C}_2$ à l'aide d'une succession de modifications élémentaires, alors $\Sigma(\mathscr{C}_1)\Sigma(\mathscr{C}_2)^{-1}$ est de signature 1 (en d'autres termes, est un élément du groupe alterné $\mathfrak{A}_{15}$).*

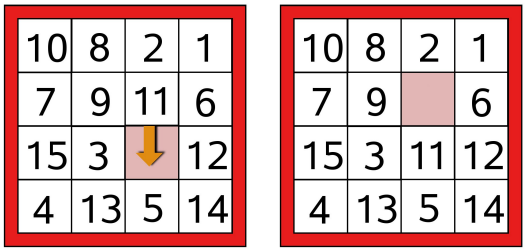
Remarque 6.35 : La réciproque est vraie, mais inutile pour la résolution du problème du taquin. Elle est laissée en exercice au lecteur intéressé. □

Démonstration : Il suffit de démontrer que si on passe de $\mathscr{C}_1$ à $\mathscr{C}_2$ par une modification élémentaire, alors $\Sigma(\mathscr{C}_1)\Sigma(\mathscr{C}_2)^{-1}$ est de signature 1. C'est évident si cette modification élémentaire consiste à glisser une plaque horizontalement ; en effet, dans ce cas, vu la définition de Σ, on a $\Sigma(\mathscr{C}_1) = \Sigma(\mathscr{C}_2)$. Toujours vu la définition de Σ, on a également $\Sigma(\mathscr{C}_1) = \Sigma(\mathscr{C}_2)$ si la modification consiste à glisser une plaque :

1. de la case supérieure gauche vers la case située immédiatemment en dessous, ou inversement ;
2. de la case inférieure gauche vers la case située immédiatemment en dessus, ou inversement ;
3. de l'une des deux cases médianes de la colonne de droite vers l'autre ;

Il reste à examiner les autres modifications élémentaires consistant à glisser une plaque verticalement. On vérifie que dans ce cas, $\Sigma(\mathscr{C}_1)\Sigma(\mathscr{C}_2)^{-1}$ est un cycle de longueur 3, 5 ou 7, en particulier de signature 1.

Par exemple, pour la modification suivante



on a que $\Sigma(\mathscr{C}_1)\Sigma(\mathscr{C}_2)^{-1}$ est le 5-cycle $(11, 9, 7, 15, 3)$. □

7 L'anneau des entiers de Gauss

7.1 Motivation

Cette partie peut être sautée en première lecture.

Lorsque l'on souhaite démontrer des résultats portant sur l'arithmétique de $\mathbf{Z}$, il peut s'avérer extrêmement utile de travailler sur un anneau plus gros. Une illustration frappante de ce procédé est la tentative de démonstration du « dernier théorème de Fermat » proposée en 1847 par le mathématicien Gabriel Lamé. Rappelons qu'il s'agit de l'énoncé suivant : pour tout entier $n \geqslant 3$, l'équation

$$x^n + y^n = z^n$$

n'a pas de solutions $(x, y, z) \in \mathbf{Z}^3$ non triviales (une solution (x, y, z) est dite triviale si $x\,y\,z = 0$, c'est-à-dire l'une des trois inconnues est nulle). L'approche proposée par Lamé

était erronée[27], mais l'erreur commise était assez subtile, tout à fait « digne » du grand mathématicien qu'était Lamé et au final très intéressante[28]. Avant d'expliquer les grandes lignes de l'idée de Lamé, rappelons l'énoncé suivant :

Proposition 7.1 *Soit $n \geqslant 2$ un entier, b et c des entiers relatifs premiers entre eux et $a = bc$. On suppose que $|a|$ est une puissance n-ème (c'est-à-dire s'écrit α^n où α est un entier relatif). Alors $|b|$ et $|c|$ sont aussi des puissances n-ème.*

La proposition se généralise à un produit quelconque de facteurs supposés premiers entre eux 2 à 2. Cette proposition ainsi que sa généralisation se démontrent à partir du théorème de décomposition en facteurs premiers. L'un des aspects les plus cruciaux de la décomposition que l'on utilise son *unicité*[29]. Cette proposition se généralise à tout anneau intègre admettant une théorème de décomposition en irréductibles semblable à celui qui existe sur $\mathbf{Z}$; en particulier, et c'est absolument fondamental, on doit avoir en un certain sens unicité d'une telle décomposition. Le lecteur attentif se souvient sans doute que nous avons déjà formalisé une telle propriété de « décomposition unique en produits d'irréductibles » : c'est la notion d'anneau factoriel, introduite dans le théorème 4.31. De fait, on a la généralisation de la proposition ci-dessus.

Proposition 7.2 *Soit A un anneau factoriel, soit $n \geqslant 2$ un entier, b et c des éléments de A premiers entre eux et $a = bc$. On suppose que a est associé à une puissance n-ème (c'est-à-dire à un élément qui s'écrit α^n où $\alpha \in A$). Alors b et c sont aussi associés à des puissances n-ème.*

Là encore, on peut généraliser à un produit fini de facteurs supposés premiers entre eux 2 à 2.

L'idée de Lamé pour démontrer qu'il n'y a pas de solutions entières non triviales à l'équation $x^p + y^p = z^p$ pour p premier impair[30] est d'écrire l'équation sous la forme

$$\prod_{i=0}^{p-1} (x + \zeta_p^i\, y) = z^p \tag{7.1.1}$$

où ζ_p est une racine primitive p-ème de l'unité.

Exercice 30

Justifier cette réécriture.

27. En fait l'énoncé ci-dessus n'a finalement été démontré dans toute sa généralité qu'en 1994 par Andrew Wiles.

28. Mais oui, bien sûr qu'une erreur en mathématiques peut être intéressante ! Celles que vous commettez le sont aussi, à condition de prendre un minimum de temps pour les comprendre.

