Licence à distance.

Laurent Evain

Cours sur les Anneaux

Introduction

Vous voici donc en possession du cours sur les anneaux, dans le cadre de votre enseignement à distance.
Le style adopté est, vous vous en rendrez compte, assez informel. Les mathématiques peuvent être enseignées de façon austère. Elles peuvent en revanche reposer sur de l'enthousiasme, des essais et des erreurs, les joies du progrès (et les peines devant les difficultés !). Bref, les mathématiques sont une activité vivante, aux antipodes de la représentation poussiéreuse qui sévit parfois. J'ai tenté de mettre en évidence ce point de vue, de partir des exemples en les motivant, en les examinant, en les modifiant et en les mettant en action. A l'inverse, j'ai essayé de ne pas plaquer des théorèmes sans justification.
Néanmoins, extraire d'un enseignement un savoir personnel dépend d'abord de vous. Regarder un conducteur d'un oeil critique est certes profitable, mais se mettre au volant est la seule piste sérieuse pour apprendre à conduire. Le professeur est le guide, mais vous n'acquerrez vraiment un savoir qu'en vous confrontant vous même à des exercices, en les cherchant avec patience et énergie. Pour cette raison de nombreux exercices sont intégrés au fil du cours. Ils sont ensuite repris dans les feuilles d'exercices accompagnés d'exercices supplémentaires.
D'un point de vue pratique, effercez-vous de chercher tous les exercices. La rédaction étant une activité très chronophage, vous n'aurez peut-être pas le temps de rédiger toutes vos solutions. Essayez cependant d'en rédiger complètement *au moins* une sur trois. L'expérience montre que l'effort de verbalisation/rédaction est source de progrès. Ne négligez pas cet outil.
Enfin, dernier conseil, ne soyez pas timide et posez vos questions sur les forums. Il serait absurde par simple pudeur de vous retrouver bloqué au milieu de la route.
Bon courage !

“Je peux vous conduire jusqu’à la source, mais le seul qui puisse boire, c’est vous même”.
Buddha Gautama.

Chapitre 1

Anneaux et morphismes entre anneaux

Objectif: Dans ce chapitre, on présente les objets que l'on rencontrera tout au long de ce cours, à savoir anneaux, morphismes d'anneaux et idéaux, ainsi que les exemples que l'on suivra en continu. Le chapitre se termine avec la présentation des objectifs de ce cours.

1.1 Anneaux et sous anneaux

Ce cours traite des anneaux. Essentiellement un anneau est un ensemble sur lequel on peut faire des additions, des soustractions et des multiplications. Par exemple, l'ensemble $\mathbb{N}$ des entiers naturels n'est pas un anneau puisque la soustraction $4 - 8$ n'est pas bien définie. En revanche, l'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau. De même les matrices de taille 3×3 à coefficients réels forment un anneau puisqu'on peut additionner, multiplier et soustraire des matrices 3×3. Bien sûr, pour avoir une structure intéressante et riche de propriétés, il faut des compatibilités entre addition, multiplication et soustraction. Ces règles de compatibilité ne sont pas des règles abstraites introduites par les caprices des mathématiciens, mais simplement les règles que vous utilisez tous les jours avec les entiers ou les matrices. Par exemple la distributivité $x(y + z) = xy + xz$. Ou encore le fait que $-1.x + x = 0$ (c'est une propriété qui n'utilise que $-, +$ et la multiplication . donc qui a un sens dans un anneau). Donnons maintenant une définition plus formelle.

Définition 1. *Un anneau est un ensemble A muni de deux opérations $+ : A \times A \to A$ et $. : A \times A \to A$, et de deux éléments privilégiés 0 et 1 satisfaisant aux conditions suivantes:*

- *le $+$ est associatif:* $(a+b)+c = a+(b+c)$
- *le $+$ est commutatif:* $a+b = b+a$
- 0 *est un neutre pour* $+$*:* $0+a = a$
- *tout $a \in A$ admet un élément inverse, noté $-a$, pour $+$, i.e. un élément vérifiant $a+(-a) = 0$.*
- *la mulitiplication est associative:* $(ab)c = a(bc)$
- 1 *est un neutre pour la multiplication:* $1.a = a.1 = a$
- *la multiplication est distributive par rapport à l'addition:* $a.(b+c) = a.b + a.c$.

Commençons par remarquer que la différence n'est pas explicitement définie, mais implicitement: par définition, la soustraction $a-b$ dans un anneau est égale à la quantité $a+(-b)$. Au niveau notation, on omettra souvent le signe . du produit et on notera ab plutôt que $a.b$.
Les exemples d'anneau cités précédemment sont $\mathbb{Z}$ et $M_{3\times 3}(\mathbb{R})$. Essayons d'en construire d'autre. Considérons par exemple un ensemble réduit à un élément $\{*\}$. Il n'y a qu'une seule addition possible $*+*=*$ et une seule multiplication possible $**=*$. L'élément privilégié 0 ne peut être que $*$, de même pour 1. Les tables d'addition et de multiplication sont donc particulièrement simples:

$+$	$*$
$*$	$*$

,

$.$	$*$
$*$	$*$

Exercice 1. Vérifiez que l'ensemble $\{*\}$ muni de la seule addition et de la seule multiplication possible est un anneau pour lequel $0 = 1 = *$.

Correction 1. Toutes les égalités à vérifier sont forcément vérifiées puisque de part et d'autre de l'égalité on ne peut avoir que $*$ comme résultat.

Le fait que $0 = 1$ peut vous choquer. Mais effectivement, ce n'est pas interdit au vu de la définition précédente. Rassurez vous, en pratique, cela n'arrive jamais sauf pour le cas précédent.

Exercice 2. Le seul anneau pour lequel $0 = 1$ est l'anneau réduit à un élément 0 avec l'addition $0+0=0$ et $0.0=0$.

Correction 2. On commence par remarquer que dans un anneau $0.a$ vaut toujours 0. En effet $0a = (0+0)a = 0a+0a$. Donc en ajoutant $-(0a)$ de chaque côté de l'égalité, on trouve $0 = 0a$. Si A est un anneau dans lequel $0 = 1$, alors $a = 1a = 0a = 0$, ie. tout élément est nul.

Remarquons également que l'on n'a pas supposé que la multiplication est commutative, ie. que $a.b = b.a$. Ce n'est d'ailleurs pas le cas pour les matrices

Exercice 3. Trouver deux matrices M et N de taille 2×2 telles que $M.N \neq N.M$.

Correction 3. Presque tous les couples de matrices conviennent. Au hasard, avec $M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $N = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$, on a $NM = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix}$ tandis que $MN = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

Néanmoins, les exemples intéressants que nous seront amenés à considérer à notre niveau seront tous des anneaux commutatifs, ie. des anneaux dont la multiplication est commutative. Comme il est toujours déconseillé de faire de la théorie qui tourne à vide, sans exemple, on adopte la convention suivante: **Dans ce cours, sauf mention explicite du contraire, le mot anneau sera synonyme d'anneau commutatif.**
Essayons maintenant de construire un anneau (commutatif) à deux éléments. Puisque l'anneau contient 0 et 1, l'ensemble est forcément $E = \{0, 1\}$. Pour l'addition $0 + x = x$ par définition. Donc la seule addition qu'on peut choisir est $1 + 1$. Doit-on choisir $1 + 1 = 1$ ou $1 + 1 = 0$? On sait que dans un anneau, 1 a un inverse, qu'on note symboliquement -1 (on ne sait pas pour l'instant si $-1 = 0$ ou si $-1 = 1$). Si $1 + 1 = 1$, alors en ajoutant (-1) de chaque côté de l'égalité, on obtient $(-1)+1+1 = (-1)+1$, c'est à dire après simplification $0 = 1$. Mais ce n'est pas possible, puisqu'on a vu que le seul anneau pour lequel $0 = 1$ est l'anneau réduit à un élément. Donc $1 + 1 = 0$. D'où la table d'addition:

+	0	1
0	0	1
1	1	0

Pour la table de multiplication, on n'a pas le choix pour la multiplication par 1, qui est neutre pour la multiplication. Le seul choix qu'on peut éventuellement faire est celui de 0.0. Est-ce que ça vaut 0 ou 1. Supposons $0.0 = 1$. Calculons $(0 + 0).0$. Si on calcule la parenthèse, on trouve 0, donc au total, on trouve $(0 + 0).0 = 0.0 = 1$. Mais si on utilise la distributivité, on trouve $(0 + 0).0 = 0.0 + 0.0 = 1 + 1 = 0$. Bref, on trouve deux résultats différents pour le même calcul. Contradiction. C'est qu'en fait $0.0 = 0$.

D'où la table de multiplication:

.	0	1
0	0	0
1	0	1

En résumé, s'il existe une structure d'anneau sur l'ensemble à deux éléments, elle est nécéssairement donnée par les tables d'addition et multiplication précédentes. On peut vérifier qu'on a bien construit ainsi un anneau à deux éléments. On le note $\mathbb{Z}/2\mathbb{Z}$.

Exercice 4. Considérons un ensemble à trois éléments $\{0, 1, 2\}$. Montrer qu'il n'existe qu'au plus une façon de construire une table d'addition et de multiplication qui donne une structure d'anneau.

Correction 4. L'addition avec 0 est entièrement déterminée: $0 + a = a$ pour tout a. Pour l'addition avec 1, il faut trouver les valeurs possibles pour $1 + 1$ et $1 + 2$. Si $1 + 1 = 1$, après addition de l'inverse -1 de 1 pour l'addition, on obtient $1 = 0$, ce qui est exclu. Si $1 + 1 = 0$, alors l'inverse -2 de 2 ne pourrait être 1 ni 0 car ces nombres sont les inverses respectifs de 1 et 0. Donc l'inverse -2 de 2 serait 2, ie. $2 + 2 = 0$. Mais alors on ne peut pas donner de valeur raisonnable à $2 + 1$: pas 0 car 1 et 2 ne sont pas inverses, pas 1 car $2 \neq 0$ et pas 2 car $1 \neq 0$. La contradiction ne peut être levée que si $1 + 1 \neq 0$. La seule possibilité restante est donc $1 + 1 = 2$. En particulier, 1 n'est pas son propre inverse. L'élément 1 doit avoir un inverse -1 qui ne peut être ni 0, ni 1, donc c'est 2: $1 + 2 = 0$. Il reste à déterminer $2 + 2$: $2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 0 + 1 = 1$. La table d'addition est maintenant entièrement déterminée.
Pour la table de multiplication, la multiplication avec 0 est connue: on a vu dans un exercice précédent que dans un anneau $0.a = 0$ pour tout élément a. Par définition du neutre multiplicatif 1, $1a = a$. Il reste uniquement à déterminer 2.2: $2.2 = (1 + 1).2 = (1.2) + (1.2) = 2 + 2 = 1$. D'où les tables:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

,

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Toujours plus haut, si l'on essaye à présent de construire un anneau à quatre éléments on trouve plusieurs anneaux possibles. Voici les deux plus simples, que l'on note traditionnellement $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et dont les

tables respectives sont:

$\mathbb{Z}/4\mathbb{Z}$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

,

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ou

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$:

+	(0,0)	(1,1)	(1,0)	(0,1)
(0,0)	(0,0)	(1,1)	(1,0)	(0,1)
(1,1)	(1,1)	(0,0)	(0,1)	(1,0)
(1,0)	(1,0)	(0,1)	(0,0)	(1,1)
(0,1)	(0,1)	(1,0)	(1,1)	(0,0)

,

.	(0,0)	(1,1)	(1,0)	(0,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(1,0)	(0,1)
(1,0)	(0,0)	(1,0)	(1,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)

Exercice 5. Trouver qui est l'élément 0 et l'élément 1 dans l'anneau $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Correction 5. Le neutre 0 pour l'addition est $(0,0)$ tandis que le neutre 1 pour la multiplication est $(1,1)$.

Notation 2. *On s'aperçoit sur ces exemples que* 0 *est une notation symbolique. En fait il y a un element* 0 *dans* $\mathbb{Z}$ *et un élément* 0 *dans* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ *qui sont différents. La notation* 0 *désigne simplement le neutre pour l'addition de l'anneau considéré. Parfois, on aura envie de bien préciser de quel* 0 *on parle et on utilisera la notation plus précise* 0_A *pour signifier l'élément neutre de l'anneau* A*. De même, on emploiera occasionnellement la notation* 1_A*.*

On peut se demander si les deux anneaux sont vraiment différents. Est-ce que l'on n'a pas simplement changé les noms des éléments ? Par exemple en remplaçant 0 par $(0,0)$, 1 par $(1,1)$ etc... ou tout autre traduction.

Exercice 6. Montrer que les anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ne diffèrent pas l'un de l'autre par un simple changement de nom des éléments.

Correction 6. Dans $\mathbb{Z}/4\mathbb{Z}$, il y a un élément a de carré $a^2 = 0$, à savoir $a = 2$. Dans $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, il n'y a pas de tel élément comme on le vérifie en regardant dans les tables écrites dans le cours. Les deux anneaux sont donc vraiment différents puisque l'un deux a une propriété que l'autre n'a pas.

Ces exemples peuvent sembler à première vue un peu artificiels. On verra dans la suite du cours qu'ils ne le sont pas, et qu'ils peuvent par exemple être très utiles dans des problèmes de cryptographie. Mais relativement à votre savoir actuel, y a-t-il d'autres ensemble qui sont des anneaux, ie. dans lesquels vous utilisez une addition et une multiplication en utilisant implicitement les propriétés énumérées dans la définition 1 ? La réponse est oui.

Exemple 3. *Les ensembles suivants sont des anneaux.*

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- *les anneaux de polynômes* $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$
- *les fonctions de* $\mathbb{R}$ *dans* $\mathbb{R}$.

Exercice 7. Vérifier pour chacun des exemples $\mathbb{Q}, \mathbb{C}, \mathbb{Q}[X]$ fonctions de $\mathbb{R}$ dans $\mathbb{R}$, que vous savez qui sont les éléments 0 et 1 et que vous comprenez comment on fait la multiplication, l'addition et qui est l'élément $-a$ associé à un élément a.

Correction 7. Additionner ou multiplier des fractions, des complexes, ou des polynômes ne doit pas poser de problèmes. La seule difficulté concerne les fonctions. Si f et g sont deux fonctions, on définit leur somme $f + g$ par sa valeur en tout point: $(f + g)(x) = f(x) + g(x)$ et de même pour la multiplication. Le neutre pour l'addition est la fonction constante égale à 0 tandis que le neutre pour la multiplication est la fonction constante égale à 1. La fonction $-f$ inverse de la fonction f est celle qui en tout point x prend la valeur $-f(x)$.

Le premier des deux exemples d'un anneau à quatre éléments $(\mathbb{Z}/4\mathbb{Z})$ se généralise pour construire un anneau à n éléments. Essentiellement, dans $\mathbb{Z}/4\mathbb{Z}$, les tables se calculent en faisant comme si l'on travaillait avec les restes des divisions par quatre. Par exemple, on voit dans la table d'addition que $3 + 3 = 2$. En fait, on a calculé $3 + 3 = 6$, puis pris le reste de la division de 6 par 4, qui est deux. Les mêmes règles permettent de calculer les multiplications. On peut essayer de construire sur ce modèle un anneau à six éléments, qu'on note $\mathbb{Z}/6\mathbb{Z}$. Ses éléments au nombre de 6 sont notés $\dot{0}, \dot{1}, \ldots, \dot{5}$. Je définis la somme et la multiplication par les formules $\dot{x} + \dot{y} =$ reste de la division par 6 de $x + y$. par $\dot{x}.\dot{y} =$ reste de la division par 6 de xy.

Exercice 8. Dresser la table d'addition et de multiplication de l'ensemble $\mathbb{Z}/6\mathbb{Z}$. Vérifier que les éléments $\dot{0}$ et $\dot{1}$ satisfont aux propriétés voulues dans un anneau. Vérifier avec $a = \dot{2}, b = \dot{3}, c = \dot{4}$ que la distributivité est vérifiée.

Correction 8.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

,

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

A l'aide de ces tables, on vérifie facilement que $a(b+c) = ab + ac = 0$.

On a vérifié dans l'exercice la distributivité pour un triplet (a, b, c) particulier. Pour s'assurer que les tables de $\mathbb{Z}/4\mathbb{Z}$ définissent bien un anneau, il faudrait vérifier la distributivité pour tous les triplets, puis vérifier encore toutes les autres propriétés intervenant dans la définition d'un anneau. Il semble un peu miraculeux que toutes ces propriétés soient vérifiées. En fait, on verra dans un chapitre suivant que la structure d'anneau résulte de ce que l'ensemble des multiples de 6, à savoir l'ensemble $6\mathbb{Z} = \{\dots, -12, -6, 0, 6, 12, \dots\}$ a des propriétés particulieres de stabilité par différence et par multiplication comme le montre l'exercice suivant:

Exercice 9. Vérifier que la différence entre deux multiples de 6 est encore un multiple de 6. De même, vérifier que le produit entre un multiple de 6 et un entier quelconque est encore un multiple de 6.

Correction 9. Si $a = 6x$ et $b = 6y$ sont deux multiples de 6, $a-b = 6(x-y)$ est un multiple de 6. Si c est quelconque, $ac = 6xc$ est bien un multiple de 6.

Ces propriétes sont si importantes qu'on leur donne un nom:

Définition 4. *ideal Un sous-ensemble non vide $I \subset A$ est un ideal de A si:*

- $\forall x, y \in I,\ x - y \in I$
- $\forall x \in I, \forall y \in A, xy \in A$

Ainsi $I = 6\mathbb{Z}$ est un idéal de $A = \mathbb{Z}$ d'après l'exercice précédent. Comme on le verra dans les cours prochains, c'est pour cette raison que l'ensembe $\mathbb{Z}/6\mathbb{Z}$ est un anneau. Plus généralement, quand on aura un anneau A et un idéal $I \subset A$, on pourra construire un anneau quotient A/I. On aura donc à notre disposition beaucoup de nouveaux exemples d'anneau.
De même, le deuxième exemple d'anneau à quatre éléments $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$

se généralise. Regardons sa construction. Pour calculer $(a, b) + (a', b')$, on a simplement calculé $(a + a', b + b')$, où la somme $a + a'$ (resp. $b + b'$) est la somme de deux éléments de $\mathbb{Z}/2\mathbb{Z}$. Par exemple $(0, 1) + (1, 1) = (1, 0)$. Autrement dit, on a fait la somme sur chaque composante. De même pour le produit qui a été fait composante par composante.

Définition-Proposition 5. *anneauProduit Soient A et B des anneaux. Soit $A \times B$ l'ensemble des couples (a, b), $a \in A, b \in B$. L'ensemble $A \times B$ muni de l'addition $(a, b) + (a', b') = (a + a', b + b')$ et de la multiplication $(a, b)(a', b') = (aa', bb')$ est un anneau dont le neutre pour l'addition est $(0_A, 0_B)$ et le neutre pour la multiplication est $(1_A, 1_B)$. On l'appelle anneau produit de A et de B.*

Pour se familiariser avec cette notion, une vérification facile:

Exercice 10. Ecrire les tables d'addition et de multiplication de l'anneau produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Correction 10.