29. Les énoncés d'unicité sont traditionnellement négligés par nombre d'étudiants, pour lesquels de tels énoncés sont au mieux anecdotiques ; c'est peu de dire qu'ils se fourvoient complètement.

30. Sachant que le dernier théorème de Fermat est vrai pour $n = 4$, pour démontrer le théorème en toute généralité, il suffit de considérer des exposants premiers impairs ; voyez-vous pourquoi ?

Ceci permet de voir l'équation (7.1.1) comme une égalité dans l'anneau noté $\mathbf{Z}[\zeta_p]$ et définit comme le sous-anneau de $\mathbf{C}$ suivant :

$$\mathbf{Z}[\zeta_p] \stackrel{\text{déf}}{=} \{P(\zeta_p), \quad P \in \mathbf{Z}[X]\}.$$

Par des manipulations relativement standards, on montre que s'il existe un triplet $(x, y, z) \in \mathbf{Z}^3$ vérifiant (7.1.1), alors il en existe un tel que les éléments de $\mathbf{Z}[\zeta]$

$$x + \zeta_p\, y,\, x + \zeta_p^2\, y, \ldots, x + \zeta_p^{p-1}\, y \tag{7.1.2}$$

sont premiers entre eux 2 à 2. Comme leur produit est d'après (7.1.1) une puissance p-ème, chacun de ces éléments est associés à une puissance p-ème. De ce dernier fait on arrive à déduire une contradiction.

L'idée de Lamé est très séduisante. Sa faiblesse fondamentale réside cependant dans l'étape consistant à montrer que les éléments (7.1.2) sont des puissances p-ème. En fait, on applique à ce stade la (généralisation de la) proposition 7.2. Le problème est que l'anneau $\mathbf{Z}[\zeta_p]$ n'est en général pas factoriel. À l'époque où Lamé propose sa démonstration, l'existence d'anneaux non factoriels n'était vraiment pas une évidence, et il semblait naturel de penser que les propriétés de $\mathbf{Z}$ se généralisaient aisément [31] aux anneaux $\mathbf{Z}[\zeta_p]$.

La stratégie de Lamé s'applique quand même dans certains cas. Insistons lourdement sur le fait que le problème des anneaux $\mathbf{Z}[\zeta_p]$ en général n'est pas le défaut d'*existence* d'une décomposition en produit d'irréductibles. Cette propriété d'existence est en fait vraie pour tous les anneaux $\mathbf{Z}[\zeta_p]$. Ce qui fait défaut, ce qui est vraiment exigant, est la propriété d'*unicité* de la décomposition.

Il est à noter également que le défaut de factorialité d'anneaux tel que les anneaux $\mathbf{Z}[\zeta_p]$ est ce qui a poussé Kummer et Dedekind à dégager la notion d'*idéal*[32], fondement de l'approche algébrique de la théorie des nombres et de l'algèbre moderne en général.

Dans ce chapitre nous allons suivre une approche similaire, dans son point de départ, à celle utilisée par Lamé, à savoir nous allons résoudre un problème d'arithmétique sur $\mathbf{Z}$ en nous plaçant dans un anneau plus gros. Cet anneau, appelé anneau des entiers de Gauss, est factoriel, et ainsi nous ne risquons pas d'être confronté au même souci que Lamé. On va même voir qu'il est doté d'une propriété bien plus forte : on peut y pratiquer une division euclidienne similaire à celles qui existent sur $\mathbf{Z}$ et $\mathbf{K}[X]$.

7.2 Énoncé du théorème des deux carrés

Le problème qui va nous occuper est le suivant : quels sont les nombres premiers qui s'écrivent comme la somme de deux carrés d'entiers [33] ? En d'autres termes, peut on

31. Bien sûr, en toute rigueur, Lamé aurait dû penser à le vérifier ; que celui qui n'est jamais tombé dans le piège d'une généralisation hâtive lui jette la première pierre... En fait, Kummer avait peu de temps auparavant justement démontré que cette généralisation n'était pas valide, mais Lamé n'était pas au courant de ce travail ; à l'époque, la circulation des nouvelles découvertes scientifiques n'était évidemment pas aussi aisée qu'actuellement !

32. Oui, c'est bien celle qu'on a vue dans ce cours !

33. Pour en savoir plus sur ce problème et ses généralisations naturelles, notamment du point de vue historique, vous pouvez consulter le premier chapitre du très bel ouvrage *Primes of the form* $x^2 + n\,y^2$.

caractériser les nombres premiers p tels que l'équation

$$x^2 + y^2 = p \tag{7.2.1}$$

possède au moins une solution $(x, y) \in \mathbf{Z}$? Commençons par remarquer que si l'on se fixe p, il est facile de borner la valeur absolue des solutions éventuelles (x, y) de (7.2.1) : une telle solution vérifie en effet nécessairement $x^2 \leqslant p$ soit $|x| \leqslant \sqrt{p}$. Comme il n'y a qu'un nombre fini d'entiers x vérifiant cette condition, un examen au cas par cas permet de déterminer en un temps fini si (7.2.1) possède ou non des solutions. Considérons à titre d'exemple le cas $p = 19$. Si (x, y) est une solution, nécessairement on a $|x| \leqslant \sqrt{19}$, d'où $|x| \in \{0, 1, 2, 3, 4\}$. Mais aucun des entiers

$$19 = 19 - 0^2,\ 18 = 19 - 1^2,\ 15 = 19 - 2^2,\ 10 = 19 - 3^2,\ 3 = 19 - 4^2$$

n'est le carré d'un entier ; ainsi dans ce cas (7.2.1) n'est vérifiée par aucun couple $(x, y) \in \mathbf{Z}^2$. En revanche si $p = 17$, le couple $(4, 1)$ est solution.

On peut ainsi examiner le problème pour de petits nombres premiers p, en s'aidant éventuellement d'un calculateur. On s'aperçoit assez vite que les nombres premiers qui sont somme de deux carrés semblent être, hormis 2, exactement ceux qui vérifient la congruence $p \equiv 1 \mod 4$. Nous allons démontrer que c'est effectivement le cas.

Théorème 7.3 (Théorème des deux carrés) *Soit p un nombre premier impair. Alors les conditions suivantes sont équivalentes :*

1. *il existe $(x, y) \in \mathbf{Z}^2$ tel que $p = x^2 + y^2$;*
2. *on a $p \equiv 1 \mod 4$.*

Au cours de la démonstration, nous produirons en outre un algorithme efficace qui, étant donné un nombre premier p congru à 1 modulo 4, produit un couple $(x, y) \in \mathbf{Z}^2$ solution de (7.2.1). Notez que nous connaissons déjà un algorithme naïf : celui donné par la procédure décrite ci-dessus de recherche de solutions basée sur la majoration a priori de leur valeur absolue. L'algorithme décrit ci-dessous est beaucoup plus rapide (mais nous ne démontrerons pas ce fait).

7.3 La condition $p \equiv 1 \mod 4$ dans le théorème des deux carrés est nécessaire

Soit p un nombre premier impair tel qu'il existe $(x, y) \in \mathbf{Z}^2$ vérifiant

$$x^2 + y^2 = p. \tag{7.3.1}$$

Montrons qu'on a nécessairement $p \equiv 1 \mod 4$.

Fermat, class field theory and complex multiplication. de David Cox ; il vous faudra attendre un peu pour aborder les autres chapitres mais ils sont tout aussi intéressants et bien écrits.

7.3.1 Première démonstration par réduction modulo 4

En réduisant (7.3.1) modulo 4, on obtient

$$x^2 + y^2 \equiv p \mod 4. \tag{7.3.2}$$

Mais pour tout x dans $\mathbf{Z}$, x est congru à 0, 1, 2, ou 3 modulo 4, donc x^2 est congru à 0, 1^2, $2^2 = 4 + 0$, $3^2 = 2.4 + 1$ modulo 4, en d'autres termes x^2 est congru à 0 ou 1 modulo 4. Ainsi pour tout couple (x, y) de $\mathbf{Z}^2$, $x^2 + y^2$ est congru à $0 + 0$, $0 + 1$ ou $1 + 1$ modulo 4. De (7.3.2), on déduit que p est congru à 0, 1 ou 2 modulo 4. Mais un entier congru à 0 ou 2 modulo 4 est nécessairement pair. Ainsi p est nécessairement congru à 1 modulo 4.

7.3.2 Deuxième démonstration par le théorème de Lagrange

Commençons par montrer que si (x, y) vérifie (7.3.1), alors y n'est pas divisible par p. Raisonnons par l'absurde et supposons le contraire. Alors p (et même p^2) divise y^2 et (7.3.1) montre que p divise $x^2 = p - y^2$. Par le lemme d'Euclide p divise x, donc p^2 divise x^2 ; finalement p^2 divise $x^2 + y^2$, donc p^2 divise p, d'où p divise 1, contradiction. Ainsi $[y]_p$ est non nul, donc inversible. Soit t l'élément de $\mathbf{F}_p$ définit par $t = [x]_p[y]_p^{-1}$. En appliquant le morphisme $[\,.\,]_p$ à (7.3.1), on obtient $[x]_p^2 + [y]_p^2 = 0$, d'où $t^2 = -1$. En particulier $t^4 = 1$ et t est d'ordre 4 dans $\mathbf{F}_p^\times$. Par le théorème de Lagrange, 4 divise l'ordre de $\mathbf{F}_p^\times$, soit $p - 1$. On a donc bien $p \equiv 1 \mod 4$.

7.4 L'anneau des entiers de Gauss

Pour démontrer la réciproque du théorème des deux carrés, on introduit l'anneau des entiers de Gauss.

7.4.1 Définition et premières propriétés de l'anneau des entiers de Gauss

Proposition 7.4 *Le sous-ensemble de* $\mathbf{C}$

$$\{a + b\,i, \quad (a, b) \in \mathbf{Z}^2\}$$

est un sous-anneau de $\mathbf{C}$.

Définition 7.5 L'anneau des entiers de Gauss *est le sous-anneau de* $\mathbf{C}$ *introduit dans la proposition précédente. On le note* $\mathbf{Z}[i]$.

Définition 7.6 *Pour tout* $z \in \mathbf{C}$, *on pose* $N(z) = |z|^2 = z\,\overline{z}$. *On définit ainsi une application* $N : \mathbf{C} \to \mathbf{R}^+$ *appelée* norme.

Remarque 7.7 : Attention, cette application n'est pas la norme euclidienne usuelle sur $\mathbf{C}$ (identifié à $\mathbf{R}^2$ via la $\mathbf{R}$-base $\{1, i\}$) mais son carré. En particulier, si $x \in \mathbf{R}$, on a $N(x) = x^2$. La terminologie adoptée, bien que pouvant donc porter à confusion, est cependant tout à fait standard. □

Remarque 7.8 : Pour tout $z \in \mathbf{C}$, on a $N(z) = 0$ si et seulement si $z = 0$.

Si $z \in \mathbf{C}$ est écrit sous la forme $a + i\,b$ avec $(a, b) \in \mathbf{R}^2$, alors on a $N(z) = a^2 + b^2$. □

La norme est un outil extrêmement utile pour travailler avec l'anneau des entiers de Gauss, grâce notamment au lemme suivant, dont la démonstration est élémentaire et laissée au lecteur.