+	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(0,0)	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(1,1)	(1,1)	(0,2)	(1,2)	(1,0)	(2,1)	(0,0)
(0,1)	(0,1)	(1,2)	(0,2)	(0,0)	(1,1)	(1,0)
(0,2))	(0,2)	(1,0)	(0,0)	(0,1)	(1,2)	(1,1)
(1,0)	(1,0)	(0,1)	(1,1)	(1,2)	(0,0)	(0,2)
(1,2)	(1,2)	(0,0)	(1,0)	(1,1)	(0,2)	(0,1)

.	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(0,1)	(0,0)	(0,1)	(0,1)	(0,2)	(0,0)	(0,2)
(0,2)	(0,0)	(0,2)	(0,2)	(0,1)	(0,0)	(0,1)
(1,0)	(0,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)
(1,2)	(0,0)	(1,2)	(0,2)	(0,1)	(1,0)	(1,1)

Exercice 11. Vérifier que les lois d'addition et de multiplication données sur le produit $A \times B$ définissent bien un anneau.

Correction 11. La liste de toutes les vérifications est longue et montrons par exemple la distributivité et l'existence d'un inverse pour l'addition. Soit $(a, b) \in A \times B$. L'addition $(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0_A, 0_B)$ montre que (a, b) admet bien un inverse, à savoir $(-a, -b)$. Pour

la distributivité, il faut voir $(a_1, b_1)((a_2, b_2) + (a_3, b_3)) = (a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3)$. Or

$$\begin{aligned}(a_1, b_1)((a_2, b_2) + (a_3, b_3)) &= (a_1, b_1)((a_2 + a_3, b_2 + b_3)) \\ &= (a_1(a_2 + a_3), b_1(b_2 + b_3)) \\ &= (a_1a_2 + a_1a_3, b_1b_2 + b_1b_3) \\ &= (a_1a_2, b_1b_2) + (a_1a_3, b_1b_3) \\ &= (a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3)\end{aligned}$$

Ce procédé nous permet également de construire de nouveaux anneaux à partir des anneaux que nous connaissons.
Citons enfin une dernière manière de construire des anneaux qui consiste à prendre des sous-ensembles de A ayant des propriétés particulières.

Définition 6. *Un sous-ensemble B d'un anneau A est appelé sous-anneau s'il vérifie les conditions suivantes:*

- $1 \in B$
- $\forall a, b \in B,\ a + b \in B$
- $\forall a \in B, -a \in B$
- $\forall a, b \in B,\ ab \in B$

Étant donnés deux éléments de B, je peux les regarder en particulier comme des éléments de A puisque $B \subset A$. Je peux les ajouter puisque A est un anneau, et le résultat se trouve être un élément de B d'après la définition d'un sous-anneau. On a donc défini une addition sur B. De même, on peut définir une multiplication et un passage à l'inverse pour l'addition.

Définition 7. *induit On dit que l'addition et la multiplication sur B sont induites par celles sur A.*

La compatibilité entre la multiplication et l'addition (distributivité) et autres conditions (associativité,commutativité de l'addition) nécéssaires pour être un anneau sont vraies sur A. Étant donné que sur B, l'addition et la multiplication sont les mêmes que sur A, elles sont également vérifiées sur B. De plus B contient 1 et $0 = 1 - 1$. On a donc finalement:

Proposition 8. *Si B est un sous-anneau de l'anneau A, alors B muni des opérations induites par celles de A est un anneau.*

Exercice 12.
a)Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.
b)Est-ce que $\mathbb{Z}[x^n]$ est un sous-anneau de $\mathbb{Z}[x]$, où $\mathbb{Z}[x^n]$ est par définition l'ensemble des polynômes $\sum a_i x^i$ pour lesquels $a_i \neq 0 \Rightarrow i$ est un multiple de n ?
c)Est-ce que les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ qui s'annulent au point $x = 3$ forment un sous-anneau de l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$?

Correction 12.
a)Un sous-anneau de $\mathbb{Z}$ doit contenir 0 et 1 par définition, donc aussi $\underbrace{1 + \cdots + 1}_{n\ fois} = n$. Donc il contient tous les nombres positifs. Mais s'il contient un nombre positif n, il contient aussi son inverse $-n$. Donc un sous-anneau de $\mathbb{Z}$ contient tous les éléments de $\mathbb{Z}$, il est égal à $\mathbb{Z}$.
b)Les polynômes constants 0 et 1 sont bien dans $\mathbb{Z}[x^n]$. Soient deux polynômes $P = \sum a_i x^{in}$ et $Q = \sum b_i x^{in} \in \mathbb{Z}[x^n]$. Alors $-P = \sum -a_i x^{in}$ est bien dans $\mathbb{Z}[x^n]$ ainsi que $P + Q = \sum (a_i + b_i) x^{in}$. Donc $\mathbb{Z}[x^n] \subset \mathbb{Z}[x]$ est un sous-anneau.
c)Non, les fonctions s'annulant en trois ne forment pas un sous-anneau puisque la fonction constante 1 (le neutre multiplicatif) n'est pas dans cet ensemble.

Nous avons dit que la structure d'anneau était une structure qui nous permettait de faire des calculs comme avec les entiers. On termine par un exercice qui liste des propriétés auxquelles on est habitué avec les entiers et qui sont vraies dans les anneaux. Nous les utiliserons tout au long de ce cours

Exercice 13. Vérifier que les propriétés suivantes sont vérifiées dans tout anneau.

- $0x = 0$
- l'inverse $-a$ est unique ie. $a + b = a + c = 0 \Rightarrow b = c$.
- $-1.a + a = 0$

Correction 13. Le premier point a déjà été vérifié dans l'exercice où l'on a trouvé la seule structure possible d'anneau sur un ensemble à trois éléments. Reproduisons l'argument qui montre que $0.a$ vaut toujours 0. Puisque $0a = (0+0)a = 0a + 0a$, en ajoutant $-(0a)$ de chaque côté de l'égalité, on trouve $0 = 0.a$.
Pour montrer que l'inverse est unique, si $a+b = a+c$, on obtient en ajoutant l'inverse $-a$ des deux côtés de l'égalité la relation voulue $b = c$. Enfin, pour le troisième point, $-1.a + a = -1.a + 1.a = (-1 + 1).a = 0.a = 0$.

1.2 Morphismes d'anneaux

Nous avons expliqué dans la section précédente que nous avons des anneaux de base (entiers, polynômes), puis des procédés de construction qui permettent de construire de nouveaux anneaux à partir de ces anneaux de base (quotients, produits, sous-anneaux). Tous ces anneaux peuvent être reliés entre eux par des applications. Bien évidemment, si A et B sont deux anneaux et si $f : A \to B$ est une application qui les relie, on aimerait que f soit en un sens "compatible" avec la structure d'anneau de A et B, c'est à dire qu'on aimerait que f ait des propriétés particulières relativement aux symboles $0, 1, +, ., -$ apparaissant dans les anneaux. C'est la notion de morphisme d'anneaux.

Définition 9. *morphisme Soit A et B deux anneaux. Un morphisme d'anneaux $f : A \to B$ est une application qui satisfait au propriétés suivantes:*

- *f(1)=1*
- *f(0)=0*
- *f(x+y)=f(x)+f(y)*
- *f(-x)=-f(x)*
- *f(xy)=f(x)f(y)*

Très souvent, on trouve dans les livres la définition suivante:

Définition 10. *Soit A et B deux anneaux. Un morphisme d'anneaux $f : A \to B$ est une application qui satisfait aux propriétés suivantes:*

- *f(1)=1*
- *f(x-y)=f(x)-f(y)*
- *f(xy)=f(x)f(y)*

Ou encore:

Définition 11. *Soit A et B deux anneaux. Un morphisme d'anneau $f : A \to B$ est une application qui satisfait au propriétés suivantes:*

- *f(1)=1*
- *f(0)=0*
- *f(x+y)=f(x)+f(y)*
- *f(xy)=f(x)f(y)*

Ces définitions sont bien sûr équivalentes. Les définitions alternatives ont l'avantage d'être plus courtes. La définition adoptée dans ce cours a

l'avantage d'être plus naturelle: pour chacun des symboles intervenant dans la définition d'un anneau, on a une relation correspondante.

Remarque 12. *On peut montrer facilement que $f(x+y+z) = f(x) + f(y) + f(z)$ pour un morphisme d'anneaux et plus généralement, montrer par récurrence que $f(x_1) + \cdots + f(x_n) = f(x_1 + \cdots + x_n)$. On a également des énoncés équivalents pour la multiplication.*

Concrétisons la notion de morphisme d'anneaux sur un exemple. Essayons de comprendre quels sont les morphismes d'anneaux f de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$. Pour l'image de 0 et de 1, on n'a pas le choix par définition: $f(0) = 0$ et $f(1) = 1$. Mais alors $f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 0$. Et $f(3) = f(2+1) = f(2) + f(1) = 1 + 0 = 1$. En continuant ainsi, on montre facilement par récurrence $f(n) = \underbrace{1 + \cdots + 1}_{n \text{ fois}}$ pour n positif. Si n est pair, $f(n) = 0$ et si n est impair $f(n) = 1$. D'autre part, pour un nombre négatif $(-n)$, l'égalité $f(n) + f(-n) = f(n-n) = f(0) = 0$ montre que $f(-n) = -f(n)$, c'est à dire 0 si n est pair, et -1 si n est impair. Or $-1 = 1$ dans $\mathbb{Z}/2\mathbb{Z}$. Autrement dit, nous avons montré qu'il existait au plus un morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$, à savoir l'application qui à n associe 0 si n est pair, et qui associe 1 si n est impair. On peut vérifier qu'on a en fait bien défini un morphisme d'anneau.

Notation 13. *Soit A un anneau. On note $n.1$ l'élément $\underbrace{1 + \cdots + 1}_{n \text{ fois}} \in A$ et on note $-n.1$ son opposé dans A. Par convention $0.1_A = 0_A$.*

Ces notations ont été choisies de façon à se rappeler les formules $1.1_A = 1_A$, $n.1 + p.1 = (n+p).1$ et $(n.1)(p.1) = (np).1$, ce qui se vérifie aisément. On peut généraliser l'étude précédente:

Théorème 14. *Soit A un anneau. Il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$. Ce morphisme est défini par les formules $f(n) = n.1$ et $f(-n) = -n.1$ pour n positif.*

Démonstration. L'unicité se démontre exactement comme dans l'exemple. On n'a pas le choix pour $f(1)$, puis pour $f(2), f(3)$, puis pour $f(n)$ et $f(-n)$. De plus, ce raisonnement montre que nécéssairement $f(n) = n.1$ et $f(-n) = -n.1$. Donc, il y a au plus un morphisme qui est celui donné par les formules. Pour l'existence, il reste à vérifier que les formules définissent bien un morphisme d'anneau. On a bien $f(1) = 1$ et $f(0) = 0$ par les formules. Il faut vérifier maintenant $f(x+y) = f(x) + f(y)$, $f(xy) = f(x).f(y)$ et

$f(-x) = -f(x)$. Ces trois vérifications se ressemblent et nous ne ferons que la première. On a $f(x+y) = (x+y).1$ et $f(x) + f(y) = x.1 + y.1$. On a donc bien $f(x+y) = f(x) + f(y)$. ■

Exercice 14. Soit f l'unique morphisme $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Que valent $f(5)$ et $f(-2)$?

Correction 14. L'élément $f(5)$ vaut 1 et $f(-2)$ vaut 2.

On appelle propriété universelle d'un anneau B une caractérisation des morphismes de B dans un autre anneau ou des morphismes d'un autre anneau dans B. Dans le cas de $B = \mathbb{Z}$, la propriété universelle dit que pour tout anneau A, il existe un unique morphisme $\mathbb{Z} \to A$ et que celui-ci est donné explicitement par la formule précédente.
Une propriété importante des morphismes d'anneaux est qu'ils sont stables par composition.

Proposition 15. *Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux, alors la composition $g \circ f : A \to C$ est un morphisme d'anneaux.*

Démonstration. C'est une vérification facile que nous omettrons. ■

Un cas particulier très important de morphisme d'anneaux est la notion d'isomorphisme, dont la signification sera expliquée au chapitre suivant.

Définition-Proposition 16. *Un isomorphisme d'anneaux est un morphisme $f : A \to B$ qui est bijectif. On vérifie que l'application inverse f^{-1} est aussi un morphisme d'anneaux.*

1.3 Objectifs du cours

On sait à présent ce qu'est un anneau et, à partir des exemples de base (entiers,complexes,polynômes), on sait construire par produit, par quotient ou par sous-anneau de nombreux nouveaux exemples. Voici un certain nombre de problèmes dont la formulation inclut des opérations d'addition et de multiplication, donc implicitement des anneaux, et qui se résolvent par des raisonnements dans des anneaux bien choisis.

- Montrer que tout entier n se décompose en produit de nombre premiers: $n = n_1 . . . . n_r$.

- Peut-on décomposer de la même façon un polynôme en produit de polynômes premiers par analogie avec les entiers ? Est-ce qu'une telle décomposition est unique ? Comment la calculer ?
- Quels sont les nombres entiers x qui s'écrivent comme somme de 2 carrés $x = n_1^2 + n_2^2$?

Le but de ce cours est de donner une réponse à ces questions, et plus généralement, de présenter une théorie des anneaux qui permette de répondre à des problèmes de théorie des nombres. Nous donnerons également une application de ces théories "dans la vie courante", en cryptographie.
Les méthodes pour atteindre ces buts sont celles qui ont été suggérées dans ce premier chapître. Il conviendra d'introduire les anneaux adaptés aux problèmes que l'on veut résoudre et d'étudier ces anneaux, c'est à dire comprendre leurs idéaux et leur propriété universelle.

Chapitre 2

L'anneau $\mathbb{Z}$

Objectif: Nous avons appris au collège un certain nombre de propriétés sur les entiers naturels: décomposition en nombre premiers, existence de ppcm et de pgcd, méthodes de calcul du ppcm et du pgcd ... Bien sûr, seules des techniques de calcul étaient enseignées, sans la moindre démonstration. Dans ce chapitre, nous allons donner des démonstrations de ces faits bien connus. Nous allons également donner un algorithme de calcul du pgcd et du ppcm plus rapide que les algorithmes élémentaires enseignés au collège. Le point clé pour tout cela est de quitter l'ensemble $\mathbb{N}$ des entiers naturels qui n'est pas assez riche et de travailler plutôt dans $\mathbb{Z}$, qui est muni d'une structure d'anneau. La clé de voute des démonstrations est la compréhension des idéaux de $\mathbb{Z}$.

2.1 Décomposition en irréductibles dans un anneau

Dans $\mathbb{N}$, comme on l'a dit, il existe une décomposition des entiers en produits de nombres premiers, par exemple $28 = 2.2.7$ où l'on décrète par définition qu'un nombre est premier s'il n'est divisible que par 1 et lui-même. En fait tous les nombres ne peuvent pas se décomposer. En effet, on ne peut décomposer le nombre 0 car si $0 = n_1 n_2 \dots n_k$, l'un des n_i doit être nul. Mais c'est impossible car les n_i doivent être des nombres premiers, et 0 n'est pas premier. Donc le théorème que l'on pressent est que tout nombre entier non nul se décompose en produit de nombres premiers. Cette décomposition est elle unique ? Remarquons qu'on peut aussi écrire $28 = 1.2.2.7$, donc la décomposition n'est pas unique. On choisit par convention de dire que 1 n'est pas premier, ce qui élimine ce problème. Donc la définition d'un

nombre premier est finalement:

Définition 17. *Un nombre entier positif est premier s'il est différent de* 1 *et s'il n'est divisible que par* 1 *et lui-même.*

En ayant éliminé ce problème lié au nombre 1, a-t-on maintenant unicité de la décomposition ? Pas tout à fait, mais presque. On peut juste changer l'ordre des facteurs. Par exemple, $28 = 2.2.7 = 2.7.2$.
En éliminant le nombre 1 de la liste des nombres premiers, on a gagné l'unicité de la décomposition à l'ordre premier des facteurs près. En revanche, on ne peut plus décomposer le nombre 1 en produit de nombre premiers. Donc finalement, le théorème que l'on pourra démontrer est:

Théorème 18. *Tout nombre entier positif différent de* 0 *et de* 1 *se décompose en produit de nombre premiers et cette décomposition est unique à l'ordre des facteurs près.*

Pour établir ce théorème, nous allons en fait devoir travailler avec des entiers relatifs au lieu des entiers positifs. C'est une démarche un peu surprenante mais assez courante en mathématiques. On ne sait pas démontrer un résultat alors on imagine un problème plus large. Ici, par exemple, nous allons essayer de décomposer tous les nombres de $\mathbb{Z}$ au lieu de décomposer seulement les nombres positifs de $\mathbb{N}$. L'avantage espèré est que l'on dispose de structures supplémentaires pour le problème plus large qui facilitent l'étude. Dans notre cas, $\mathbb{Z}$ est muni d'une structure d'anneau qui n'existe pas sur $\mathbb{N}$.
Plaçons nous donc sur $\mathbb{Z}$ et essayons d'imaginer un théorème qui généralise le théorème de décomposition énoncé ci-dessus pour $\mathbb{N}$.
Tout d'abord par quoi remplacer la notion de nombre premier dans $\mathbb{Z}$? Dans $\mathbb{Z}$, 5 est divisible par $1, -1, 5, -5$. De même, -5 est divisible par $1, -1, 5, -5$. Donc on ne peut pas dire que les nombres qui nous intéressent sont les nombres qui ne sont divisibles que par un et par eux-mêmes. Ceux qui nous intéressent portent le nom d'éléments irréductibles.

Définition 19. *inversible Un élément a d'un anneau A est dit inversible (pour la multiplication) s'il existe un élément b tel que $ab = ba = 1$.*

Définition 20. *irreductible Un élément $a \in A$ est irréductible s'il est non inversible et si pour toute écriture $a = bc$, alors b ou c est inversible.*

Exercice 15.
a)Montrer que les inversibles de $\mathbb{Z}$ sont 1 et -1.
b)Montrer que pour un élément $z \in \mathbb{Z}$, les trois conditions suivantes sont équivalentes:

- z est irréductible
- z est différent de 1 et -1 et les seuls éléments qui divisent z sont $1, -1, z, -z$
- la valeur absolue $|z|$ de z est un nombre premier

Correction 15.
a)Les éléments 1 et -1 sont évidemment inversibles d'inverse respectif 1 et -1. L'élement nul n'est pas inversible: pour tout a, $0a = 0 \neq 1$. Enfin, un élément a différent de $0, 1, -1$ ne peut être inversible. En effet, en valeur absolue $|a| > 1 > 0$. Donc l'inverse b de a vérifie $0 < |b| = \frac{1}{|a|} < 1$ ce qui n'est pas possible puisque $b \in \mathbb{Z}$.
b)$1 \Rightarrow 2$. Si z est irréductible, il est différent de 1 et -1 puisque non inversible. Soit a un diviseur de z: $z = ab$. Si a est inversible alors $a = 1$ ou -1. Sinon, puisque z est irréductible, c'est b qui est inversible et qui vaut 1 ou -1. Dans ce cas a vaut z ou $-z$. Un diviseur a de z est donc bien dans l'ensemble $\{1, -1, z, -z\}$.
$2 \Rightarrow 3$. Par contraposée. Supposons que $|z|$ n'est pas un nombre premier, de sorte que $|z| = pq$ avec p et q différents de 1. Alors l'écriture $z = p\frac{z}{p}$ montre que z n'est pas irréductible car p et $\frac{z}{p}$ ne sont pas inversibles.
$3 \Rightarrow 1$. Soit z un nombre entier de valeur absolue un nombre premier. Montrons z irréductible. Soit $z = pq$ une écriture en produit. On a $|z| = |p||q|$ qui est une écriture du nombre premier $|z|$ en produit. Donc $|p|$ ou $|q|$ est égal à 1. C'est à dire que p (ou q) vaut plus ou moins 1 et est inversible.