Lemme 7.9 *La norme N vérifie les propriétés suivantes.*

1. *Pour tous $z, z' \in \mathbf{C}$, on a $N(z\,z') = N(z)\,N(z')$.*
2. *Pour tout $z \in \mathbf{Z}[i]$, on a $N(z) \in \mathbf{N}$.*

Illustrons tout de suite l'intérêt de la norme par la détermination des éléments inversibles de $\mathbf{Z}[i]$.

Proposition 7.10 *Soit $z \in \mathbf{Z}[i]$. Alors $z \in \mathbf{Z}[i]^\times$ si et seulement si $N(z) = 1$. En particulier $\mathbf{Z}[i]^\times = \{1, -1, i, -i\}$.*

Démonstration : Cette démonstration est prototypique de l'utilisation de la norme dans l'étude arithmétique de $\mathbf{Z}[i]$. Il est donc conseillé de la travailler soigneusement.

Supposons $z \in \mathbf{Z}[i]^\times$. Il existe donc $z' \in \mathbf{Z}[i]$ vérifiant $z\,z' = 1$. En prenant la norme et en utilisant le lemme 7.9, on obtient $N(z)N(z') = 1$. Toujours d'après le lemme 7.9, $N(z)$ et $N(z')$ sont des entiers naturels. On a donc nécessairement $N(z) = 1$.

Supposons $N(z) = 1$. Ceci se réécrit $z\,\overline{z} = 1$. Mais comme on a $z \in \mathbf{Z}[i]$, on a également $\overline{z} \in \mathbf{Z}[i]$ (lecteur : pourquoi ?). Ainsi z est bien un élément de $\mathbf{Z}[i]^\times$.

On a donc

$$\mathbf{Z}[i]^\times = \{a + i\,b, \quad (a, b) \in \mathbf{Z}^2, \quad a^2 + b^2 = 1\}$$

et on conclut en déterminant les triplets $(a, b) \in \mathbf{Z}^2$ vérifiant $a^2 + b^2 = 1$ (noter qu'on a nécessairement $|a| \leqslant 1$ et $|b| \leqslant 1 \ldots$). □

Remarque 7.11 : Attention ! si $z \in \mathbf{C}$ et $N(z) = 1$, z n'est pas nécessairement un élément de $\mathbf{Z}[i]^\times$. □

Corollaire 7.12 *Soit z, z' des éléments de $\mathbf{Z}[i]$. Supposons que z divise z', et qu'on a $N(z) = N(z')$. Alors z et z' sont associés.*

Démonstration : Rappelons que « z divise z' » signifie qu'il existe un élément u de $\mathbf{Z}[i]$ vérifiant $z' = u\,z$. Si $N(z) = N(z') = 0$ alors z et z' sont nuls tous les deux, et sont donc bien associés. Sinon, prenant la norme dans l'égalité $z' = u\,z$, on trouve $N(z') = N(u)N(z)$, d'où, comme $N(z) = N(z') \neq 0$, $N(u) = 1$. Ainsi on a $u \in \mathbf{Z}[i]$ et $N(u) = 1$. D'après la proposition 7.10, on a $u \in \mathbf{Z}[i]^\times$. Donc z et z' sont bien associés. □

Remarque 7.13 : On remarquera que même si on connaît explicitement tous les éléments de $\mathbf{Z}[i]^\times$, il peut être très pratique pour certains raisonnements d'utiliser la première caractérisation de $\mathbf{Z}[i]^\times$ donnée par la proposition 7.10, à savoir celle en termes de la norme. □

7.4.2 Division euclidienne dans $\mathbf{Z}[i]$

Lemme 7.14 *Pour tout $z \in \mathbf{C}$, il existe $u \in \mathbf{Z}[i]$ tel que $N(u - z) < 1$.*

Démonstration : En raisonnant dans le plan complexe, il s'agit de montrer que tout point du plan est à distance strictement inférieure à 1 d'un point à coordonnées entières, ce qui se ramène aussitôt à l'énoncé suivant : tout point contenu dans un carré de côté 1 est à distance strictement inférieure à 1 de l'un des sommets du carré. Ceci se vérifie facilement par exemple à l'aide du théorème de Pythagore et de l'identité triangulaire (en fait, étant donné un point d'un carré de côté 1, sa plus petite distance aux sommets est toujours inférieure à $\frac{\sqrt{2}}{2}$, et cette borne n'est atteinte que pour le centre du carré). □

Remarque 7.15 : Plus prosaïquement, on peut constater que si l'on écrit $z = a + i\,b$ avec $(a, b) \in \mathbf{R}^2$ et qu'on pose $v = \mathrm{Ent}(a) + i\ \mathrm{Ent}(b) \in \mathbf{Z}[i]$, alors

1. si $(\mathrm{Frac}(a), \mathrm{Frac}(b)) \in [0, \frac{1}{2}] \times [0, \frac{1}{2}]$, $u = v$ convient ;
2. si $(\mathrm{Frac}(a), \mathrm{Frac}(b)) \in [0, \frac{1}{2}] \times [\frac{1}{2}, 1]$, $u = v + i$ convient ;
3. si $(\mathrm{Frac}(a), \mathrm{Frac}(b)) \in [\frac{1}{2}, 1] \times [0, \frac{1}{2}]$, $u = v + 1$ convient ;
4. si $(\mathrm{Frac}(a), \mathrm{Frac}(b)) \in [\frac{1}{2}, 1] \times [\frac{1}{2}, 1]$, $u = v + 1 + i$ convient.

□

Remarque 7.16 : En général, u n'est pas unique ! Ceci aura pour conséquence (sans gravité aucune) la non unicité de la division euclidienne dans $\mathbf{Z}[i]$ en général. □

Théorème 7.17 (Division euclidienne dans l'anneau des entiers de Gauss) *Soient z et z' des éléments de $\mathbf{Z}[i]$, z' étant supposé non nul. Il existe alors un couple (q, r) d'éléments de $\mathbf{Z}[i]$ vérifiant $z = q\,z' + r$ et $N(r) < N(z')$.*

Remarque 7.18 : Le lecteur attentif aura remarqué que contrairement au cas de $\mathbf{Z}$ ou $\mathbf{K}[X]$, nous n'énonçons pas ici de propriété d'unicité de la division euclidienne. Il y a une bonne raison à cela : comme nous l'avons déjà évoqué, une telle propriété est fausse pour $\mathbf{Z}[i]$. Ceci n'a aucune espèce d'importance dans la pratique. Pour le coup, et contrairement à un principe général énoncé un peu plus haut dans ce cours, l'unicité de la division euclidienne dans $\mathbf{Z}$ ou $\mathbf{K}[X]$ n'est pas une propriété très importante. Ce qui est important, et ce que trop d'étudiants ont tendance à négliger, que ce soit sur $\mathbf{Z}$, sur $\mathbf{K}[X]$ ou sur $\mathbf{Z}[i]$, c'est la *condition sur le reste.* □

Démonstration : D'après le lemme 7.14, il existe $q \in \mathbf{Z}[i]$ vérifiant

$$N\left(\frac{z}{z'} - q\right) < 1.$$

Posant $r = z - q\,z' \in \mathbf{Z}[i]$, l'inégalité précédente, après multiplication par $N(z')$, se réécrit $N(r) < N(z')$. □

Remarque 7.19 : En dépit de la non-unicité de la division euclidienne dans $\mathbf{Z}[i]$ en général, on a que z' divise z (autrement dit $\frac{z}{z'} \in \mathbf{Z}[i]$) si et seulement s'il existe une division euclidienne avec un reste nul (et dans ce cas la division euclidienne est unique). □

Dans la pratique, « la » division euclidienne de z par z' s'effectue comme indiqué par la démonstration : on détermine $q \in \mathbf{Z}[i]$ vérifiant $N\left(\frac{z}{z'} - q\right) < 1$ et on pose $r = z - z'\,q$. Pour expliciter q, on commence par écrire $\frac{z}{z'}$ sous la forme $a + i\,b$ avec $a, b \in \mathbf{Q}$ (en multipliant par la quantité conjuguée du dénominateur) et on détermine les parties entières et fractionnaires de a et b (dans la pratique, cela met en jeu une division euclidienne du numérateur par le dénominateur). On peut alors se référer à la remarque 7.15 et/ou faire un petit dessin.

Exemple 7.20 : Soit à effectuer « la » division euclidienne de $15 + 3\,i$ par $3 + i$. On a

$$\frac{15 + 31\,i}{3 + i} = \frac{(15 + 31\,i)(3 - i)}{10} = \frac{76 + 78\,i}{10} = 7 + 7\,i + \frac{6}{10} + \frac{8}{10}\,i.$$

On voit (dessin ou remarque 7.15) qu'on a $N\left(\frac{15+31\,i}{3+i} - (8 + 8\,i)\right) < 1$. On calcule alors

$$15 + 31\,i - (3 + i)(8 + 8\,i) = 15 + 3\,i - (16 + 32\,i) = -1 - i.$$

Ainsi

$$15 + 31\,i = (3 + i)(8 + 8\,i) + (-1 - i)$$

est une division euclidienne de $15 + 31\,i$ par $3 + i$, de quotient $8 + 8\,i$ et de reste $-1 - i$.

Noter qu'on a également $N\left(\frac{15+31\,i}{3+i} - (7 + 8\,i)\right) < 1$. On en déduit que

$$15 + 31\,i = (3 + i)(7 + 8\,i) + 2$$

est une autre division euclidienne de $15 + 31\,i$ par $3 + i$, de quotient $7 + 8\,i$ et de reste 2. □

7.4.3 L'anneau des entiers de Gauss est principal

Tout comme dans le cas de $\mathbf{Z}$ et de $\mathbf{K}[X]$, l'existence d'une division euclidienne sur $\mathbf{Z}[i]$ va nous permettre de montrer qu'il s'agit d'un anneau principal, c'est-à-dire que tous ses idéaux sont engendrés par un élément (*cf.* les définitions 4.15 et 4.28). La démonstration présentera des similarités frappantes avec les démonstrations correspondantes sur $\mathbf{Z}$ (théorème 3.1) et $\mathbf{K}[X]$ (théorème 4.30). En fait, il est possible (nous ne le ferons pas dans ce cours) d'unifier les trois démonstrations en utilisant le concept d'anneau euclidien, et en montrant qu'un anneau euclidien est principal.

Théorème 7.21 *L'anneau $\mathbf{Z}[i]$ est principal.*

Démonstration : En tant que sous-anneau de $\mathbf{C}$, $\mathbf{Z}[i]$ est intègre.

Soit I un idéal de $\mathbf{Z}[i]$. Il s'agit de montrer qu'il existe $z \in \mathbf{Z}[i]$ vérifiant $I = z.\mathbf{Z}[i]$. Si $I = \{0\}$, $z = 0$ convient. Sinon, l'ensemble

$$\{N(z), \quad z \in I \setminus \{0\}\}$$

est une partie non vide de $\mathbf{N} \setminus \{0\}$. Soit N_0 son plus petit élément et $z_0 \in I$ vérifiant $N(z_0) = N_0$. Nous allons montrer qu'on a $I = z_0\mathbf{Z}[i]$. Comme $z_0 \in I$, on a déjà l'inclusion $z_0\mathbf{Z}[i] \subset I$ (*cf.* le lemme 4.14).