En essence, la définition de a irréductible signifie que a ne peut pas s'écrire comme un produit non trivial. Plus précisément, on voit qu'on peut toujours écrire un élément a comme produit de deux éléments. En effet choisissons u et v tel que $uv = 1$. Alors $a = (uv)a = u(va)$. Mais ces décompositions sont des décompositions bêtes obtenues à partir de la décomposition du nombre 1. Cela se traduit par le fait que l'un des termes du produit est inversible. Le fait d'être irréductible dit donc en substance que les seules décompositions qui peuvent arriver sont les décompositions bêtes obtenues à partir de l'écriture de 1 comme un produit.
Comme l'exercice précédent l'a montré, les éléments irréductibles de $\mathbb{Z}$ sont donc ceux dont la valeur absolue est un nombre premier. Dans $\mathbb{N}$, on peut décomposer les éléments en produits de nombres premiers. De même dans $\mathbb{Z}$, on peut décomposer en produit d'irréductibles. Par exemple $-6 = 2.(-3)$. A-t-on existence et unicité d'une décomposition en irréductibles dans $\mathbb{Z}$. Non, tout d'abord les nombres $0, 1, -1$ ne peuvent pas se décomposer. Ensuite, même pour les décomposables comment choisir entre les différentes décompositions ? Par exemple entre $-6 = 2.(-3)$ et $-6 = 3.(-2)$? Et bien

on ne va pas choisir, on dira simplement que la décomposition est connue au signe près. Le théorème que l'on peut espérer est donc:

Théorème 21. *Tout élément non nul et non inversible $z \in \mathbb{Z}$ se décompose en produit d'éléments irréductibles et la décomposition est unique à l'ordre des facteurs et multiplication par des inversibles près. Plus précisément, cela signifie que si $z = p_1 \dots p_r = q_1 \dots q_s$ sont deux décompositions, alors $r = s$ et, quitte à intervertir les q_i, on a $p_i = \epsilon_i q_i$ où ϵ_i est inversible.*

On peut remarquer que la condition $p_i = \epsilon_i q_i$ où ϵ_i est inversible est une manière prétentieuse de dire que p_i est égal à q_i au signe près, puisque ϵ_i vaut 1 ou -1. La raison pour laquelle on a choisi cette formulation est qu'elle se généralisera à d'autres anneaux que $\mathbb{Z}$.

ExoTD 1.
c)*Montrer que les inversibles de $\mathbb{Q}[x]$ sont les polynômes constants non nuls.*
d)*Montrer qu'on ne peut pas remplacer $\mathbb{Q}$ par $\mathbb{Z}$ dans la question précédente. Par quoi peut on remplacer $\mathbb{Q}$?*

correcTD 1.
e)*Soit P est un polynôme inversible. Montrons que P est une constante. En effet, si Q est son inverse, $PQ = 1$. Donc par la formule des degrés, $deg(P) + deg(Q) = 0$. La seule possibilité est $deg(P) = deg(Q) = 0$, c'est à dire que P et Q sont des constantes non nulles. Réciproquement, si $P = p$ est une constante non nulle, il est clair que c'est un polynôme inversible d'inverse le polynôme constant $\frac{1}{p}$.*
f)*La constante $2 \in \mathbb{Z}[X]$ n'est pas inversible. On peut remplacer $\mathbb{Q}$ par un corps quelconque.*

ExoTD 2. *Montrer que si a est inversible et si $a = a_1 \dots . a_n$ est une décomposition de a sous forme d'un produit, alors tous les a_i sont inversibles.*

correcTD 2. *Par symétrie, il suffit de montrer que a_1 est inversible. Soit b l'inverse de a. L'écriture $1 = ab = a_1.(a_2 \dots a_n b)$ montre que a_1 est inversible d'inverse $a_2 \dots a_n b$.*

2.2 Idéaux de $\mathbb{Z}$

Le théorème annoncé s'obtient en étudiant les idéaux de $\mathbb{Z}$. On commence par quelques exemples.

2.2.1 Idéaux engendrés par un seul élément

Exercice 16.
a)Montrer que l'ensemble $12\mathbb{Z} = \{\dots, -24, -12, 0, 12, 24, \dots\}$ est un idéal de $\mathbb{Z}$. On le désignera par le symbole (12).
b)Donner un idéal plus grand que (12) au sens de l'inclusion.
c)Montrer que l'ensemble $12\mathbb{Z}$ est le plus petit idéal de $\mathbb{Z}$ contenant le nombre 12.
d)Donner sans démonstration une généralisation de cet énoncé.
e)Montrer que $(12) = (-12)$.
f)Y a-t-il d'autres a tels que $(12) = (a)$?

Correction 16.
a)Si $a = 12x$ et $b = 12y$ sont deux multiples de 12, $a - b = 12(x - y)$ est un multiple de 12. Si c est quelconque, $ac = 12xc$ est bien un multiple de 12.
b)L'idéal $(6) = \{\dots, -24, -18, -12, -6, 0, 6, 12, 18, 24, \dots\}$ est plus grand que (12).
c)Si un idéal contient le nombre 12, il contient tous les multiples $12a$ de 12 par définition d'un idéal, ie. il contient $12\mathbb{Z} = (12)$.
d)L'idéal (a) est le plus petit idéal contenant le nombre a.
e)Puisque (12) contient le nombre -12, il contient le plus petit idéal contenant le nombre -12, à savoir (-12), ie. $(12) \supset (-12)$. Par symétrie $(-12) \supset (12)$ et donc finalement $(12) = (-12)$.
f)Si a est un nombre tel que $(12) = (a)$. Puisque $a \in (a)$, on a $a \in (12)$, c'est à dire par définition de 12, $a = 12b$. Par symétrie entre a et 12, il existe c tel que $12 = ac$. D'où $12 = 12bc$, c'est à dire $bc = 1$. Comme b et c sont dans $\mathbb{Z}$, il faut que b et c valent plus ou moins 1. C'est à dire $a = 12$ ou -12. Les seuls nombres a tels que $(a) = (12)$ sont donc 12 et -12.

Cette étude faite pour l'idéal (12) se généralise aux idéaux (a).

Notation 22. *Soit A un anneau et $a \in A$. On note (a) l'ensemble des multiples de a.*

Définition 23. *On dit que a divise b dans A s'il existe $c \in A$ tel que $b = ac$.*

Exemple 24. *Le nombre 5 divise 12 dans $\mathbb{Q}$ mais pas dans $\mathbb{Z}$.*

Proposition 25.
- *(a) est un idéal de A*
- *(a) est le plus petit idéal de A contenant a.*
- *$(a) \subset (b)$ ssi b divise a.*

Démonstration. Soient x et y deux eléments de (a) , ie. $x = \lambda a$ et $y = \mu a$. Soit $z \in A$. Il nous faut montrer $x - y \in (a)$ et $xz \in (a)$ pour voir que (a) est un idéal. Les égalités $x - y = (\lambda - \mu)a$ et $xz = (\lambda z)a$ montrent que ce sont bien des multiples de a.
Si un idéal I de A contient a, il contient nécéssairement tous les multiples de a par définition (puisque $a \in I \Rightarrow ax \in I$ pour tout x) donc il contient (a). Tout ideal I contenant l'élément a contient l'ideal (a): (a) est bien le plus petit idéal contenant a.
Si b divise a, tout multiple de a est un multiple de b. Donc $(a) \subset (b)$. Réciproquement, si $(a) \subset (b)$, puisque $a \in (a)$, alors $a \in (b)$. Par définition de (b), cela signifie qu'il existe λ avec $a = b\lambda$. Donc b divise a. ■

Essayons de comprendre quels sont les éléments b tels que $(b) = (a)$? Si $(b) = (a)$, alors $b = \lambda a$ et $a = \mu b$. Donc $b = \lambda\mu b$. On aimerait simplifier par b si b est non nul et dire que $\lambda\mu = 1$.

Exercice 17. Trouver un exemple dans la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$ qui montre qu'on peut avoir $b = \lambda\mu b$ sans avoir $\lambda\mu = 1$ ou $b = 0$.

Correction 17. On a $2 = 3.1.2$.

Donc dans $\mathbb{Z}$ on peut simplifier, mais dans un anneau général, on ne le peut pas. Quels sont les anneaux dans lesquels on peut faire des simplifications pour la multiplication ie tq. $ab = ac$ *et* $a \neq 0 \Rightarrow b = c$?

Proposition 26. *Soit A un anneau. Les conditions suivantes sont équivalentes:*

- *On peut simplifier dans A par tous les éléments non nuls ie.* $(ab = ac$ *et* $a \neq 0) \Rightarrow b = c$
- *Pour tout couple (a, b) avec $a \neq 0$ et $b \neq 0$, on a $ab \neq 0$*

Démonstration. Si on peut simplifier dans A, montrons que $ab = 0$ implique $a = 0$ ou $b = 0$. Si $ab = 0 = 0a$ et $a \neq 0$, en simplifiant par a, on obtient $b = 0$.
Réciproquement, supposons que $ab = 0 \Rightarrow a = 0$ *ou* $b = 0$. Supposons $ab = ac$. Montrons qu'on peut simplifier ie. que $b = c$. Puisque $a(b-c) = 0$, et puisque $a \neq 0$, il faut $b - c = 0$ donc $b = c$. ■

Définition 27. *intègre Un anneau vérifiant l'une des deux conditions équivalentes ci-dessus est appelé un anneau intègre.*

Exercice 18. Si A est un anneau non intègre et $a \in A$, donner une condition sur a pour qu'on puisse simplifier par a (examiner la démonstration faite pour caractériser les anneaux intègres).

Correction 18. On peut simplifier dans un anneau par un élément a (ie. $ab = ac \Rightarrow b = c$) si a n'est pas diviseur de 0, ie. si le seul d tel que $ad = 0$ est $d = 0$.

Définition 28. *Deux éléments a et b d'un anneau sont associés s'il existe un inversible c tel que $a = bc$.*

Remarque 29. *C'est une relation symétrique puisque $b = a(c^{-1})$.*

On a vu dans l'exercice introductif que $(12) = (-12)$ et qu'il n'y avait pas d'autre nombre tel que $(12) = (a)$. L'exercice suivant donne un énoncé généralisant cet exemple et valable dans tous les anneaux intègres.

Exercice 19.
a)Montrer que deux idéaux (a) et (b) dans un anneau intègre A sont égaux ssi a et b sont associés.
b)En particulier si $A = \mathbb{Z}$, les éléments b tels que $(a) = (b)$ sont $b = a$ et $b = -a$.

Correction 19.
a)Supposons $(a) = (b)$. Si $a = b = 0$, a et b sont associés. Sinon, on peut supposer par symétrie entre a et b que $b \neq 0$. Puisque $a \in (a)$, on a $a \in (b)$, c'est à dire par définition de (b), $a = bc$ pour un certain c. Par symétrie entre a et b, il existe d tel que $b = ad$. D'où $b = bcd$. Comme l'anneau est intègre, on peut simplifier par $b \neq 0$, d'où $cd = 1$. Comme c et d sont inversibles a et b sont associés. Réciproquement, si a et b sont associés montrons $(a) = (b)$. Par symétrie il suffit de montrer $(a) \subset (b)$. Comme il existe c inversible tel que $a = bc$, $a \in (b)$ par définition de (b). Comme (b) est un idéal, s'il contient a, il contient tous les multiples de a, c'est à dire que $(a) \subset (b)$.
b)Dans le cas de $\mathbb{Z}$, si $(a) = (b)$ on a d'après ce qui précède, $a = bc$ avec c inversible. Mais les inversibles de $\mathbb{Z}$ sont 1 et -1. Donc $b = a$ ou $b = -a$.

Exercice 20. Les propositions suivantes sont elles équivalentes ?

- a et b sont associés
- a divise b et b divise a.

Correction 20. Dans un anneau intègre, les propositions sont équivalentes. En effet a divise b et b divise a peut se traduire par $(b) \subset (a)$ et $(a) \subset (b)$, c'est à dire par $(a) = (b)$. Mais d'après l'exercice précédent, $(a) = (b)$ ssi a et b sont associés (dans un anneau intègre).

On a donc étudié dans cette section les idéaux (a) engendrés par un élément a. Ces idéaux sont importants, et on leur donne un nom:

Définition 30. *principa Un idéal $I \subset A$ est dit principal s'il est de la forme (a) pour un élément $a \in A$.*

2.2.2 Les idéaux de $\mathbb{Z}$ sont principaux

On a vu dans la section précédente que le plus petit idéal contenant a est l'ensemble (a) formé des multiples de a. Montrez plus généralement le résultat suivant.

Exercice 21.
a)Le plus petit idéal d'un anneau A contenant les éléments a et b est l'ensemble (a, b), où la notation (a, b) est une convention pour désigner l'ensemble $\{r \in A, \exists x, y \in A \text{ t.q. } r = ax + by\}$ contenant les éléments r qui sont somme d'un multiple de a et d'un multiple de b.
b)Énoncer sans démonstration une généralisation décrivant le plus petit idéal contenant des éléments $a_1, \ldots, a_n$.

Correction 21.
a)Si un idéal contient les éléments a et b, alors puisqu'un idéal est stable par multiplication par un élément quelconque, il contient nécéssairement les nombres ax et by, et comme un idéal est stable par somme, il contient $ax+by$ (pour tout x, y.). Donc un idéal contenant a et b contient (a, b). On aura gagné si on montre que (a, b) est un idéal. Si $m = ax + by$ et $n = a'x + b'y$ sont deux éléments de (a, b), alors $m-n = (a-a')x+(b-b')y$ est bien dans (a, b). Si p est un élément quelconque $mp = (ap)x + (bp)y$ est dans (a, b). Donc on a fait les vérifications qui montrent que (a, b) est un idéal.
b)Le plus petit idéal contenant les éléments $a_1, \ldots, a_n$ est l'ensemble $(a_1, \ldots, a_n)$ qui contient les éléments $\{r \in A, \exists x_1, \ldots, x_n \in A \text{ t.q. } r = a_1x_1 + \cdots + a_nx_n\}$. Autrement dit, le plus petit idéal contenant les a_i est l'ensemble des combinaisons linéaires des a_i à coefficients dans A.

Définition 31. *On note $(a_1, \ldots, a_n)$ le plus petit idéal de A contenant les éléments $a_1, \ldots, a_n$. D'après l'exercice précédent, c'est aussi l'ensemble des éléments r t.q. il existe $x_1 \ldots, x_n \in A$ t.q. $r = a_1x_1 + \cdots + a_nx_n$.*

En fait, dans $\mathbb{Z}$, on n'a pas besoin de considérer les ideaux engendrés par un nombre fini d'éléments.

Proposition 32. *Pour tout ideal $I = (a_1, \ldots, a_n)$ de $\mathbb{Z}$, il existe un élément a tel que $I = (a)$.*

Commençons par quelques lemmes.

Lemme 33. *L'idéal I est le même si on change un nombre en son opposé. L'ideal I est le même si on supprime de la liste les a_i qui sont nuls.*

Démonstration. Montrons que $(a_1, a_2, \ldots, a_n) \subset (-a_1, a_2, \ldots, a_n)$. Un élément de $(a_1, a_2, \ldots, a_n)$ est par définition un élément r qui s'écrit $a_1x_1 + \ldots a_nx_n$. Donc il s'écrit aussi $(-a_1)(-x_1) + a_2x_2 + \ldots a_nx_n$, ce qui montre que $(a_1, a_2, \ldots, a_n) \subset (-a_1, a_2, \ldots, a_n)$. Par symétrie, on obtient $(-a_1, a_2, \ldots, a_n) \subset (a_1, a_2, \ldots, a_n)$, d'où l'égalité $(a_1, a_2, \ldots, a_n) = (-a_1, a_2, \ldots, a_n)$. Ce qu'on a fait pour l'élément a_1 se fait pour les autres a_i et on peut donc changer les signes des a_i sans changer l'idéal engendré. Montrer qu'on peut enlever les zeros se fait par un raisonnemnent du même type, en regardant la forme des éléments r de l'idéal. ■

On peut donc supposer tous les a_i positifs et non nuls.

Lemme 34. *Si $a = bq + r$ est une division dans $\mathbb{N}$, alors les ideaux $(a, b, a_3, \ldots, a_n)$ et $(b, r, a_3, \ldots, a_n)$ sont égaux.*

Démonstration. Montrons $(a, b, a_3, \ldots, a_n) \subset (b, r, a_3, \ldots, a_n)$. Un élément s de $(a, b, a_3, \ldots, a_n)$ s'écrit par définition sous la forme $s = ax_1 + bx_2 + a_3x_3 \ldots a_nx_n$. En écrivant $a = bq + r$, on obtient $s = b(qx_1 + x_2) + rx_1 + a_3x_3 + \ldots a_nx_n$, ce qui montre $s \in (b, r, a_3, \ldots, a_n)$. L'inclusion réciproque se montre de manière similaire. ■

Exemple 35. *Considerons l'idéal $(20, 15, 2)$. On a $20 = 1.15 + 5$ donc $(20, 15, 13) = (15, 5, 13)$. Comme $15 = 5.3 + 0$, $(15, 5, 13) = (5, 0, 13) = (5, 13)$. En continuant les divisions, $(5, 13) = (13, 5) = (5, 3) = (3, 2) = (2, 1) = (1, 0) = (1)$. Donc $(20, 15, 2) = (1) = \mathbb{Z}$.*

Exercice 22.
a)Calculer un générateur de l'idéal $(30, 36)$.
b)Calculer un générateur de l'idéal $(30, 36, 10)$.

Correction 22.
a)Les divisions $36 = 1.30 + 6$ et $30 = 5.6 + 0$ montrent que $(30, 36) = (30, 6) = (6)$. Un générateur est donc (6).
b)$(30, 36, 10) = (6, 10)$. Les divisions $10 = 1.6 + 4$, $6 = 1.4 + 2$, $4 = 2.2 + 0$ montrent que $(6, 10) = (6, 4) = (4, 2) = (2)$. Un générateur est donc (2).

Il est clair qu'on peut ainsi par divisions réduire le nombre de générateurs pour n'en avoir plus qu'un à la fin pourvu que le nombre de générateurs soit fini au départ, ce qui montre la proposition 32. En fait, pour montrer que tout idéal I est de la forme (a) sans supposer que I est engendré par un nombre fini d'éléments, il faut une preuve plus abstraite.

Théorème 36. *Tout idéal I de $\mathbb{Z}$ est principal.*

Démonstration. Si $I = \{0\}$, on a évidemment I principal engendré par 0. Sinon, I contient un élément i non nul et son inverse $-i$. Donc I contient un élément strictement positif. Soit a le plus petit élément strictement positif de I. On va montrer que I est principal en montrant $I = (a)$. Il est d'abord clair que $I \supset (a)$ puisque I contient a et que (a) est le plus petit idéal contenant a. Montrons réciproquement $I \subset (a)$. Soit donc $i \in I$. Il nous faut $i \in (a)$. Traitons d'abord le cas i positif. On fait la division $i = aq + r$. L'élement $r = i - aq \in I$ (pourquoi ?). Or $0 \leq r < a$ et a est minimal parmi les éléments positifs de I, donc c'est que r n'est pas positif: $r = 0$. D'où $i = aq$ et l'appartenance recherchée $i \in (a)$. Si i est négatif, $-i \in I$ donc est dans (a) par ce qui précède. Donc $i \in (a)$. ∎

2.2.3 Conséquences de la principalité

Le fait que les idéaux de $\mathbb{Z}$ soient principaux a de nombreuses conséquences, existence d'un ppcm, d'un pgcd, théorèmes de Bezout et de Gauss que nous allons détailler maintenant. Ce sont des étapes vers l'existence et l'unicité de la décomposition dans $\mathbb{Z}$.
Commençons par l'existence d'un plus grand commun diviseur (un pgcd) d'une famille de nombres. Ici attention, quand on veut dire plus grand, on parle au sens de la divisibilité. Par exemple, -6 et 3 sont deux diviseurs de 12. Le plus grand au sens usuel est 3, mais au sens de la divisibilité, c'est -6 car 3 divise -6.

Définition 37. *Soient a et b deux éléments d'un anneau intègre A. On dit que a est plus petit que b au sens de la divisibilité si $a|b$.*

Définition 38. *Soit $a_1, \ldots, a_n$ une famille de nombres. Un nombre $d \in \mathbb{Z}$ est un pgcd des a_i si*

- *d divise chaque a_i*
- *d est maximal pour cette propriété au sens de la divisibilité, ie. si x divise chaque a_i, alors x divise d.*

Définition 39. *Soit $a_1, \ldots, a_n$ une famille de nombres. Un nombre $d \in \mathbb{Z}$ est un plus petit commun multiple (ppcm) des a_i si*

- *d est un multiple de chaque a_i*
- *d est minimal pour cette propriété au sens de la divisibilité, ie. si x est un multiple de chaque a_i, alors d divise x.*

Comment calculer un pgcd ? Voici un critère.

Proposition 40. *Soit d un générateur de l'idéal $(a_1, \ldots, a_n)$ ie. un nombre tel que $(d) = (a_1, \ldots, a_n)$. Alors d est un pgcd des a_i.*

Démonstration. Montrons d'abord que d divise chaque a_i: puisque $a_i \in (a_1, \ldots, a_n) = (d)$, a_i est un multiple de d. Soit maintenant un élément x.Si x divise tous les a_i il divise d car $d \in (d) = (a_1, \ldots, a_n)$ donc d s'écrit $a_1x_1 + \ldots a_nx_n$. ∎

Exercice 23.
a)Si d est un pgcd des a_i dans $\mathbb{Z}$, quels sont les autres pgcd des a_i.
b)Plus généralement, même question dans un anneau principal et intègre quelconque.

Correction 23.
a)Un pgcd est un générateur a d'un idéal. Or on a vu qu'un nombre a tel que $(a) = I$ est défini au signe près dans $\mathbb{Z}$. Donc les deux pgcd possibles sont a et $-a$.
b)Dans un anneau intègre, on a vu en exercice que les générateurs d'un idéal sont définis à multiplication par un inversible près. Autrement dit, si a et b sont deux pgcd, il existe un élément c inversible tel que $a = bc$. (Remarque: puisque dans $\mathbb{Z}$, les inversibles sont 1 et -1, on retrouve bien le fait qu'un pgcd est défini au signe près).

Exercice 24. Calculer $pgcd(12, 20)$ avec cette définition de pgcd et vérifier que cela correspond à ce que vous attendiez.

Correction 24. Les divisions $20 = 1.12 + 8$, $12 = 1.8 + 4$, $8 = 2.4 + 0$ montrent que $(20, 12) = (12, 8) = (8, 4) = (4)$. Le pgcd (au signe près) est donc 4. Si on écrit les décompositions $20 = 2.2.5$ et $12 = 2.2.3$, on retrouve bien que les termes en commun sont $2.2 = 4$.

De même, la notion de ppcm est lié à la notion d'idéal. Il faut commencer par remarquer qu'une intersection d'idéaux de $\mathbb{Z}$ est encore un idéal.

Exercice 25. Si I_1,...,I_n sont des idéaux de A, alors l'intersection $I_1 \cap I_2 \cap \cdots \cap I_n$ est un idéal de A.

Correction 25. Si x et y sont dans I, ils sont dans chaque I_k par définition de l'intersection, donc $x-y$ est dans chaque I_k puisque I_k est un idéal, donc $x-y \in I$. Le même type de démonstration montre que si a est un élément quelconque $ax \in I$. Donc on a fait les vérifications qui montrent que I est un idéal.

Proposition 41. *Soient $a_1, \ldots, a_n$ des éléments de $\mathbb{Z}$ et m tel que $(m) = (a_1) \cap (a_2) \cdots \cap (a_n)$. Soit $x \in \mathbb{Z}$ alors x est un multiple de chaque a_i ssi x est un multiple de m. En particulier m est un ppcm des a_i.*

Démonstration. Si x est un multiple de chaque a_i, il appartient à chaque idéal (a_i), donc à l'intersection (m), donc c'est un multiple de m. Réciproquement, si x est un multiple de m, il est dans (m), donc dans chaque (a_i) puisque $(m) \subset (a_i)$, donc c'est un multiple de chaque a_i. ∎

On remarquera que tout comme le pgcd, le ppcm n'est défini qu'au signe près puisque les générateurs d'un idéal de $\mathbb{Z}$ ne sont définis qu'au signe près.

Définition 42. *Des éléments $a_1, \ldots, a_n \in \mathbb{Z}$ sont dits premiers entre eux si 1 est un pgcd des a_i.*

Un corollaire du fait que les idéaux sont principaux dans $\mathbb{Z}$ est que l'on peut caractériser les ensembles de nombres premiers entre eux par une égalité numérique.

Théorème 43. ***Théorème de Bezout.*** *Des éléments $a_i \in \mathbb{Z}$ sont premiers entre eux ssi il existe des $\lambda_i \in \mathbb{Z}$ tels que $\sum \lambda_i a_i = 1$*

Démonstration. Si les a_i sont premiers entre eux, 1 est un pgcd donc $(1) = (a_1, \ldots, a_n)$. Donc $1 \in (a_1, \ldots, a_n)$ ce qui donne l'écriture de 1 voulu. Réciproquement si $1 = \sum \lambda_i a_i$, alors $1 \in (a_1, \ldots, a_n)$, donc $(1) \subset (a_1, \ldots, a_n)$ puisque (1) est le plus petit idéal contenant 1. Mais l'inclusion réciproque $(a_1, \ldots, a_n) \subset (1) = \mathbb{Z}$ est évidente. D'où finalement $(1) = (a_1, \ldots, a_n)$. ∎

Cette caractérisation de Bezout nous permet de démontrer le corollaire suivant bien connu.

Corollaire 44. *Si a est premier avec b et avec c, alors a est premier avec bc.*

Démonstration. Si a est premier avec b, alors $1 = \lambda a + \mu b$. De même, $1 = \nu a + \rho c$. En multipliant les deux égalités membre à membre, on trouve une expression de la forme $1 = \alpha a + \beta bc$, ce qui montre que a et bc sont premiers entre eux. ■

Des exemples de nombres premiers entre eux sont facilement construits avec des nombres irréductibles.

Proposition 45. *Soit p un nombre irréductible et q un nombre non divisible par p. Alors p et q sont premiers entre eux.*

Démonstration. Soit $d = pgcd(p, q)$. On veut dire que d est inversible. Par définition du pgcd, on a l'égalité des idéaux $(d) = (p, q)$. L'élément p qui est dans le deuxième idéal est dans le premier et donc $p = d.\lambda$ pour un certain λ. En vertu de l'irréductibilité de p, soit d soit λ est inversible. Si c'est d, on a gagné. Il faut donc éliminer l'autre cas. Raisonnons par l'absurde. Supposons que λ est inversible, alors $d = p$ ou $-p$ et $(d) = (p)$. Mais alors q qui est dans (d) est aussi dans (p), donc divisible par p, ce qui est exclu par hypothèse. ■

Corollaire 46. ***Théorème de Gauss*** *Si a est premier avec b et divise bc, alors a divise c.*

Démonstration. Par le théorème de Bezout: $1 = \lambda a + \mu b$, d'où on tire $c = \lambda ac + \mu bc$. Puisque a divise ac et bc, il divise c. ■

ExoTD 3. *Vérifier que la relation être plus petit au sens de la divisibilité est une relation d'ordre sur $\mathbb{N}$.*

correcTD 3. *Rappelons que $\mathcal{R}$ est une relation d'ordre si elle vérifie les mêmes propriétés que la relation $\leq$, à savoir:*

- $x\mathcal{R}x$
- $x\mathcal{R}y$ *et* $y\mathcal{R}z \Rightarrow x\mathcal{R}z$
- $x\mathcal{R}y$ *et* $y\mathcal{R}x \Rightarrow x = y$

Pour la relation de divisibilité. Le premier point demande que x divise x. C'est vrai: $x = x.1$. Si x divise y et y divise z, ie. $y = kx$ et $z = ly$, alors $z = (lk)x$, ce qui montre que x divise z et donc le deuxième point. Enfin, si x divise y et y divise x, on a $y = kx$ et $x = ly$, donc $x = klx$. Si $x \neq 0$, on

a $kl = 1$*, et comme* k *et* l *sont positifs (on travaille dans* $\mathbb{N}$*), on a* $k = l = 1$ *donc* $x = y$*. Si* $x = 0$*,* $y = kx = 0 = x$ *également.*

2.3 Démonstration du théorème de décomposition

Dans la section précédente, nous avons établi les conséquences importantes de la principalité des idéaux de $\mathbb{Z}$, les theorèmes de Gauss et de Bezout. Nous allons maintenant utiliser ces résultats pour démontrer le théorème de factorisation dans $\mathbb{Z}$, existence et unicité. Commençons par l'existence. Prenons un nombre $z \in \mathbb{Z}$ non inversible et essayons de le décomposer en produit d'irréductibles. Soit z est irreductible et on a une décomposition triviale $z = z$ en produit d'irréductibles (où le terme de droite est vu comme un produit de 1 terme par convention). Sinon, par contraposition de la définition d'irréductibilité, cela signifie que z s'écrit sous la forme $z = z_1 z_2$ où aucun des deux z_i n'est inversible. Si chacun des z_i est irréductible, on a trouvé la décomposition en produit d'irréductibles. Sinon, on peut supposer par exemple que z_1 n'est pas irréductible et on peut écrire z_1 comme un produit de 2 éléments non inversibles:$z_1 = z_3.z_4$, d'où $z = z_2 z_3 z_4$. S'il existe un z_i non irréductible, on le casse de nouveau en deux pour obtenir un produit de 4 termes et ainsi de suite. J'affirme qu'au bout d'un nombre fini d'étapes, tous les nombres sont irréductibles et l'algorithme s'arrete (et nous donne donc la décomposition voulue de z). En effet, puisque chaque z_i est non inversible, leur valeur absolue vaut au moins 2. Donc si z s'écrit comme un produit de n termes, z vaut au moins $2n$. Donc le nombre de termes qui apparait dans la décomposition de z est au plus $[\frac{z}{2}]$, où [ ] désigne la partie entière.
Pour l'unicité, considérons deux décompositions $z = x_1 \dots x_n = y_1 \dots y_p$. La première égalité montre que x_1 divise z. Donc x_1 n'est pas premier avec z. Donc x_1 ne peut être premier avec tous les y_i en raison du corollaire 44. Quitte à réordonner les y_i, on peut supposer que x_1 n'est pas premier avec y_1. Mais cela ne se peut que quand x_1 divise y_1 d'après la proposition 45:$y_1 = x_1.q$. Comme y_1 est irréductible et que x_1 est non inversible on en déduit que q est inversible et que $y_1 = x_1$ au signe près. On a donc trouvé un élément en commun dans les deux factorisations (au signe près). On simplifie par ce terme x_1 et on trouve deux factorisations de $z' = \frac{z}{x_1}$, à savoir $z' = x_2 \dots .x_n$ et $z' = \epsilon y_2 \dots y_p$ où ϵ est un signe. Quitte à remettre ce signe dans le y_2, on peut supposer que ce signe vaut 1 et le supprimer de l'écriture. On peut maintenant recommencer l'opération avec z' à la place de z, puis avec $z'' = \frac{z'}{x_2}$ etc...et montrer ainsi que chaque x_i correspond à

un y_i qui lui est égal au signe près. En particulier $n \leq p$, donc par symétrie $n = p$, et les x_i correspondent au y_i au signe près et à permutation des y_i près. C'est l'unicité cherchée.

Exercice 26. Relire la démonstration de l'existence et de l'unicité de la factorisation des entiers de $\mathbb{Z}$ et dire à quel endroit a été utilisé (implicitement) la description des idéaux de $\mathbb{Z}$, dans l'existence ou dans l'unicité ?

Correction 26. On a utilisé pour l'unicité la description des idéaux de $\mathbb{Z}$. En fait, on a utilisé le corollaire 44, qui venait du théorème de Bezout, qui lui même a été établi en montrant que les idéaux de $\mathbb{Z}$ sont principaux.

2.4 Résultats dans $\mathbb{N}$

On a donc démontré l'existence et l'unicité d'une décomposition dans $\mathbb{Z}$. Un élément n de $\mathbb{N}$ est en particulier un élément de $\mathbb{Z}$ et on peut donc le décomposer en produit d'irréductibles: $n = p_1 \dots p_r$. En passant aux valeurs absolues, on a $n = |p_1| \dots |p_r|$. Puisqu'on a vu qu'un nombre de $\mathbb{Z}$ est irréductible si sa valeur absolue est un nombre premier, on a la décomposition voulue de n en produit de nombre premiers. Pour l'unicité d'une telle décomposition, on peut reprendre la démonstration de l'unicité faite sur $\mathbb{Z}$, en remarquant que les signes ϵ qui y apparaissent sont positifs. Donc la décomposition est unique à l'ordre des facteurs près au lieu d'être unique à l'ordre des facteurs et au signe près. En résumé, on a dans $\mathbb{N}$ le théorème.

Théorème 47. *Tout nombre entier positif différent de* 0 *et* 1 *s'écrit sous la forme* $n = n_1 \dots n_r$ *d'un produit de nombre premiers. En outre cette décomposition en produit est unique à l'ordre des facteurs près.*

Il nous reste à nous convaincre d'une dernière chose, c'est que les calculs de ppcm et de pgcd appris au collège sont corrects. C'est le but de l'exercice suivant.

Exercice 27. Soit $z = z_1^{a_1} \dots z_n^{a_n}$ et $w = w_1^{b_1} \dots w_p^{b_p}$ deux nombres entiers différents de 0 et 1 et leur décomposition en puissance d'irréductibles deux à deux distincts.
a)Dire pourquoi on peut supposer que $p = n$ et que $z_i = w_i$ pour tout i. On se place désormais dans ce cadre.
b)Rappeler comment on calcule le pgcd et le ppcm à partir de cette décomposition.
c)Donner une démonstration de votre affirmation pour le pgcd.

Correction 27.
a)Il suffit d'ajouter des éléments avec des puissances 0. Par exemple, pour $6 = 2.3$ et $5 = 5$. On peut prendre les décompositions $6 = 2^1 3^1 5^0$ et $5 = 2^0 3^0 5^1$.
b)Si $z = z_1^{a_1} \dots z_n^{a_n}$ et $w = z_1^{b_1} \dots z_n^{b_n}$, en posant $M_i = max(a_i, b_i)$ et $m_i = min(a_i, b_i)$, on a $pgcd(z, w) = \prod z_i^{m_i}$ et $ppcm(z, w) = \prod z_i^{M_i}$.
c)Il est clair que $D = \prod z_i^{m_i}$ divise à la fois z et w (pourquoi ?). Pour démontrer que ce nombre est bien le pgcd il suffit de montrer que c'est le plus grand diviseur. Soit d un diviseur commun à z et w et $d = \prod z_i^{d_i}$ sa décomposition en facteurs premiers. Pour démontrer que d divise D (donc que D est plus grand au sens de la divisibilité), il suffit de voir que d_i est plus petit que $m_i = min(a_i, b_i)$. Par symétrie, il suffit de traiter le cas $i = 1$. Remarquons que $z_1^{d_1}$ divise d et que d divise z. Donc $z_1^{d_1}$ divise $z = z_1^{a_1} \dots z_n^{a_n}$. Comme $z_1^{d_1}$ est premier avec $z_2^{a_2} \dots z_n^{a_n}$, il divise $z_1^{a_1}$. Mais ceci n'est possible que si $d_1 \leq a_1$. Le même raisonnement montre que $d_1 \leq a_2$, et donc finalement $d_1 \leq min(a_1, a_2) = m_1$, ce qu'on voulait.

2.5 Méthodes de calcul du ppcm et du pgcd

Puisque le pgcd a été caractérisé comme le générateur d'un certain idéal, et qu'on a vu comment calculer en pratique un générateur dans la section 2.2.2, on sait donc calculer facilement des pgcd par la méthode expliquée ie. par une suite de divisions. Relire l'exemple 35 qui montre que le pgcd de $(20, 5, 13)$ est 1.
Pour le ppcm de deux nombres, il se déduit en une ligne à partir du calcul du pgcd par la formule suivante.

Proposition 48. *Soient $a, b \in \mathbb{Z}$, d leur pgcd, m leur ppcm (définis au signe près). On a l'égalité $dm = ab$ au signe près.*

Démonstration. Les pgcd et les ppcm étant définis au signe près, on peut remplacer tous les nombres par leur valeur absolue et supposer que tous les nombres en jeu sont positifs. Si on regarde la décomposition de a en produit de nombres premiers, notons a_p la puissance à laquelle le nombre p apparaît. Notons de même b_p la puissance de p relative au nombre b. Alors $(ab)_p = a_p + b_p$. Par ailleurs $d_p = min(a_p, b_p)$ et $m_p = max(a_p, b_p)$. Donc $(dm)_p = min(a_p, b_p) + max(a_p, b_p) = a_p + b_p$. On a donc démontré que tout nombre premier p apparaît avec la même puissance dans la décomposition des nombres ab et dm, à savoir avec la puissance $a_p + b_p$. Cela suffit à montrer que $dm = ab$ au signe près. ∎

On applique tout de suite cette proposition dans l'exercice suivant.

Exercice 28. Calculer le ppcm de 28 et 36.

Correction 28. Le pgcd d est tel que $(d) = (28, 36)$. Les divisions $36 = 1.28 + 8$, $28 = 3.8 + 4$ et $8 = 4.2$ montrent que $(28, 36) = (4)$. Donc le pgcd est 4. Le ppcm est donc $\frac{28.36}{4} = 7.36$.

L'exercice suivant explique comment calculer un ppcm quand on a plus de deux nombres. On se ramène au cas de deux nombres.

Exercice 29.
a)Considérons trois nombres $a_1, a_2, a_3 \in \mathbb{Z}$. On procède de la façon suivante. On calcule le ppcm m_{12} de a_1 et a_2, puis le ppcm m_{123} de m_{12} et de a_3. Montrer que m_{123} est le ppcm des a_i.
b)Calculer le ppcm de $28, 36, 45$ par cette méthode.
c)Généraliser à un nombre quelconque d'éléments.