Montrons l'inclusion inverse. Soit $z \in I$. Comme z_0 est non nul, on peut considérer une division euclidienne de z par z_0 ; on a donc une écriture $z = z_0\, q + r$ avec $q, r \in \mathbf{Z}[i]$ et $N(r) < N(z_0)$. Comme z et z_0 sont dans I, $r = z - z_0\, q$ est également un élément de I. Ainsi r vérifie les deux propriétés :

1. $r \in I$
2. $N(r) < \mathrm{Min}\{N(z), \quad z \in I \setminus \{0\}\}$.

On en déduit aussitôt que $r = 0$. Ainsi $z = z_0\, q$ et on a bien $z \in I$. □

Remarque 7.22 : Puisque $\mathbf{Z}[i]$ est principal, le théorème 4.31 s'applique. En particulier, toute paire d'élément possède « un » pgcd et le théorème de Bézout vaut. Dans la pratique, il est important de pouvoir calculer efficacement des pgcd et des coefficients de Bézout dans $\mathbf{Z}[i]$.

Dans un anneau principal quelconque, c'est loin d'être évident ; mais s'il existe une division euclidienne[34] le bon vieil algorithme d'Euclide (et sa version étendue) utilisé sur $\mathbf{Z}$ et $\mathbf{K}[X]$ marche tout aussi bien sur $\mathbf{Z}[i]$. □

Exemple 7.23 : Illustrons la remarque précédente sur un exemple. Soit à calculer un pgcd de $15 + 31\, i$ et $3 + i$ et une relation de Bézout pour ces éléments.

On a déja vu que

$$15 + 31\, i = (3 + i)(8 + 8\, i) + (-1 - i)$$

est une division euclidienne de $15 + 31\, i$ par $3 + i$, de quotient $8 + 8\, i$ et de reste $-1 - i$.

Il s'agit à présent d'effectuer « la » division euclidienne de $3 + i$ par $-1 - i$. On calcule

$$\frac{3 + i}{-1 - i} = \frac{(3 + i)(-1 + i)}{2} = -2 + i.$$

Ainsi $\frac{3+i}{-1-i} \in \mathbf{Z}[i]$, autrement dit $-1 - i$ divise $3 + i$ et le reste est nul. Un pgcd de $15 + 31\, i$ et $3 + i$ est donc $-1 - i$.

Pour trouver une relation de Bézout, on peut, tout comme sur $\mathbf{Z}$, « remonter » les calculs[35]. Ici il n'y a qu'une étape qui consiste à réécrire la première division euclidienne sous la forme

$$-1 - i = (-1).(15 + 31\, i) + (8 + 8\, i)(3 + i).$$

34. Il est difficile d'exhiber un anneau principal qui n'admet pas de division euclidienne.

35. L'algorithme d'Euclide étendu est également disponible ; les formules sont exactement les mêmes que sur $\mathbf{Z}$.

□

7.5 -1 est-il un carré modulo p ?

7.5.1 Une caractérisation des carrés modulo p

Définition 7.24 *Soit $N \geqslant 1$ un entier et $a \in \mathbf{Z}$. On dit que a est un carré modulo N si l'une des deux conditions équivalentes suivantes est vérifiée :*

1. *il existe $b \in \mathbf{Z}$ tel que $a \equiv b^2 \mod p$;*
2. *il existe $x \in \mathbf{Z}/N\mathbf{Z}$ tel que $[a]_N = x^2$.*

Remarque 7.25 : Si a est le carré d'un entier, a est un carré modulo N pour n'importe quel $N \geqslant 1$. □

Théorème 7.26 *Soit p un nombre premier impair. Alors il y a exactement $\frac{p-1}{2}$ éléments de $\mathbf{F}_p^\times$ qui sont des carrés, c'est-à-dire des éléments x de $\mathbf{F}_p^\times$ tels qu'il existe $y \in \mathbf{F}_p^\times$ vérifiant $x = y^2$.*

Par ailleurs $x \in \mathbf{F}_p^\times$ est un carré si et seulement si on a $x^{\frac{p-1}{2}} = 1$.

Démonstration : Considérons l'application

$$\begin{array}{rccc} \mathcal{C} : & \mathbf{F}_p^\times & \longrightarrow & \mathbf{F}_p^\times \\ & x & \longmapsto & x^2 \end{array}$$

et notons C son image. Pour tout $y \in \mathbf{F}_p^\times$, l'équation $x^2 = y^2$ a exactement deux solutions dans $\mathbf{F}_p^\times$; en effet elle se réécrit

$$(x-y)(x+y) = 0$$

soit comme $\mathbf{F}_p$ est intègre, $x \in \{y, -y\}$; or comme p est impair et y est non nul, on a $y \neq -y$.

Ainsi pour tout élément z de C, $\mathcal{C}^{-1}(\{z\})$ est de cardinal 2. Quand z varie dans C, les ensembles $\mathcal{C}^{-1}(\{z\})$ forment une partition de $\mathbf{F}_p^\times$. On a donc

$$p - 1 = \mathrm{card}(\mathbf{F}_p^\times) = \sum_{z \in C} \mathrm{card}(\mathcal{C}^{-1}(\{z\})) = \sum_{z \in C} 2 = \mathrm{card}(C).2$$

d'où $\mathrm{card}(C) = \frac{p-1}{2}$.

Soit $x \in \mathbf{F}_p^\times$. S'il existe $y \in \mathbf{F}_p$ tel que $x = y^2$, nécessairement y est non nul, et on a

$$x^{\frac{p-1}{2}} = \left(y^2\right)^{\frac{p-1}{2}} = y^{p-1} = 1,$$

la dernière égalité provenant du petit théorème de Fermat (*cf.* le corollaire 3.57).