Correction 29.
a)On peut supposer que les a_i sont positifs pour calculer les ppcm. Soit $a_1 = \prod n_i^{m_i}$, $a_2 = \prod n_i^{p_i}$ et $a_3 = \prod n_i^{r_i}$ les décompositions en puissances d'irréductibles.Alors $m_{12} = \prod n_i^{max(m_i,p_i)}$. Et $m_{123} = \prod n_i^{max(max(m_i,p_i),r_i)}$ tandis que $ppcm(a_1, a_2, a_3) = \prod n_i^{max(m_i,p_i,r_i)}$. Le nombre m_{123} est donc bien un ppcm puisque $max(max(m_i, p_i), r_i) = max(m_i, p_i, r_i)$.
b)On a déjà vu dans un exercice précédent que $ppcm(28, 36) = 14.36$. Maintenant $ppcm(14.36, 45) = 9.ppcm(14.\frac{36}{9}, \frac{45}{9}) = 9ppcm(14.4, 5) = 9.14.4.5$.
c)Si $m_{12\ldots k}$ est le ppcm de nombres $a_1, \ldots, a_k$, on a la formule $m_{12\ldots k} = ppcm(m_{12\ldots k-1}, a_k)$.

En relisant les deux exercices précédents, vous pouvez trouver bien compliqué de considérer le ppcm comme le générateur d'un idéal et d'adopter des méthodes de calcul sophistiquées alors que la méthode de calcul que l'on connaissait au collège semble bien plus pratique à mettre en œuvre. La réponse est dans l'exercice suivant, qui vous convaincra que sauf pour des très petits nombres, votre ancienne méthode pour calculer un pgcd est en pratique infaisable: les calculs sont incroyablement trop longs à effectuer. En revanche, la nouvelle méthode est fonctionnelle.

Exercice 30.
a)Calculer le pgcd et le ppcm de 6557 et 6873 par votre ancienne méthode.
b)Même chose avec les nouvelles méthodes.

Correction 30.
a)Il est quasiment impossible de trouver les facteurs de ces nombres à la main, sans utiliser d'ordinateur.... En tout cas, je n'ai pas la patience !
b)Les divisions $6873 = 1.6557 + 316$ et $6557 = 316.20 + 237$, $316 = 237 + 79$, $237 = 3.79$ montrent que le pgcd est 79. Le ppcm est donc $\frac{6557.6873}{79} = 83.6873$.

2.6 Propriété universelle de $\mathbb{Z}$

Comme on l'a dit dans le chapitre précédent, on essaiera si c'est possible de comprendre pour chaque anneau ses idéaux et une propriété universelle.

Exercice 31. Rappeler la propriété universelle de $\mathbb{Z}$.

Correction 31. Cf le cours. chapitre 1 (14).

Si on dit de cette propriété qu'elle est universelle, c'est qu'elle caractérise $\mathbb{Z}$. Le problème c'est que ce n'est pas tout à fait exact: elle le caractérise à isomorphisme près. Revenons un instant sur cette notion d'isomorphisme. Considérons les matrices de taille 2×2 à coefficients dans $\mathbb{Z}$. Notons $M_i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$.

Exercice 32. Vérifier les formules $M_i + M_j = M_{i+j}$ et $M_i.M_j = M_{ij}$.

Correction 32. C'est une vérification évidente.

Les matrices M_i forment un sous-anneau A commutatif de $M_{2\times 2}(\mathbb{Z})$ et on a par exemple les formules $M_3 + M_4 = M_7$, $M_3.M_4 = M_{12}$ d'après l'exercice précédent. Autrement dit, tout se passe comme si on avait simplement changer les noms des éléments, fait une traduction. Au lieu d'écrire le nombre 3 on écrit M_3 et ainsi de suite. On a donc envie de dire que l'anneau A formé par les matrices M_i est "le même" que $\mathbb{Z}$, à changement de nom des éléments près. Cela se traduit mathématiquement par la notion d'isomorphisme

Exercice 33. Vérifier que l'anneau A contenant les matrices $M_i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $i \in \mathbb{Z}$ et $\mathbb{Z}$ sont deux anneaux isomorphes.

Correction 33. Considérons l'application $f : \mathbb{Z} \to A$ qui envoie 1 sur M_1, bien définie par propriété universelle de $\mathbb{Z}$. Cette application envoie i sur M_i (pourquoi ?) On a $f(i + j) = M_{i+j} = M_i + M_j = f(i) + f(j)$ d'après

l'exercice précédent. De même, $f(ij) = f(i)f(j)$. De plus $f(1) = M_1$ et M_1 est le neutre multiplicatif de A. Donc f est un morphisme d'anneaux. Il est clairement bijectif donc c'est un isomorphisme.

Puisque en essence, deux anneaux qui sont isomorphes sont les mêmes à changement de nom près, toute propriété vraie pour l'un doit être vraie pour l'autre. Voici un petit exercice pour s'en convaincre.

Exercice 34. Soient A et B deux anneaux isomorphes. Montrer que si A contient un élément de carré nul, alors B contient également un élément de carré nul.

Correction 34. Soit $a \in A$ l'élément de carré nul et $b \in B$ son image par l'isomorphisme $A \to B$. On a $b^2 = b.b = f(a).f(a) = f(a.a) = f(a^2) = f(0) = 0$. Donc B contient un élément de carré nul, à savoir b.

Donc finalement, on ne veut pas dire qu'il existe un unique anneau satisfaisant la propriété universelle de $\mathbb{Z}$, mais un unique anneau à isomorphisme près. C'est ce qu'affirme le théorème suivant.

Théorème 49. *Soit A un anneau satisfaisant la propriété universelle de $\mathbb{Z}$: ie. pour tout anneau B, il existe un unique morphisme d'anneaux $f : A \to B$. Alors A est isomorphe à $\mathbb{Z}$.*

Démonstration. Le raisonnement est court mais sans doute un peu déroutant la première fois qu'on le rencontre. La propriété universelle de A nous assure qu'il existe un unique morphisme $f : A \to \mathbb{Z}$. Je veux montrer que ce f est un isomorphisme, c'est à dire qu'il est bijectif. Pour cela il me suffit de construire une bijection inverse, c'est à dire un morphisme $g : \mathbb{Z} \to A$ telle que $f \circ g = Id_{\mathbb{Z}}$ et $g \circ f = Id_A$ sont les applications identités. A l'aide de la propriété universelle de $\mathbb{Z}$, je peux définir g comme étant l'unique morphisme de $\mathbb{Z}$ dans A. Nous aurons gagné si nous vérifions qu'on a bien comme voulu $f \circ g = Id_{\mathbb{Z}}$ et $g \circ f = Id_A$. Les deux raisonnements sont similaires et on ne fait que le premier. L'application $f \circ g : \mathbb{Z} \to \mathbb{Z}$ est un morphisme d'anneaux (pourquoi ?). Mais l'application identité de $\mathbb{Z}$ est un autre morphisme d'anneaux et par propriété universelle, il existe un unique morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}$. On en déduit l'égalité cherchée $f \circ g = Id_{\mathbb{Z}}$. ■

Chapitre 3

Anneau quotient et anneau produit. Applications cryptographiques

Objectif Dans ce chapitre, on introduit les notions d'anneau quotient et d'anneau produit, en se concentrant essentiellement sur l'anneau $\mathbb{Z}/n\mathbb{Z}$, dont on a déjà rencontré les tables de multiplication et d'addition dans le cas particulier $n = 6$ (exercice 8). Une application frappante et concrète de l'étude mathématique de ces anneaux est donné par la cryptographie.

3.1 Présentations de $\mathbb{Z}/n\mathbb{Z}$ par les congruences

Commençons par un petit exemple. Monsieur X est à table avec ses amis et se plaint que le premier mai est un dimanche cette année (un jour férié de perdu...) Que se passera-t-il l'année prochaine ? Monsieur X calcule "de tête" devant ses amis et pronostique que l'an prochain, ce sera un lundi. Vérification faite sur le calendrier, il a raison. Comment a-t-il fait ?
Il a d'abord remarqué que comme l'année n'était pas bissextile, il y avait 365 jours dans une année. Ensuite, il s'est aperçu que ce qui comptait n'était pas vraiment le nombre de jours. En effet, s'il y avait sept jours en plus ou en moins dans une année, cela ajouterait ou retirerait une semaine complète, et ne changerait pas le jour obtenu. Donc si on fait une division, $365 = 7.q+r$, ce qui compte ce n'est pas le nombre de semaines entières d'ici l'an prochain (matérialisé par le nombre q de la division) mais le reste r. Monsieur X a donc cherché de tête le reste de la division par 7. Mais comme il est très mauvais en calcul mental, il a fait la simplification suivante. Il a

dit $365 = 360 + 5 = 36.10 + 5$. Ensuite, il a remplacé chaque nombre par le reste de la division par 7, ce qui signifie qu'au lieu de calculer $36.10 + 5$, il a calculé $1.3 + 5 = 8$. Le reste de la division de 8 par 7 étant 1, il a donc dit tout se passe comme s'il y avait 1 seul jour dans l'année. Donc si le premier mai est un dimanche cette année, ce sera un lundi l'an prochain.
Comment a donc fait Monsieur X ? A-t-il simplement eu de la chance (après tout, il avait une chance sur sept de trouver le résultat juste) ? Ou bien est-ce que son raisonnement est correct ? Analysons son raisonnement. Ce qui est correct visiblement, c'est qu'il suffit de connaitre le reste de la division par 7. En revanche, la façon dont il calcule ce reste est suspecte. Sans tout à fait s'en rendre compte, il utilise la règle suivante. Si un nombre n s'écrit comme une somme $n = a + b$, alors pour calculer le reste de la division par 7, on peut calculer d'abord le reste r_a de a, puis le reste r_b de b, additionner les deux restes $r_a + r_b$, et prendre enfin le reste de r_c de cette somme en disant que c'est le reste de la division de n. Il a fait la même approximation pour le calcul du reste dans une multiplication, $n = a.b$. Est-ce correct ?
Oui, c'est correct. Mais pour en faire une démonstration mathématique propre, il nous faut introduire le vocabulaire adapté.

Définition 50. *congru On dit qu'un nombre $a \in \mathbb{Z}$ est congru à b modulo d si d divise $b - a$ et on notera cette propriété par $a \equiv b(d)$.*

Exercice 35.
a)Montrer que la relation $\mathcal{R}$ défini par $a\mathcal{R}b$ si a est congru à b modulo d est une relation d'équivalence.
b)Montrer qu'il existe un unique nombre r tel que $a \equiv r(d)$ et tel que $0 \leq r < |d|$.

Correction 35.
a)Il faut montrer que la relation est reflexive, symétrique et transitive ie. que:

- $x \equiv x(d)$ pour tout x
- $x \equiv y(d) \Rightarrow y \equiv x(d)$
- $x \equiv y(d)$ et $y \equiv z(d) \Rightarrow x \equiv z(d)$

(Vous remarquerez que les propriétés sont celles qu'on utilise implicitement avec le symbole $=$). Le premier point est évident: $x - x = 0$ est divisible par d donc $x \equiv x(d)$. Pour le deuxième point, si $y - x = kd$ est divisible par d, $x - y = -kd$ est aussi divisible par d. Enfin, si $y - x = kd$ et si $z - y = ld$, alors $z - x = (l + k)d$ est divisible par d.
b)Si $r_1 \geq r_2$ sont deux nombres qui peuvent jouer le rôle de r, alors $r_1 - r_2$

est un nombre vérifiant $0 \leq r_1 - r_2 < |d|$ et divisible par d, donc c'est 0. D'où $r_1 = r_2$ et le nombre r est unique.

Définition 51. *Soit $d \in \mathbb{N}$ et $a \in \mathbb{Z}$. L'unique nombre r de l'exercice précédent tel que $a \equiv r(d)$ et $0 \leq r < |d|$ est appelé le reste de la division de a par d.*

Exercice 36. Montrer que $a \equiv b(d)$ ssi a et b ont le même reste pour la division par d.

Correction 36. Soit r le reste de la division de a par d. Alors par définition, $0 \leq r < d$ et $r \equiv a(d)$. Puisque $b \equiv a(d)$, on a par transitivité de l'équivalence $r \equiv b(d)$. Donc par définition du reste, r est également le reste de la division de b par d. Réciproquement, si a et b ont même reste r par division par d, alors $a \equiv r(d)$ et $b \equiv r(d)$ et donc par transitivité, $a \equiv b(d)$.

La proposition qui justifie le calcul de Monsieur X est la suivante.

Proposition 52. *Soit a et b deux élements de $\mathbb{Z}$. Si $a \equiv a'(d)$ et $b \equiv b'(d)$, alors $ab \equiv a'b'(d)$ et $a + b \equiv a' + b'(d)$.*

Avant de faire la démonstration, expliquons en quoi ce résultat justifie le calcul de Monsieur X. Pour montrer que le reste de la division de 365 par 7 est 1, avec notre nouveau vocabulaire et par définition du reste, cela revient à montrer que $365 \equiv 1(7)$. Le problème étant maintenant reformulé en termes de congruence, on peut utiliser la proposition 52. On a $36 \equiv 1(7)$ et $10 \equiv 3(7)$ par définition de $\equiv$. Donc par la proposition 52, $360 \equiv 1.3(7)$. Comme $5 \equiv 5(7)$, toujours par la proposition, $360 + 5 \equiv 3 + 5(7)$. Et comme finalement $8 \equiv 1(7)$, on a l'égalité voulue $365 \equiv 1(7)$ par transitivité.
Revenons à la démonstration de la proposition.
Démonstration. Montrons que $b \equiv a'b'(d)$. Par hypothèse et par définition du symbole $\equiv$, il existe deux nombres q et q' tels que $a = qd + a'$ et $b = q'd + b'$. Donc $ab = (qd + a')(q'd + b') = d(qq'd + qb' + a'q) + a'b'$. Cette dernière égalité montre qu' on a bien la congruence $ab \equiv a'b'$. L'équivalence $a + b \equiv a' + b'$ se démontre de façon similaire. ∎

Exercice 37. Soit a et b deux élements de $\mathbb{Z}$. Si $a \equiv a'(d)$ et $b \equiv b'(d)$, alors $a + b \equiv a' + b'(d)$.

Correction 37. Si $a \equiv a'(d)$ et $b \equiv b'(d)$, alors $a' - a = kd$ et $b' - b = ld$. Donc $(a' + b') - (a + b) = (k + l)d$, c'est à dire $a + b \equiv a' + b'(d)$

Exercice 38. En mimant la méthode de Monsieur X, calculer le reste de la division de 1234 par 12. Calculer de même le reste de la division de -145 par -15

Correction 38. $1234 = 12.100 + 12.2 + 10$. En remplaçant les termes de droite par leur reste de division par 12, on obtient $0. * +0.2 + 10 = 10$. Donc le reste de la division par 12 est 10. Pour le deuxieme calcul, $-145 = -15.10+5$. En passant aux restes, dans le terme de droite, on trouve $0.10+5$, donc le reste est 5.

3.2 Définition de $\mathbb{Z}/n\mathbb{Z}$

Dans la section précédente, nous avons travaillé avec les restes des divisions et multiplié ou additionné les restes. Qui dit addition et multiplication dit structure d'anneau. Autrement dit, la section précédente suggére qu'il existe une structure d'anneau sur l'ensemble $\{\dot{0}, \ldots, n \dot{-} 1\}$ des restes possibles des divisions par n. En effet, une telle structure d'anneau existe et l'ensemble $\{\dot{0}, \ldots, \dot{n}-1\}$ muni de sa structure d'anneau est noté $\mathbb{Z}/n\mathbb{Z}$. Noter au niveau calligraphique que l'on met des points sur les nombres pour signifier que ce sont des restes. Cela nous permet ainsi de distinguer l'opération $\dot{3} + \dot{5} = \dot{1}$ (quand on fait le calcul dans $\mathbb{Z}/7\mathbb{Z} = \{\dot{0}, \ldots, \dot{6}\}$) de l'addition $3 + 5 = 8$ (dans $\mathbb{Z}$).
On rappelle qu'une partition de E est un découpage de E en sous-ensembles E_i de sorte que:

- les E_i sont disjoints: $E_i \cap E_j = \emptyset$ si $i \neq j$.
- les E_i recouvrent E: $E = \cup_{i \in I} E_i$.

Exemple 53. *Soit P l'ensemble des entiers positifs pairs et I l'ensemble des entiers impairs. Alors $\mathbb{N} = P \cup I$ est une partition. En général, on utilise le symbole $\mathbb{N} = P \coprod I$ pour signaler que la réunion est disjointe.*

Exercice 39. Soit E_i l'ensemble des éléments de $\mathbb{Z}$ congrus à i modulo trois. Montrer que E_0, E_1, E_2 forment une partition de $\mathbb{Z}$.

Correction 39. Montrons d'abord que les E_i sont disjoints. Par symétrie, montrons simplement que E_0 et E_1 sont disjoints. Si un élément est dans E_0, son reste dans la division par 3 est 0. S'il est dans E_1, son reste est 1. Donc un élément ne peut être à la fois dans E_0 et E_1. Montrons maintenant que les E_i recouvrent $\mathbb{Z}$, c'est à dire que tout $x \in \mathbb{Z}$ est dans l'un des E_i. Quand on divise x par trois, le reste est 0, 1 ou 2. Si c'est 0 (resp. 1, resp 2), x est dans E_0 (resp. E_1, E_2). Tout élément est bien dans l'un des E_i.

Essentiellement, se donner une partition revient à se donner une relation d'équivalence. Ainsi, dans l'exemple $\mathbb{N} = P \cup I$, on va dire que tous les nombres pairs sont équivalents entre eux. De même, on dira que tous les nombres impairs sont équivalents entre eux. Si on veut une définition précise, on définit la relation d'équivalence associé à une partition de la façon suivante.

Définition-Proposition 54. *Soit $E = \coprod_{i \in I} E_i$ une partition de E. La relation $a\mathcal{R}b$ ssi $\exists i \in I$, tel que $a \in E_i, b \in E_i$ est une relation d'équivalence appelée relation d'équivalence associée à la partition.*

Démonstration. Pour voir que la relation est une relation d'equivalence il faut voir qu'elle est réflexive, symétrique, transitive, ce qui signifie

- $x\mathcal{R}x$
- $x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$

Mais ces affirmations sont évidentes: x est dans le même sous-ensemble que lui même, si x et y sont dans le même sous ensemble, alors y et x également. Enfin si x et y sont dans le même sous-ensemble et si y et z sont dans le même sous-ensemble, alors x et z sont dans le même sous-ensemble. ■

Donc à une partition est associée une relation d'équivalence. Mais réciproquement, si on dispose d'une relation d'équivalence sur E, on peut définir une partition: le découpage de E en sous-ensembles consiste à mettre dans un même paquet tous les éléments qui sont équivalents entre eux. Les paquets ainsi définis sont appelés classes d'équivalence. Formellement, la définition est la suivante.

Définition-Proposition 55. *Soit $\mathcal{R}$ une relation d'équivalence sur E. Un sous-ensemble non vide $F \subset E$ est appelé classe d'équivalence s'il existe $e \in E$ tel que $f \in F$ ssi $e\mathcal{R}f$. On notera ce sous ensemble $\dot{e}$ et on dira que $\dot{e}$ est la classe d'équivalence associée à e. L'ensemble des classes d'équivalence forme une partition de E.*

Démonstration. Tout élément $e \in E$ est dans la classe $\dot{e}$ par définition de $\dot{e}$, donc les classes d'équivalence recouvrent E. Pour voir que E est la réunion disjointe de ses classes d'équivalence, il reste à voir que si deux classes $\dot{e}$ et $\dot{f}$ sont distinctes, alors elles sont d'intersection vide. Et ce résultat est démontré dans l'exercice qui suit. ■

En résumé, se donner une relation d'équivalence sur E ou se donner une partition de E, c'est la même chose. Cela consiste simplement à regrouper les éléments de E en sous-ensembles d'éléments équivalents.

Exercice 40. Soit $\mathcal{R}$ une relation d'équivalence sur E et $e, f \in E$ deux éléments
a)Montrer que les ensembles $\dot{e}$ et $\dot{f}$ sont soit d'intersection vide, soit égaux.
b)Montrer que $\dot{e} = \dot{f}$ ssi $e \in \dot{f}$.
c)Montrer que $\dot{e} = \dot{f}$ ssi $e\mathcal{R}f$.

Correction 40.
a)Supposons que $\dot{e} \cap \dot{f} \neq \emptyset$. Montrons qu'alors $\dot{e} = \dot{f}$. Par hypothèse $\dot{e}$ et $\dot{f}$ contiennent tous deux un élément g. Soit $x \in \dot{e}$. Alors $x\mathcal{R}e\mathcal{R}g\mathcal{R}f$. Donc $x\mathcal{R}f$, ie. $x \in \dot{f}$. On a donc montré $\dot{e} \subset \dot{f}$. Par symétrie on a $\dot{f} \subset \dot{e}$ et finalement $\dot{e} = \dot{f}$.
b)Puisque $e \in \dot{e}$, si $\dot{e} = \dot{f}$, alors $e \in \dot{f}$. Réciproquement, si $e \in \dot{f}$, alors $\dot{f}$ et $\dot{e}$ contiennent tous deux l'élément e, donc $\dot{e} = \dot{f}$ par le premier point de l'exercice.
c)Les conditions $e \in \dot{f}$ et $e\mathcal{R}f$ sont identiques, donc cette question est la même que la précédente.

Proposition 56. *Soit A un anneau et $I \subset A$ un idéal. La relation définie par $x\mathcal{R}y \Leftrightarrow x - y \in I$ est une relation d'équivalence.*

Démonstration. Il faut voir que la relation est reflexive, symétrique, transitive.

- reflexive: $x\mathcal{R}x$ puisque $x - x = 0 \in I$
- symétrique: si $x\mathcal{R}y$, on a $x - y \in I$, donc en multipliant par -1, $y - x \in I$, ce qui signifie $y\mathcal{R}x$.
- transitive: si $x\mathcal{R}y$ et $y\mathcal{R}z$, on a $x - y \in I$ et $y - z \in I$, donc par somme $x - z \in I$, c'est à dire $x\mathcal{R}z$.

■

Mettons cette définition un peu abstraite en œuvre sur un exemple.

Exercice 41. Considérons $A = \mathbb{Z}$, $I = (3)$ et $\mathcal{R}$ la relation d'équivalence associée à l'idéal I.
a)Décrire $\dot{3}$, $\dot{4}$, $\dot{6}$.
b)Donner une condition nécéssaire et suffisante pour que $\dot{x} = \dot{3}$.
c)Combien y-a-t-il de classes d'équivalences ?
d)Donner sans démonstration, une condition nécessaire et suffisante pour que les classes $\dot{x}, \dot{y}, \dot{z}$ forment une partition de $\mathbb{Z}$.

Correction 41.
a)$\dot{3} = \{\cdots -3, 0, 3, 6, 9 \ldots\}$. $\dot{4} = \{\cdots -2, 1, 4, 7 \ldots\}$. $\dot{6} = \{\cdots -$

$3, 0, 3, 6, 9 \dots\} = \dot{3}$.
b)On a $\dot{x} = \dot{3}$ ssi $x \equiv 3(3)$ ssi $x \equiv 0(3)$ ssi 3 divise x.
c)Il y a trois classes d'équivalence: $\dot{3}, \dot{4}$ et $\dot{5}$, qui sont aussi les classes $\dot{0}, \dot{1}, \dot{2}$.
d)Les classes $\dot{x}$, $\dot{y}$, $\dot{z}$ forment une partition de $\mathbb{Z}$ ssi les restes de la division par 3 de x, y, z sont tous les trois différents.

Proposition 57. *Soit $n \in \mathbb{N}$, $I = (n)$ l'idéal de $\mathbb{Z}$ correspondant et $\mathcal{R}$ la relation d'équivalence associée. Alors la partition de $\mathbb{Z}$ formée par les classes d'équivalence est formée de n classes d'équivalence distinctes $\{\dot{0}, \dot{1}, \dots, n \dot{-} 1\}$, où*

$$\dot{i} = \{\dots, i - 2n, i - n, i, i + n, i + 2n, \dots\}.$$

De plus, pour deux éléments $p, q \in \mathbb{Z}$, on a $\dot{p} = \dot{q}$ dans $\mathbb{Z}/n\mathbb{Z}$ ssi $p \equiv q(n)$.

Démonstration. Commençons par le dernier point. Pour que $\dot{p} = \dot{q}$, il faut et suffit d'après l'exercice 40 que $p\mathcal{R}q$, c'est à dire ici par définition de la relation d'équivalence que $p - q \in (n)$. On peut traduire cette appartenance par le fait que n divise $p - q$, ou encore que $p \equiv q(n)$.
Puisque les nombres, $0, \dots, n - 1$ ne sont pas deux à deux congrus modulo n, il s'ensuit d'après le premier point que les classes $\dot{0}, \dot{1}, \dots, n \dot{-} 1$ sont bien distinctes. Il reste à vérifier qu'on a bien décrit toutes les classes d'équivalence. Si $\dot{p}$ est une classe d'équivalence, considérons le reste r de la division de p par n. On a par construction $p \equiv r(n)$, donc par le premier point $\dot{p} = \dot{r}$, avec $r \in \{0, \dots, n - 1\}$. Toute classe d'équivalence est donc bien une des classes $\dot{0}, \dot{1}, \dots, n \dot{-} 1$. ∎

Notation 58. *On note $\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \dots, n \dot{-} 1\}$ l'ensemble des classes d'équivalence sur $\mathbb{Z}$ défini par l'idéal (n). Plus généralement, on note A/I l'ensemble des classes d'équivalence de A pour la relation d'équivalence définie par un idéal I.*

On veut mettre une structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$ et plus généralement sur A/I. Autrement dit, on veut définir une addition et une multiplication sur l'ensemble des classes. Pour dire qui est la somme $C+D$ de deux classes, qui est le produit de deux classes, on fait l'opération suivante. On choisit un élément $c \in C$ et $d \in D$. Et on pose $C + D =$ la classe d'équivalence associée à l'élément $c+d$. Reprenons ainsi l'exemple de $\mathbb{Z}/3\mathbb{Z}$ considéré dans l'exercice précédent. Pour additionner les classes $C = \{\dots, -4, -1, 2, \dots\}$ et $D = \{\dots, -2, 1, 4, \dots\}$, on peut choisir les éléments $c = 2 \in C$ et $d = 1 \in D$

et on a donc $C + D = \dot{3} = \{\dots, -3, 0, 3, \dots\} = \dot{0}$. Ce qu'on peut résumer par la formule $\dot{1} + \dot{2} = \dot{0}$ dans $\mathbb{Z}/3\mathbb{Z}$. On peut définir de façon similaire un produit de deux classes en multipliant deux représentants c et d des deux classes C et D que l'on veut multiplier. Évidemment, le problème ici est que l'on a fait des choix pour les représentants c et d. Est-ce qu'on aurait trouvé un résultat différent si on avait fait des choix différents pour c et d? La proposition suivante dit que non. Nous avons besoin au préalable d'une notation.

Notation 59. *Si c et d sont dans A, on note $c\dot{+}d$ la classe de $c + d$ dans A/I (respectivement $\dot{c}\dot{d}$ la classe de cd).*

Proposition 60. *Soit $C, D \in A/I$, $c, c' \in C$, $d, d' \in D$. Si $\dot{c} = \dot{c'}$ et $\dot{d} = \dot{d'}$, alors les classes de $c + d$ et $c' + d'$ coïncident. De même, les classes des produits cd et $c'd'$ sont égales. En particulier les formules $\dot{c} + \dot{d} = c\dot{+}d$ et $\dot{c}\dot{d} = \dot{c}\dot{d}$ sont des formules définissant les quantités $\dot{c}+\dot{d}$ et $\dot{c}\dot{d}$ sans ambiguité au sens où ces formules ne dépendent pas du choix de c et d.*

Démonstration. Puisque $\dot{c} = \dot{c'}$, on a $c - c' \in I$. De même, $d - d' \in I$. Alors par somme $(c + d) - (c' + d') \in I$ puisque I est stable par addition, c'est à dire que $c + d$ et $c' + d'$ définissent la même classe. De même $cd - c'd' = d(c - c') + c'(d - d') \in I$, donc les classes de cd et $c'd'$ coïncident. ■

Exercice 42. Considérons l'ensemble $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$. Calculer les produits et les sommes d'éléments de $\mathbb{Z}/3\mathbb{Z}$ en utilisant la définition précédente. Consigner vos résultats dans une table d'addition et de multiplication.

Correction 42. Calculons par exemple $\dot{2} + \dot{1}$. Les autres calculs se font de même. On choisit deux éléments dans $\dot{2}$ et $\dot{1}$ respectivement, par exemple 2 et 4. On fait leur somme: $2 + 4 = 6$. L'élément 6 est dans $\dot{0}$, donc $\dot{2} + \dot{1} = \dot{0}$. Les autres calculs sont résumés dans les tables suivantes.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

,

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

On a donc défini une addition et une multiplication sur l'ensemble A/I des classes. Montrons que nous avons ainsi défini un anneau.

Théorème 61. *L'ensemble A/I muni des lois $+$ et $.$ ci-dessus est un anneau dans lequel*

- *l'élément privilégié* 0 *est* $\dot{0}$
- *l'élément privilégié* 1 *est* $\dot{1}$
- *l'opposé de* $\dot{a}$ *est* $\dot{-a}$.

Démonstration. La définition d'un anneau demande de vérifier une longue liste de propriétés. Toutes les vérifications se font dans le même esprit et nous n'en ferons que quelques unes par souci de concision. Montrons par exemple

- que $\dot{0}$ est un neutre pour l'addition
- que $\dot{-a}$ est l'opposé de $\dot{a}$
- que la multiplication est distributive par rapport à l'addition.

Les autres vérifications sont laissées au lecteur. Pour le premier point, $\dot{0}+\dot{a} = \dot{0+a} = \dot{a}$. Pour le second, $\dot{-a}+\dot{a} = \dot{-a+a} = \dot{0}$. Pour le troisième, $\dot{x}(\dot{y}+\dot{z}) = x(\dot{y+z}) = \dot{xy+xz} = \dot{x}\dot{y}+\dot{x}\dot{z}$. ∎

On peut maintenant reformuler le raisonnement de Monsieur X en travaillant dans l'anneau $\mathbb{Z}/7\mathbb{Z}$ puisqu'il veut le résultat de la division par 7. On obtient $\dot{365} = \dot{360}+\dot{5} = \dot{36}.\dot{10}+\dot{5} = \dot{1}.\dot{3}+\dot{5} = \dot{8} = \dot{1}$. Donc le reste de la division par 7 est 1. On peut noter comme le nouveau formalisme de travail dans $\mathbb{Z}/7\mathbb{Z}$ rend la rédaction de la solution beaucoup plus facile. Évidemment, nous avons payé un prix pour cela, c'est celui de l'effort de construction des anneaux $\mathbb{Z}/n\mathbb{Z}$.
Le rapport entre l'anneau A et l'anneau quotient A/I est donné par un morphisme.

Proposition 62. *L'application* $A \to A/I$, $a \mapsto \dot{a}$ *est un morphisme d'anneaux.*

La démonstration est assez formelle et laissée au lecteur. Voyons en exercice les propriétés de ce morphisme.

Exercice 43. Montrer que le morphisme d'anneaux $A \to A/I$ est surjectif et que son noyau est l'idéal I.

Correction 43. Par définition de A/I, un élément de A/I est de la forme $\dot{a}$. C'est donc l'image de $a \in A$. Donc le morphisme est surjectif. Si un élément a s'envoie sur $\dot{0}$, cela signifie que $\dot{a} = \dot{0}$, ce qui, d'après un exercice précédent signifie que $a \in \dot{0}$. Or $\dot{0} = I$. Donc $a \in I$. On vient donc de montrer que le noyau du morphisme est I.

3.3 Propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ et des quotients.

ExoTD 4. *Quel est le noyau du morphisme de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

correcTD 4. *Le noyau du morphisme $A \to A/I$ étant l'idéal I, le noyau de ce morphisme est l'idéal $n\mathbb{Z}$ formé des multiples de n.*

Essayons de comprendre la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$, ie. comment se donner un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to A$. Pour l'image de $\dot{0}$, on n'a pas le choix, c'est le 0_A de A. De même, l'image de $\dot{1}$ est l'élément 1_A de A. Mais alors $\varphi(\dot{2}) = \varphi(\dot{1}+\dot{1}) = \varphi(\dot{1})+\varphi(\dot{1}) = 2.1_A$. On a de même $\varphi(\dot{3}) = 3.1_A$ etc... On pourrait croire que l'on a bien défini le morphisme puisqu'on a défini φ de nimporte quel élément. Mais il y a un petit problème. Si je continue le raisonnement précédent, on a $\varphi(\dot{n}) = n.1_A$. Mais comme on a $\dot{n} = \dot{0}$, on doit avoir $\varphi(\dot{n}) = 0$. On a donc deux définitions différentes pour $\varphi(\dot{0})$, à savoir 0_A et $n.1_A$. Ce n'est pas génant si $0_A = n.1_A$. Donc en résumé, si cette égalité n'est pas vérifiée, il n'y a pas de morphisme $\mathbb{Z}/n\mathbb{Z} \to A$. Sinon, on peut espérer qu'il existe un morphisme. C'est effectivement ce qui se passe.

Théorème 63. ***Propriété universelle de*** $\mathbb{Z}/n\mathbb{Z}$**.** *Soit A un anneau et notons 1_A son unité. Si $n.1_A = 0_A$, alors il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z}/n\mathbb{Z} \to A$. En outre, ce morphisme est donné par la formule $\varphi(\dot{k}) = k.1_A$. Si $n.1_A \neq 0_A$, alors il n'existe pas de morphisme $\mathbb{Z}/n\mathbb{Z} \to A$.*

Démonstration. Par le raisonnement qui précède l'énoncé du théorème, on voit que le morphisme s'il existe doit vérifier $\varphi(\dot{k}) = k.1_A$, donc on n'a aucun choix et ce morphisme est alors unique. Le problème de l'unicité étant réglé, reste à traiter le problème de l'existence. Comme on l'a vu ci-dessus, ce morphisme ne peut exister que si $n.1_A = 0$. Réciproquement, si $n.1_A = 0$, on définit l'application par la formule $\varphi(\dot{k}) = k.1_A$. Dit de manière différente, on choisit un élément k dans la classe $\dot{k}$ et on pose, $\varphi(\dot{k}) = k.1_A$. Il faut d'abord vérifier que la formule ne dépend pas du choix de $k \in \dot{k}$. Si k' est un autre élément tel que $k' \in \dot{k}$, alors $k' - k = \mu n$ est un multiple de n. Donc $k'.1_A = (k + \mu n)1_A = k.1_A + \mu.n.1_A = k.1_A$. Donc le résultat ne dépend pas du choix de k et la formule est bien définie. Reste finalement à vérifier que la formule définit bien un morphisme d'anneaux:

- $\varphi(\dot{1}) = 1_A$ est évident par construtions
- $\varphi(\dot{x} + \dot{y}) = \varphi(\dot{x+y}) = (x + y).1_A = x.1_A + y.1_A = \varphi(\dot{x}) + \varphi(\dot{y})$.
- $\varphi(\dot{x}\dot{y}) = \varphi(\dot{xy}) = (xy).1_A = (x.1_A)(y.1_A) = \varphi(\dot{x})\varphi(\dot{y})$.

■

Exercice 44.
a)Montrer qu'il existe un unique morphisme d'anneaux $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Quelle est l'image de $\dot{4}$?
b)Soient n et m deux entiers positifs. Montrer que si m ne divise pas n, il n'existe pas de morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.
c)Montrer que si m divise n, il existe un unique morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Donner une formule pour ce morphisme. Montrer qu'il est surjectif. Donner un exemple qui montre qu'il n'est pas injectif en général.

Correction 44.
a)Puisque $6.1_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}} = 6.(1_{\mathbb{Z}/2\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}) = (\dot{6}, \dot{6}) = (\dot{0}, \dot{0}) = 0_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}}$, par propriété universelle de $\mathbb{Z}/6\mathbb{Z}$ il existe bien un morphisme f unique. On a $f(\dot{4}) = (\dot{4}, \dot{4}) = (\dot{0}, \dot{1})$.
b)$\underbrace{\dot{1} + \cdots + \dot{1}}_{n \ fois} = \dot{n}$ est différent de $\dot{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ si m ne divise pas n. D'après la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$, il n'existe dans ce cas pas de morphisme d'anneaux.
c)Dans le cas où m divise n, alors $n.\dot{1}_{\mathbb{Z}/m\mathbb{Z}} = \dot{0}$, donc il existe un morphisme $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ d'après la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ qui est donné par la formule $\varphi(\dot{k}) = \dot{k}$. Ce morphisme est évidemment surjectif puisque tout élément $\dot{k}$ a un antécédent, à savoir $\dot{k}$. Si $n = 4$ et $m = 2$, les éléments $\dot{0}$ et $\dot{2}$ s'envoient sur le même élément $\dot{0}$ (car $\dot{2} = \dot{0}$ dans $\mathbb{Z}/2\mathbb{Z}$), donc le morphisme $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ n'est pas injectif.

Pour finir, essayons de généraliser la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ en un énoncé sur les anneaux quotients. On veut montrer que se donner un morphisme $\bar{\varphi} : A/I \to B$ équivaut à se donner un morphisme $\varphi : A \to B$ vérifiant $\varphi(I) = 0$. Comment définir $\bar{\varphi}$ à partir de φ ? L'idée est la même que pour $\mathbb{Z}/n\mathbb{Z}$. Pour toute classe $\dot{a}$, on choisit un élément $a \in \dot{a}$ et on définit un morphisme $\bar{\varphi}$ par la formule $\bar{\varphi}(\dot{a}) = \varphi(a)$. La question est de savoir si la formule définissant $\bar{\varphi}$ ne dépend pas du choix de a.