On a donc montré l'inclusion

$$C \subset \{x \in \mathbf{F}_p^\times, \quad x^{\frac{p-1}{2}} = 1\}$$

et il s'agit de montrer qu'on a en fait égalité. Mais l'ensemble de droite est l'ensemble des racines dans $\mathbf{F}_p$ du polynôme $X^{\frac{p-1}{2}} - 1$, il est donc de cardinal au plus $\frac{p-1}{2}$ d'après le corollaire 4.9. Comme C est de cardinal $\frac{p-1}{2}$, on a nécessairement égalité. □

Corollaire 7.27 *Soit p un nombre premier impair. Alors -1 est un carré modulo p si et seulement si on a $p \equiv 1 \mod 4$.*

Démonstration : D'après le théorème précédent, -1 est un carré modulo p si et seulement si on a $[-1]_p^{\frac{p-1}{2}} = [1]_p$, ce qui équivaut à $[(-1)^{\frac{p-1}{2}}]_p = [1]_p$. Or $(-1)^{\frac{p-1}{2}}$ vaut 1 ou -1 selon que p est congru respectivement à 1 ou 3 modulo 4, et comme p est impair, on a $[-1]_p \neq [1]_p$, d'où le résultat. □

Exercice 31

Donner un autre démonstration du corollaire utilisant le théorème de Lagrange ; on pourra s'inspirer de la partie 7.3.2.

7.5.2 Calcul effectif d'une racine carrée de -1 modulo p

Si p est un nombre premier congru à 1 modulo 4, on sait d'après le paragraphe précédent que -1 est un carré modulo p, c'est-à-dire qu'il existe $a \in \mathbf{Z}$ tel que $[a]_p^2 = [a^2]_p = [-1]_p$. Comment déterminer un tel a ? Une possibilité est d'énumérer les « carrés modulo p », et de regarder à chaque fois si le résultat obtenu est égal à $[-1]_p$. Prenons par exemple $p = 17$. On a

$$[1]_p^2 = [1]_p \neq [-1]_p, \quad [2]_p^2 = [4]_p \neq [-1]_p, \quad [3]_p^2 = [9]_p \neq [-1]_p, \quad [4]_p^2 = [16]_p = [17-1]_p = [-1]_p.$$

On sait que ce procédé aboutira toujours au bout d'un nombre fini d'étapes, quitte à devoir calculer les $\frac{p-1}{2}$ carrés non nuls de $\mathbf{F}_p$. Dans la pratique, lorsque p est grand, cette énumération a un coût en termes de temps de calcul trop important [36].

Nous donnons à présent un algorithme beaucoup plus efficace (mais nous passerons sous silence l'estimation de sa complexité). On commence par écrire $p - 1 = 2^n.m$ avec $n \geqslant 2$ et m impair (rappelons que p est congru à 1 modulo 4).

On choisit au hasard $x \in \mathbf{F}_p^\times$ et on calcule $y = x^m$ à l'aide de la méthode d'exponentiation binaire, vue dans le module « Méthodes formelles 1 ». Supposons qu'on ait $y \notin \{[1]_p, [-1]_p\}$.

36. À quiconque tenté de se dire « Quand même, on a des ordinateurs puissants de nos jours, ça ne doit pas être si long que ça », rappelons que, dans la pratique, « grand » signifie souvent que p est très largement supérieur au nombre d'atomes de l'univers.

On calcule y^2, $y^4 = (y^2)^2 \ldots$ Soit $1 \leqslant n_0 \leqslant n-1$ le plus petit entier vérifiant $y^{2^{n_0}} = [-1]_p$ (nous justifions ci-dessous l'existence de n_0). Alors $z = y^{2^{n_0-1}}$ vérifie $z^2 = [-1]_p$.

Pour justifier l'existence de n_0, on remarque qu'on a $y^{2^n} = x^{m\,2^n} = x^{p-1} = [1]_p$ d'après le petit théorème de Fermat. Ainsi l'ordre de y divise 2^n. Cet ordre s'écrit donc 2^m avec $1 \leqslant m \leqslant n$. Comme $y \notin \{[1]_p, [-1]_p\}$, on a $y^2 \neq [1]_p$, et donc $m \geqslant 2$. Alors $y^{2^{m-1}}$ est distinct de $[1]_p$ et son carré est $[1]_p$, donc il est égal à $[-1]_p$.

Bien sûr, pour que l'algorithme fonctionne, il faut qu'il existe au moins un $x \in \mathbf{F}_p^\times$ qui vérifie $x^m \notin \{[1]_p, [-1]_p\}$. Mais si ça n'était pas le cas, on aurait

$$\forall x \in \mathbf{F}_p^\times, \quad x^{2\,m} = [1]_p.$$

Comme $2m < p-1 = 2^n\,m$, ceci contredirait le fait que $\mathbf{F}_p^\times$ est cyclique.

Exercice 32

Calculer la proportion des éléments $x \in \mathbf{F}_p^\times$ pour lesquels on a $x^m \notin \{[-1]_p, [1]_p\}$. Montrer en particulier qu'elle est toujours supérieure à $\frac{1}{2}$.

Exemple 7.28 : On considère le nombre premier $p = 113$ qui s'écrit $2^4.7 + 1$.