Lemme 64. *Soit $\varphi : A \to B$ un morphisme d'anneaux. Soit $\dot{a} \in A/I$. Soit $a \in \dot{a}$. La quantité $\varphi(a)$ ne dépend pas du choix de a ssi φ envoie tout élément de I sur 0.*

Démonstration. Notons que $\varphi(0) = 0$ comme pour tout morphisme d'anneaux. Supposons que $\varphi(a)$ ne dépende pas de $a \in \dot{a}$. En particulier pour a et 0 dans $\dot{0}$, on doit avoir $\varphi(a) = \varphi(0) = 0$. Mais les éléments a qui sont dans $\dot{0}$ sont les a tels que $a - 0 = a \in I$ d'après l'exercice 40 et la définition de la relation d'équivalence. Autrement dit, si $\varphi(a)$ ne dépend

pas du choix de a, alors $\varphi(I) = 0$.
Supposons réciproquement que $\varphi(I) = 0$ et montrons que $\varphi(a)$ ne dépend pas du choix de a. Si a et b sont deux éléments dans $\dot{a}$, cela signifie que $a - b = i \in I$. Alors $\varphi(b) = \varphi(a - i) = \varphi(a) - \varphi(i) = \varphi(a) - 0 = \varphi(a)$. ■

Maintenant, une démonstration similaire à celle du cas $\mathbb{Z}/n\mathbb{Z}$ montre que la formule pour $\bar{\varphi}$ définit un morphisme d'anneaux. On a donc montré la proposition suivante:

Proposition 65. *Soient A,B deux anneaux, $I \subset A$ un idéal et $\varphi : A \to B$ un morphisme d'anneaux, tel que $\varphi(I) = 0$. L'application $\bar{\varphi} : A/I \to B$, $\dot{a} \mapsto \varphi(a)$ est bien définie au sens où $\varphi(a)$ ne dépend pas de $a \in \dot{a}$. En outre $\bar{\varphi}$ est un morphisme d'anneaux.*

On a donc construit un morphisme $\bar{\varphi}$ à partir d'un morphisme φ vérifiant $\varphi(I) = 0$. Réciproquement, montrons comment construire un φ à partir d'un $\bar{\varphi}$.

Proposition 66. *Soit $\bar{\varphi} : A/I \to B$ un morphisme d'anneaux. Soit $p : A \to A/I$, $a \mapsto \dot{a}$ la projection naturelle. Alors la composition $\varphi = \bar{\varphi} \circ p : A \to B$ est un morphisme d'anneaux tel que $\varphi(I) = 0$.*

Démonstration. On sait que p est un morphisme d'anneaux et que la composition de morphismes est un morphisme. Et $\varphi(I) = \bar{\varphi} \circ p(I) = \bar{\varphi}(\dot{0}) = 0$.

■

Résumons le contenu des deux propositions précédentes. Dans la première, on construit un morphisme $\bar{\varphi}$ à partir d'un φ, tandis que dans la seconde on construit un φ à partir d'un $\bar{\varphi}$. On peut vérifier que les deux constructions sont inverses l'une de l'autre. Nous avons donc montré qu'il y avait équivalence entre les deux données suivantes:

- un morphisme $\varphi : A \to B$ vérifiant $\varphi(I) = 0$.
- un morphisme $\bar{\varphi} : A/I \to B$.

Cette correspondance entre les φ et les $\bar{\varphi}$ est souvent formulée dans le théorème suivant.

Théorème 67. *Soit A un anneau, $I \subset A$ un idéal. Pour tout morphisme d'anneaux $\varphi : A \to B$ tel que $\varphi(I) = 0$, il existe un et un seul morphisme d'anneaux $\bar{\varphi} : A/I \to B$ tel que $\varphi = \bar{\varphi} \circ p$.*

Ce théorème peut être retenu à l'aide de la représentation graphique

suivante.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ p\downarrow & \nearrow \bar{\varphi} & \\ A/I & & \end{array}$$

Si on se donne la flèche diagonale $\bar{\varphi}$, on retrouve la flèche horizontale par composition, et cette flèche horizontale envoie l'idéal I sur 0. Réciproquement, si on se donne une flèche horizontale φ qui envoie I sur 0, alors il existe une unique flèche diagonale $\bar{\varphi}$ qui fait commuter le diagramme (ie. tq la flèche horizontale soit la composition des deux autres flèches).

Exercice 45. Soient A et B deux anneaux et $I \subset A$ un idéal. Considérons la correspondance entre les morphismes $\varphi : A \to B$ et les morphismes $\bar{\varphi} : A/I \to B$ donnée par le cours.
a)Montrer que φ est surjective ssi $\bar{\varphi}$ est surjective.
b)Montrer que $\bar{\varphi}$ est injective ssi $Ker\ \varphi = I$.

Correction 45.
a)Si $\bar{\varphi}$ est surjectif, alors φ est la composition de deux morphismes surjectifs donc est surjectif. Réciproquement si φ est surjectif, tout élément $b \in B$ s'écrit $\varphi(a) = \bar{\varphi}(p(a))$. Tout élément de B s'écrit donc comme $\bar{\varphi}$ d'un certain élément, ce qui prouve la surjectivité de $\bar{\varphi}$.
b)Supposons $\bar{\varphi}$ injective. Soit $a \in A$ un élément tel que $0 = \varphi(a) = \bar{\varphi}(p(a))$. On a donc $p(a) = 0$ par injectivité de $\bar{\varphi}$, ce qui signifie $a \in Ker\ p = I$. Réciproquement, si $a \in I$, $\varphi(a) = \bar{\varphi}(p(a)) = \bar{\varphi}(0) = 0$. Donc on a montré $\bar{\varphi}$ injective implique $Ker\ \varphi = I$. Supposons maintenant $Ker\ \varphi = I$. Soit $p(a) = \dot{a} \in Ker\ \bar{\varphi}$. Alors $0 = \bar{\varphi}(\dot{a}) = \varphi(a)$. Donc $a \in I$ par hypothèse sur le noyau de φ, donc $\dot{a} = \dot{0}$. Donc $\bar{\varphi}$ est injective puisque son noyau est réduit à $\dot{0}$.

On peut également retenir l'énoncé intuitivement de la façon suivante. On peut penser que $\mathbb{Z}/n\mathbb{Z}$, c'est comme $\mathbb{Z}$ hormis le fait que l'on peut remplacer n par 0. Par exemple, dans $\mathbb{Z}/5\mathbb{Z}$, on a $\dot{8} = \dot{3} + \dot{5} = \dot{3} + \dot{0} = \dot{3}$. De même, dans l'anneau quotient A/I, on peut penser que cela revient à faire des calculs dans l'anneau A, mais que chaque fois que l'on trouve un élément de I, on a le droit de dire qu'il est nul. Si on pense que l'anneau A/I est une version de A dans laquelle les éléments de I sont nuls, se donner un morphisme $A/I \to B$ revient à se donner $A \to B$ en envoyant $I = 0$ sur 0. Bien sûr, ce n'est qu'une explication "avec les mains", pour retenir l'énoncé. Le seul énoncé précis est celui du théorème et l'explication rigoureuse est celle qui précède le théorème.
Pensons maintenant à l'ensemble $\mathbb{C}$ des nombres complexes. On fait des

calculs (addition,multiplication) avec des expressions de la forme $a + bi$, en remplacant i^2 par -1 quand on le peut. On a donc $i^2 = -1$, ou encore $i^2 + 1 = 0$. Cela revient donc à travailler avec une nouvelle variable i et à décréter que $i^2 + 1 = 0$. Travailler avec une nouvelle variable que l'on peut appeler X, revient à travailler dans $\mathbb{R}[X]$ au lieu de $\mathbb{R}$. Ensuite, choisir de dire que $X^2 + 1 = 0$ revient à dire qu'on quotiente par l'idéal $(X^2 + 1)$. On s'attend donc que l'anneau $\mathbb{C}$ soit isomorphe à l'anneau quotient $\mathbb{R}[X]/(X^2 + 1)$. C'est ce qu'affirme l'exercice suivant.

Exercice 46. Montrer que $\mathbb{C}$ est isomorphe à l'anneau quotient $\mathbb{R}[X]/(X^2+1)$. On pourra procéder de la manière suivante. Considérer le morphisme d'anneaux $f : \mathbb{R}[X] \to \mathbb{C}$ qui envoie un polynôme P sur son évaluation $P(i)$ obtenue par substitution de X en i. Montrer que ce morphisme se factorise en l'isomorphisme voulu.

Correction 46. Le morphisme f envoie X^2+1 sur $i^2+1 = 0$. Maintenant si $P = \mu(X^2+1)$ est un multiple de X^2+1, il s'envoie sur $f(\mu)f(X^2+1) = f(\mu).0 = 0$. Autrement dit, l'idéal $(X^2 + 1)$ formé des multiples de $X^2 + 1$ s'envoie sur 0. Par propriété universeselle du quotient, on peut donc obtenir par factorisation un morphisme $\bar{f} : \mathbb{R}[X]/(X^2 + 1) \to \mathbb{C}$. Le morphisme f est surjectif: tout complexe $a + ib$ est l'image de l'élément $a + Xb$. Donc $\bar{f}$ est également surjectif d'après le cours. Pour montrer que $\bar{f}$ est injectif, il faut voir que le noyau de f est l'idéal $(X^2 + 1)$. Soit P un polynôme. Effectuons la division $P = (X^2 + 1).Q + R$ où $R = a + bX$ est un polynôme de degré au plus un. On a $\varphi(P) = 0.\varphi(Q) + a + bi = a + ib$. Donc P est dans le noyau ssi $R = 0$. Autrement dit, le noyau est bien l'ensemble $(X^2 + 1)$ des multiples de P.

3.4 Anneau produit et théorème chinois

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un anneau ayant n éléments. Y a-t-il un autre anneau ayant n éléments ? La réponse est non pour $n = 1, 2$ ou 3 comme on l'a vu au premier chapitre. En revanche, on a vu qu'il y avait deux anneaux distincts à quatre éléments, $\mathbb{Z}/4\mathbb{Z}$ et un autre anneau que l'on a appelé $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Cet anneau est un cas particulier de ce qu'on appelle un anneau produit.

Définition-Proposition 68. *Soient A et B deux anneaux. L'ensemble $A \times B$ muni de l'addition $(a, b)+(a', b') = (a+a', b+b')$ et de la multiplication $(a, b)(a', b') = (aa', bb')$ est un anneau dont le neutre pour l'addition est $(0_A, 0_B)$ et le neutre pour la multiplication est $(1_A, 1_B)$. On l'appelle anneau produit de A et de B.*

Pour se familiariser, une vérification facile.

Exercice 47. Ecrire les tables de multiplication et d'addition de l'anneau produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Correction 47.

+	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(0,0)	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(1,1)	(1,1)	(0,2)	(1,2)	(1,0)	(0,1)	(0,0)
(0,1)	(0,1)	(1,2)	(0,2)	(0,0)	(1,1)	(1,0)
(0,2))	(0,2)	(1,0)	(0,0)	(0,1)	(1,2)	(1,1)
(1,0)	(1,0)	(0,1)	(1,1)	(1,2)	(0,0)	(0,2)
(1,2)	(1,2)	(0,0)	(1,0)	(1,1)	(0,2)	(0,1)

.	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(0,1)	(0,2)	(1,0)	(1,2)
(0,1)	(0,0)	(0,1)	(0,1)	(0,2)	(0,0)	(0,2)
(0,2)	(0,0)	(0,2)	(0,2)	(0,1)	(0,0)	(0,1)
(1,0)	(0,0)	(1,0)	(0,0)	(0,0)	(1,0)	(1,0)
(1,2)	(0,0)	(1,2)	(0,2)	(0,1)	(1,0)	(1,1)

Pour l'anneau $A = \mathbb{Z}$ ou pour un quotient $A = B/I$, on a expliqué comment définir un morphisme $A \to C$ (propriété universelle de $\mathbb{Z}$ et des quotients). Quand A est un produit, il sera facile de se donner un morphisme dans l'autre sens $C \to A$, comme le précise la propriété universelle des produits.

Théorème 69. ***Propriété universelle du produit.*** *Soient A, B, C trois anneaux. Soit $\varphi = (\varphi_1, \varphi_2) : C \to A \times B$ une application et $\varphi_1 : C \to A$, $\varphi_2 : C \to B$ les composantes de la fonction φ. Alors φ est un morphisme d'anneaux ssi φ_1 et φ_2 sont des morphismes d'anneaux.*

En substance, ce théorème nous dit donc comment se donner un morphisme φ dans un produit: il faut se donner deux morphismes φ_1 et φ_2.
Voici immédiatement une application.

Exercice 48.
a)Montrer qu'il existe un unique morphisme $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
b)Décrire explicitement l'image de chaque élément.
c)Montrer que ce morphisme est un isomorphisme.

Correction 48.
a)Si un morphisme d'anneaux existe, l'image de $\dot{1}$ est le neutre multiplicatif de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, à savoir $(\dot{1}, \dot{1})$. Puisque $6.\dot{1} = (\dot{6}, \dot{6}) = (\dot{0}, \dot{0})$ est le neutre additif, par propriété universelle de $\mathbb{Z}/6\mathbb{Z}$, il existe un unique morphisme $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
b)Si f est le morphisme, on a $f(\dot{0}) = (\dot{0}, \dot{0})$, $f(\dot{1}) = (\dot{1}, \dot{1})$, $f(\dot{2}) = (\dot{0}, \dot{2})$, $f(\dot{3}) = (\dot{1}, \dot{0})$, $f(\dot{4}) = (\dot{0}, \dot{1})$, $f(\dot{5}) = (\dot{1}, \dot{2})$.
c)Il est clair d'après la question précédente que ce morphisme est injectif et surjectif.

Exercice 49.
a)Construire un morphisme $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
b)Montrer que ce morphisme n'est pas un isomorphisme.
c)Montrer que les anneaux $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.

Correction 49.
a)En raisonnant exactement comme dans l'exercice précédent, on obtient un unique morphisme $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, qui est donné par les formules: $f(\dot{0}) = (\dot{0}, \dot{0})$, $f(\dot{1}) = (\dot{1}, \dot{1})$, $f(\dot{2}) = (\dot{0}, \dot{0})$, $f(\dot{3}) = (\dot{1}, \dot{1})$.
b)Le morphisme n'est pas injectif puisque $\dot{0}$ et $\dot{2}$ ont la même image.
c)Si les deux anneaux étaient isomorphes, il existerait par définition un isomorphisme $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mais par propriété universelle de $\mathbb{Z}/4\mathbb{Z}$, un tel morphisme s'il existe est unique, et c'est donc celui construit dans la première question. Or on a vu que ce morphisme n'était pas un isomorphisme.

Les deux exercices précédents montrent que parfois $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ et parfois non. Le théorème suivant donne une condition suffisante pour que l'isomorphisme ait lieu.

Théorème 70. ***Théorème Chinois des Restes.*** *Si n et m sont premiers entre eux. Alors $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ sont isomorphes.*

Démonstration. On sait par la propriété universelle de $\mathbb{Z}$ (théorème 14) qu'il existe un unique morphisme $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Celui-ci envoie nm sur 0 donc par propriété universelle de $\mathbb{Z}/nm\mathbb{Z}$, 63, il se factorise en un morphisme $\varphi_1 : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. De même, on dispose d'un morphisme $\varphi_2 : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Par propriété universelle du produit, l'application $\varphi : x \mapsto (\varphi_1(x), \varphi_2(x))$ est un morphisme d'anneaux. En formules $\varphi(\dot{k}) = (\dot{k}, \dot{k})$ (la notation est un peu curieuse ici: le premier $\dot{k}$ représente la classe de k dans $\mathbb{Z}/nm\mathbb{Z}$, tandis que les deuxième et troisième $\dot{k}$ représentent la classe dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$). On veut voir que φ est un isomorphisme,

c'est à dire bijectif. Comme l'ensemble de départ et d'arrivée ont même cardinal, il suffit de voir que l'application est injective. Un élément $\dot{k}$ s'envoie sur 0 par φ_1 si k est multiple de n, et s'envoie sur 0 par φ_2 si k est multiple de m. Donc $\dot{k}$ s'envoie sur $(0,0)$ par φ si k est multiple de $ppcm(n,m) = nm$. Mais cela signifie que $\dot{k} = 0$ dans $\mathbb{Z}/nm\mathbb{Z}$. Seul 0 s'envoie par φ sur $(0,0)$: le morphisme est bien injectif. ■

Exercice 50. Montrer que la réciproque du théorème chinois des restes est vraie, à savoir que si n et m ne sont pas premiers entre eux, alors les anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ ne sont pas isomorphes.

Correction 50. Il suffit de raisonner comme dans l'exercice où l'on a montré que $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes. Soient donc n et m non premiers entre eux, leur ppcm p est strictement plus petit que le produit nm. Si les anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ sont isomorphes, l'isomorphisme $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est unique par propriété universelle de $\mathbb{Z}/nm\mathbb{Z}$, et ce morphisme envoie $\dot{p}$ et $\dot{0}$ sur la même image $(\dot{0},\dot{0})$, ce qui montre que ce morphisme n'est pas injectif. Contradiction.

3.5 Intégrité et structure de corps sur $\mathbb{Z}/n\mathbb{Z}$

On rappelle la définition suivante.

Définition 71. *corps Un corps est un anneau A dans lequel les éléments 0 et 1 sont distincts et dans lequel tout élément non nul x admet un inverse x^{-1} pour la multiplication.*

Exercice 51.
a)Montrer qu'un corps est un anneau intègre.
b)Donner un exemple d'anneau intègre qui n'est pas un corps.

Correction 51.
a)Si $ab = 0$, montrons que a ou b est nul. Si $a = 0$, on a gagné. Sinon, puisqu'on est dans un corps, a admet un inverse $\frac{1}{a}$ et en multipliant chaque côté de l'égalité par cet inverse, on trouve $b = 0$.
b)$\mathbb{Z}$ par exemple.

Pour les anneaux de la forme $\mathbb{Z}/n\mathbb{Z}$, il est équivalent d'être intègre ou d'être un corps.

Théorème 72. *Soit $n \geq 2$ un entier . Les conditions suivantes sont équivalentes.*

- *n est premier*
- *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*
- *$\mathbb{Z}/n\mathbb{Z}$ est intègre.*

Démonstration. On adopte le schéma de démonstration $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.
Si n est premier, montrons que tout $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$ non nul admet un inverse. Si $\dot{x}$ est non nul, x n'est pas un multiple de n, donc il est premier avec n puisque n est premier. Alors par Bezout, on peut trouver une relation $ax + bn = 1$, ce qui donne $\dot{a}\dot{x} = \dot{1}$.
Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors il est intègre comme on l'a vu en exercice.
Pour montrer que si $\mathbb{Z}/n\mathbb{Z}$ est intègre, alors n est premier, on procède par contraposée. Si $n = pq$, alors dans $\mathbb{Z}/n\mathbb{Z}$, $\dot{0} = \dot{n} = \dot{p}\dot{q}$, ce qui contredit l'intégrité. ■

ExoTD 5.
c)*Calculer l'inverse de* 13 *dans* $\mathbb{Z}/20\mathbb{Z}$
d)*Calculer l'inverse de* 15 *dans* $\mathbb{Z}/8\mathbb{Z}$

correcTD 5.
e)*On commence par calculer une relation de Bezout.*

- *20=1.13+7*
- *13=1.7+6*
- *7=1.6+1*
- *6=6.1+0*

Donc le pgcd de 7 *et* 13 *est* 1 *(le dernier reste non nul trouvé). On remplace dans cette dernière ligne à reste non nul* 6 *par son expression venant de la deuxième, ie. on remplace* 6 *par* $13-7$. *On trouve* $1 = 7-6 = 7-(13-7) = 2.7-13$, *ce qui nous donne une nouvelle expression de* 1 *en fonction des termes* 7 *et* 13. *Enfin on remplace* 7 *par* $20-13$ *qui vient de la première ligne. On trouve* $1 = 2.20-3.13$. *C'est la relation de Bezout cherchée. En passant dans* $\mathbb{Z}/20\mathbb{Z}$, *on trouve* $\dot{1} = -\dot{3}.\dot{1}3$. *L'inverse de* $\dot{1}3$ *est donc* $-\dot{3} = \dot{1}7$.
f)*On peut procéder comme dans la première question. On peut aussi raisonner comme suit.* $\dot{1}5 = -\dot{1}$ *dans* $\mathbb{Z}/8\mathbb{Z}$. *Et l'inverse de* $-\dot{1}$ *et* $-\dot{1}$. *Donc l'inverse de* $\dot{1}5$ *est* $-\dot{1} = \dot{7}$.