Pour calculer des puissances 7ème à l'aide de l'exponentiation binaire, on décompose 7 en base 2

$$7 = 2^2 + 2^1 + 2^0$$

de sorte que pour tout x on a

$$x^7 = (x^2)^2\,x^2\,x.$$

Choisissons $x = [2]_{113}$. On a $x^2 = [4]_{113}$ et $(x^2)^2 = [4^2]_{113} = [16]_{113}$. Ainsi on a

$$x^7 = [16.4.2]_{113} = [128]_{113} = [15]_{113}.$$

En particulier on a $x^7 \notin \{[1]_{113}, [-1]_{113}\}$. Calculons à présent

$$(x^7)^2 = [15^2]_{113} = [225]_{113} = [-1]_{113}.$$

Ainsi on a $15^2 \equiv -1 \mod 113$. □

7.6 La condition $p \equiv 1 \mod 4$ dans le théorème des deux carrés est suffisante

Nous donnons d'abord la démonstration de ce fait, puis nous présentons un algorithme efficace permettant d'écrire un nombre premier congru à 1 modulo 4 sous la forme d'une somme de deux carrés.

7.6.1 Démonstration

Soit $c \in \mathbf{Z}$ tel que $c^2 \equiv -1 \mod p$. Soit z un pgcd de p et $c+i$. Comme z divise p, il existe $u \in \mathbf{Z}[i]$ tel que $p = z\,u$. En prenant la norme, on trouve $N(z)N(u) = N(p)$ et donc $N(z)$ divise $N(p) = p^2$. Ainsi $N(z) \in \{1, p, p^2\}$. Noter que si $N(z) = p$, en écrivant $z = a + i\,b$ avec $(a, b) \in \mathbf{Z}^2$ on trouve $p = a^2 + b^2$ et le théorème des deux carrés est démontré. Nous allons montrer que les cas $N(z) = p^2$ et $N(z) = 1$ ne peuvent pas se produire.

Si $N(z) = p^2$ alors p et z sont associés d'après le corollaire 7.12. Comme z divise $c + i$, p également. Il existe donc $(a, b) \in \mathbf{Z}^2$ tel qu'on ait $p\,(a + i\,b) = c + i$. En particulier, $p\,b = 1$ et p divise 1, contradiction.

Pour montrer que $N(z)$ n'est pas égale à 1, on considère l'application

$$\varphi_c : \begin{array}{ccc} \mathbf{Z}[i] & \longrightarrow & \mathbf{F}_p \\ a + i\,b & \longmapsto & [a - c\,b]_p \end{array}.$$

Nous laissons au lecteur le soin de montrer que φ_c est un morphisme d'anneaux. Montrons que $\mathrm{Ker}(\varphi_c) = z\,\mathbf{Z}[i]$. Comme z est un pgcd de p et $c + i$, et que p et $c + i$ sont visiblement dans le noyau, il suffit de montrer que tout élément de $\mathrm{Ker}(\varphi_c)$ s'écrit $\alpha.p + \beta.(c + i)$ avec $(\alpha, \beta) \in \mathbf{Z}[i]^2$. Soit $(a, b) \in \mathbf{Z}^2$ tel que $a + i\,b \in \mathrm{Ker}(\varphi_c)$, c'est-à-dire tel que p divise $a - c\,b$. Soit $\alpha \in \mathbf{Z}$ tel que $a - c\,b = \alpha\,p$. On a alors

$$a + i\,b = a - c\,b + b\,(c + i) = \alpha\,p + b\,(c + i),$$

ce qui conclut la démonstration du fait que $\mathrm{Ker}(\varphi_c) = z\,\mathbf{Z}[i]$.

Supposons à présent $N(z) = 1$, c'est-à-dire, compte tenu de la proposition 7.10, $z \in \mathbf{Z}[i]^\times$. Alors $z\,\mathbf{Z}[i] = \mathbf{Z}[i]$, et φ_c est identiquement nul ; c'est impossible compte tenu du fait que $\mathbf{F}_p$ n'est pas l'anneau nul.

7.6.2 Pratique de la décomposition en somme de deux carrés

Soit à décomposer un nombre premier p congru à 1 modulo 4 en somme de deux carrés d'entiers. On commence par déterminer $c \in \mathbf{Z}$ tel que $c^2 \equiv -1 \mod p$, à l'aide de l'algorithme décrit dans la partie 7.5.2.

On calcule ensuite un pgcd de p et $c + i$ à l'aide de l'algorithme d'Euclide. D'après la démonstration donnée dans la partie précédente, si ce pgcd s'écrit $a + i\,b$ avec $a, b \in \mathbf{Z}$ alors on a $p = a^2 + b^2$.

Exemple 7.29 : Soit à décomposer 113 en somme de deux carrés. D'après l'exemple traité dans la partie précédente, on peut prendre $c = 15$. Il s'agit à présent de déterminer un pgcd de 113 et $15 + i$, en appliquant l'algorithme d'Euclide.

Déterminons une division euclidienne de 113 par $15 + i$. On a

$$\frac{113}{15 + i} = \frac{113\,(15 - i)}{15^2 + 1} = \frac{1695 - 113\,i}{226} = 7 - i + \frac{1}{2} + \frac{1}{2}\,i.$$

Prenons $q = 7 - i$, soit $r = 113 - (15 + i)(7 - i) = 7 + 8\,i$. Ainsi

$$113 = (7 - i)\,(15 + i) + 7 + 8\,i$$

est une division euclidienne de 113 par $15 + i$, de quotient $7 - i$ et de reste $7 + 8\,i$.

Déterminons à présent une division euclidienne de $15 + i$ par $7 + 8\,i$. On a

$$\frac{15 + i}{7 + 8\,i} = \frac{(15 + i)\,(7 - 8\,i)}{7^2 + 8^2} = \frac{113 - 113\,i}{113} = 1 - i.$$

Comme $1 - i \in \mathbf{Z}[i]$, on voit que $7 + 8\,i$ divise $15 + i$, et l'algorithme d'Euclide est terminé. Ainsi un pgcd de 113 et $15 + i$ est $7 + 8\,i$. On a donc $113 = 7^2 + 8^2$ (ce dont on pouvait d'ailleurs s'apercevoir lors du dernier calcul). □