On aimerait compter le nombre d'éléments $x \in \mathbb{Z}/n\mathbb{Z}$ admettant un inverse multiplicatif x^{-1}.Notons $\varphi(n)$ ce nombre.

D'après le théorème, quand n est premier, tous les éléments non nuls x admettent un inverse x^{-1}. Bien sûr 0 n'a pas d'inverse (pourquoi ?). Donc $\varphi(n) = n - 1$ quand n est premier.
Quand n n'est pas premier, il y au moins l'élément 1 qui est inversible d'inverse 1. Comme tous les éléments non nuls ne sont pas inversibles, on a l'inégalité $1 \leq \varphi(n) \leq n - 2$.
Pour aller plus loin, commençons par l'exemple $n = 4$ qui est le premier nombre non premier que l'on rencontre. C'est en fait une puissance de nombre premier pour laquelle nous pouvons utiliser le résultat suivant.

Proposition 73. *Soit $0 \leq k < n$. L'élément $\dot{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible ssi k et n sont premiers entre eux. En particulier le nombre $\varphi(n)$ d'inversibles dans $\mathbb{Z}/n^\alpha\mathbb{Z}$ est $n^\alpha - n^{\alpha-1} = n^\alpha(1 - \frac{1}{n})$.*

Démonstration. Si k et n sont premiers entre eux, alors par Bezout, $ak + bn = 1$, ce qui implique dans $\mathbb{Z}/n\mathbb{Z}$: $\dot{a}\dot{k} = \dot{1}$, d'où l'inversibilité de $\dot{k}$. Si k et n ne sont pas premiers entre eux, il existe un nombre a plus petit que n tel que ak soit un multiple de n (prendre par exemple $a = \frac{ppcm(k,n)}{k}$). Donc dans $\mathbb{Z}/n\mathbb{Z}$, $\dot{a}\dot{k} = 0$, avec $\dot{a} \neq 0$. L'élément $\dot{k}$ étant diviseur de 0, il ne peut être inversible d'après l'exercice suivant.
Dans $\mathbb{Z}/n^\alpha\mathbb{Z}$, les éléments non inversibles sont donc ceux qui ne sont pas premiers avec n^α, c'est à dire les multiples de n: $(0, n, 2n, \ldots, n(n^{\alpha-1} - 1) = n^\alpha - n)$. Il y a $n^{\alpha-1}$ tels éléments. Les inversibles sont tous les autres. Il y en a donc $n^\alpha - n^{\alpha-1}$. ■

Par exemple pour $n = 4$ nous avons $\varphi(4) = 2^2 - 2^1 = 2$.

Exercice 52.
a)Un élément $a \in A$ d'un anneau est appelé diviseur de 0 s'il existe $b \in A$ non nul tel que $ab = 0$. Montrer qu'un diviseur de 0 dans un anneau n'est jamais inversible.
b)Vérifier à la main que la formule $\varphi(4) = 2$ est correcte en décrivant explicitement les deux inversibles de $\mathbb{Z}/4\mathbb{Z}$ et en donnant leur inverse. Montrer que les deux autres éléments sont non inversibles en montrant qu'ils sont diviseurs de 0.

Correction 52.
a)Par l'absurde, supposons a diviseur de 0 et inversible. Soit b non nul tel que $ab = 0$. En multipliant par l'inverse $\frac{1}{a}$ de a de chaque côté de l'égalité, on trouve $b = 0$. Contradiction.
b)$\dot{0}$ et $\dot{2}$ sont diviseurs de 0 car si on les mulitiplie par $\dot{2} \neq \dot{0}$, on trouve $\dot{0}$.

D'autre part $\dot{1}$ et $\dot{3}$ sont inversibles d'inverse respectif $\dot{1}$ et $\dot{3}$. On a donc bien $\varphi(4) = 2$.

Puisque $n = 5$ est premier, $\varphi(5) = 5-1 = 4$. Le nombre suivant qui pose problème est $n = 6$. Nous pouvons dans ce cas utiliser le résultat suivant laissé en exercice.

Exercice 53.
a)Un élément (a, b) est inversible dans un anneau produit $A \times B$ ssi ($a \in A$ est inversible et $b \in B$ est inversible).
b)Si A et B sont des ensembles finis, quel est le nombre d'éléments inversibles dans $A \times B$?
c)Quel est le nombre d'inversibles dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$?

Correction 53.
a)Supposons (a, b) inversible et notons (c, d) son inverse. Alors $(a, b)(c, d) = (1, 1)$ ce qui implique $ac = 1$ et $bd = 1$, donc a et b sont inversibles d'inverses c et d. Réciproquement, si a et b sont inversibles d'inverses c et d, alors (a, b) est inversible d'inverse (c, d).
b)D'après la question précédente, c'est le produit du nombre d'inversibles dans A par le nombre d'inversibles de B.
c)Le nombre d'inversible de $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ est $\varphi(n)\varphi(m)$ d'après la question précédente.

Par le théoreme chinois, $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. Par l'exercice précédent, le nombre d'inversibles dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est $\varphi(2)\varphi(3)$. Donc $\varphi(6) = \varphi(2)\varphi(3) = 1.2 = 2$.
On a maintenant toutes les cartes en main pour démontrer la formule suivante.

Théorème 74. *Soit $n = n_1^{a_1} \dots n_k^{a_k}$ la décomposition d'un élément $n \in \mathbb{N}$ en puissance de nombres premiers distincts. Le nombre $\varphi(n)$ d'inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est le produit $n(1 - \frac{1}{n_1})(1 - \frac{1}{n_2}) \dots (1 - \frac{1}{n_k})$*

Démonstration. Par le théorème chinois, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n_1^{a_1} \times \dots \times \mathbb{Z}/n_k^{a_k}$. Par l'exercice précédent, on a donc $\varphi(n) = \varphi(n_1^{a_1}) \dots \varphi(n_k^{a_k})$. Par la dernière proposition, cette quantité est aussi $n_1^{a_1}(1 - \frac{1}{n_1})n_2^{a_2}(1 - \frac{1}{n_2}) \dots n_k^{a_k}(1 - \frac{1}{n_k})$.

■

Exemple 75. *Puisque $200 = 2^3.5^2$, le nombre d'inversibles dans $\mathbb{Z}/200\mathbb{Z}$ est $200.(1 - \frac{1}{2})(1 - \frac{1}{5}) = 80$.*

Remarque 76. *Ce théorème n'est pas un théorème dont il faut retenir la formule, mais dont il faut retenir la démonstration pour l'appliquer.*

3.6 Application à la cryptographie

Nous allons maintenant appliquer nos connaissances sur $\mathbb{Z}/n\mathbb{Z}$ à la cryptographie. Le défi est le suivant. Deux personnes A et B communiquent entre elles sans s'être jamais rencontrées auparavant. Une tierce personne C peut écouter tous les messages échangés entre A et B. Pourtant, C ne peut pas connaître l'information échangée entre A et B. Cela paraît impossible ! Et pourtant...

Remarquons que cela se passe tous les jours sur Internet. Quand nous effectuons des achats en ligne, nous envoyons notre numéro de carte bancaire à un site. Il est possible à un tiers C d'écouter les informations échangées entre notre ordinateur et le site. Et pourtant la personne qui écoute ne peut savoir notre numéro de carte. Ce petit miracle repose sur la théorie des anneaux $\mathbb{Z}/n\mathbb{Z}$.

Historiquement, pour empêcher le décodage par C, A et B se mettaient d'accord en secret sur le procédé de cryptage du message (Il y a à ce sujet des anecdotes lors de la deuxième guerre mondiale). Mais cette démarche est très lourde du point de vue organisationnel. Si aujourd'hui, nous faisons des achats par Internet et que nous envoyons de façon cryptée notre numéro de carte, nous n'allons pas avant chaque achat rencontrer physiquement un responsable du site pour nous mettre d'accord sur un système de cryptage... Les logiciels de A et de B commencent par se mettre d'accord sur un système de cryptage. Bien sûr C peut intercepter ce message puisque les messages entre A et B ne sont pas encore cryptés. Ensuite, quand A et B se sont mis d'accord, A envoie des données cryptées à B et C intercepte de nouveau le message. Le système doit être tel que C, qui connait à la fois le message crypté et le système de cryptage, ne puisse décrypter.

On va alors mettre en place un système fonctionnant de la façon suivante. B publie une clé dans un annuaire public (ou de façon équivalente, le logiciel de B envoie un nombre au logiciel de A et ce nombre peut être lu par tout le monde, y compris le méchant C). Quand A veut envoyer un message m à B, il envoie un message codé qui est fonction de m et de la clé publique de B. Si C intercepte le message, comme il connait le moyen de codage public, il pourrait en théorie le décoder. La nuance est subtile ici. En théorie, effectivement, C pourrait décoder le message. En pratique, cependant, le temps de calcul nécessaire pour décoder le message est beaucoup trop grand. Le

codage et le décodage ne sont pas des opérations symétriques en termes de temps. Prenons l'exemple suivant. Si je vous demande de faire la multiplication 47*53, il vous suffit de quelques secondes pour poser l'opération sur une feuille de papier et trouver le résultat 2491. Si en revanche, je vous donne le nombre 2491 et que je vous demande de retrouver les facteurs, il vous faudra beaucoup de temps. Pour le décomposer en produit de nombre premiers, vous aller d'abord voir s'il est divisible par 2, par 3, par 5 etc ... Autrement dit les deux opérations

- faire un produit de deux nombre premiers
- trouver les facteurs d'un produit de deux nombres premiers

sont deux opérations inverses l'une de l'autre qui ne sont pas du tout équivalentes en terme de temps. Par exemple, un ordinateur sait trouver un nombre premier dont l'écriture prend une centaine de chiffres et faire le produit de deux tels nombres. Mais si vous lui donnez le produit de deux tels nombres, le temps de calcul nécessaire pour retrouver les facteurs est de l'ordre de millions d'années avec les ordinateurs d'aujourd'hui. Le point clé est donc le suivant. B choisit deux nombres premiers très grands. La clé publique publié par B est le produit de ces deux nombres premiers très gros. Pour pouvoir décoder le message, il faut connaitre chacun des facteurs. C ne peut calculer chacun des facteurs et ne peut décoder. En revanche B les connait et peut décoder. C'est cette asymétrie d'information qui fait que B peut décoder le message envoyé par A et donc connaître ce message, alors que C ne le peut pas.
Notons avant de voir les détails du cryptage-décryptage les implications pratiques de la démarche. Tout d'abord, supposons que C trouve le moyen de casser la clé de B (ie. de trouver les deux facteurs du produit) pour quelque raison que ce soit (vol de son ordinateur, progrès des méthodes mathématiques de factorisation et des ordinateurs...) , et donc qu'il puisse décoder les messages destinés à B. Alors il suffit à B quand il s'en aperçoit de publier une nouvelle clé dans l'annuaire. Il n'y a plus besoin que B et A se rencontrent en secret pour pouvoir de nouveau échanger des messages privés.
Si tout ceci vous semble un peu gratuit et artificiel, détrompez vous ! Les système que nous allons présenter maintenant, appelé système RSA du nom de ses inventeurs (Rivest,Shamir,Adleman) est utilisé en pratique dans les communications interbancaires par exemple. Il repose sur le fait, convaincant sur les exemples mais non démontré mathématiquement (!), que faire un produit de nombres est plus facile que de factoriser un nombre. Rien n'interdit de penser qu'un jour quelqu'un trouvera un algorithme rapide de

factorisation. Des mathématiciens travaillent sur la notion de complexité pour démontrer en un sens mathématique précis qu'effectuer une factorisation est un problème plus complexe qu'effectuer un produit, ce qui donnerait une base théorique à l'algorithme RSA. Les connaissances mathématiques actuelles ne permettent pas de trancher. Notons enfin que si un algorithme de factorisation simple existait, il existe d'autres systèmes de cryptage à clé publique sur lesquels on pourrait se rabattre. Néanmoins, les coûts de réorganisation, le temps nécessaire pour mettre en place la nouvelle structure provoqueraient un flottement difficilement évaluable.
Quand A veut envoyer un message à B, il commence par le transformer en un nombre par un moyen quelconque, tout comme les mots de ce texte sont stockés sur le disque dur par une suite de 0 et de 1. Donc on peut imaginer que A va envoyer à B un nombre, disons inférieur à n pour fixer les idées. Mais se donner un nombre plus petit que n revient à se donner un élément x de $\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \dot{n-1}\}$. Au lieu d'envoyer x, A va envoyer le nombre codé x^e où e est un entier. Décoder signifie trouver un moyen de calcul de la fonction inverse de $x \mapsto x^e$. La proposition suivante explique comment faire le décodage dans le cas où n est un nombre premier et où e est premier avec $n-1$. On rappelle que si e est premier avec $n-1$, alors $\dot{e}$ est inversible dans $\mathbb{Z}/(n-1)\mathbb{Z}$.

Proposition 77. *Soit n un nombre premier et $1 \leq e < n$ avec $pgcd(e, n-1) = 1$. Soit k un entier tel $\dot{e}\dot{k} = \dot{1}$ dans $\mathbb{Z}/(n-1)\mathbb{Z}$. Alors les applications $x \mapsto x^e$ et $x \mapsto x^k$ sont inverses l'une de l'autre.*

Démonstration. Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ forment un groupe, qui est de cardinal $n-1$. La théorie des groupes (théorème de Lagrange) nous dit que l'ordre de tout élément divise le cardinal du groupe, ce qui signifie dans notre cas que pour tout $x \neq 0 \in \mathbb{Z}/n\mathbb{Z}$, $x^{n-1} = 1$. La composée des fonctions $x \mapsto x^k$ et $x \mapsto x^e$ est la fonction $x \mapsto x^{ek}$, et par hypothèse $ek = 1 + (n-1)a$ pour un certain a. Donc $x^{ek} = x(x^{n-1})^a = x1^a = x$. La composition des deux fonctions est donc bien la fonction identité. ∎

En pratique, A veut envoyer le message m. Il envoie le message codé $M = m^e$ à B. Pour décoder B calcule par un algorithme de Bezout le nombre k puis M^k qui est le message initial de A.

Exercice 54. Avec les notations du cours, supposons que $n = 17$ et que A veuille envoyer le nombre 3 à B. Il lui envoie $\dot{3}^5 = \dot{5}$. Calculer le nombre k utilisé par B pour décoder et vérifier qu'on a bien $\dot{5}^k = \dot{3}$.

Correction 54. Commençons par calculer l'inverse de 5 dans $\mathbb{Z}/16\mathbb{Z}$. On peut faire avec l'algorithme de Bezout (cf. les autres exercices; et je vous conseille d'ailleurs de vérifier que vous savez appliquer cette méthode systématique). On peut aussi ruser. On remarque que $\dot{5}.\dot{3} = \dot{1}5 = -\dot{1}$. Donc $\dot{5}.(-\dot{3}) = \dot{1}$. L'inverse de 5 dans $\mathbb{Z}/16\mathbb{Z}$ est $-\dot{3} = \dot{1}3$. On prend donc $k = 13$. Dans $\mathbb{Z}/17\mathbb{Z}$, on a On a $\dot{5}^{13} = ((\dot{5}^2)^2)^3.\dot{5} = (\dot{8}^2)^3.\dot{5} = (-\dot{4})^3.\dot{5} = \dot{4}.\dot{5} = \dot{2}0 = \dot{3}$ comme annoncé.

Évidemment, ici nous n'avons pas encore tout à fait atteint notre but. Si C intercepte le message, il connait la clé publique e de B et peut tout comme B calculer le nombre k et donc décoder. On modifie alors notre procédure de codage-décodage pour que seul B puisse décoder.

Proposition 78. *Soient p, q deux nombres premiers et $n = pq$. Soit e un nombre premier à $(p-1)(q-1)$. Alors il existe un entier k tel que $\dot{e}\dot{k} = \dot{1}$ dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$. En outre, la fonction $x \to x^e$ de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même est inversible d'inverse $x \to x^k$.*

Démonstration. Puisque e est premier à $(p-1)(q-1)$, il est inversible dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$, d'où l'existence de l'entier k tel que $\dot{e}\dot{k} = \dot{1}$. Par le théorème chinois, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et au lieu de raisonner sur $\mathbb{Z}/n\mathbb{Z}$, on peut raisonner successivement sur chaque composante $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$. Il nous faut donc vérifier que les applications $x \mapsto x^e$ et $x \mapsto x^k$ sont des applications inverses dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$. Mais comme p et q sont des nombres premiers, cela résulte de la proposition précédente. ∎

Vérifions maintenant que nous avons atteint notre but, ie. que A peut envoyer un message qui ne soit décodable que par B. On note que e est la clé de codage et k la clé de décodage. Puisque B connaît les nombres p et q, il connait le nombre $(p-1)(q-1)$, donc il peut calculer l'inverse $\dot{k}$ de e dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$ par l'algorithme de Bezout comme dans l'exercice précédent. En revanche, C ne connait pas p et q, donc il connait le nombre $n = pq$ mais pas le nombre $(p-1)(q-1)$. Il ne peut donc pas calculer la clé de décodage k.

Chapitre 4

Anneaux de polynômes

Objectif: Ce chapitre est dédié à l'étude des polynômes. On y montre que les raisonnements faits sur les entiers (factorisation en produit de nombres irréductibles, ppcm,pgcd) peuvent être généralisés aux polynômes. On décrit en particulier des algorithmes pour trouver les irréductibles et/ou les factorisations sur $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$.

4.1 Définition et premières propriétés

Définition 79. *polynôme Un polynôme à coefficients dans A est une expression formelle $a_0 + a_1X + \cdots + a_nX^n$ où les a_i sont des éléments de A. L'ensemble des polynômes à coefficients dans A est noté $A[X]$.*

Bien sûr, se donner cette expression formelle équivaut à se donner la suite de coefficients $(a_0, a_1, \ldots, a_n, 0, 0 \ldots)$. On trouve donc souvent comme définition:

Définition 80. *Un polynôme à coefficients dans A est une suite de coefficients de A, $(a_0, a_1, \ldots,)$ nulle à partir d'un certain rang. On emploie la terminologie "suite presque nulle" pour désigner une suite nulle à partir d'un certain rang.*

La première définition est un peu vague. Qu'est ce qu'une "expression formelle" ? Est-ce que les polynômes $1 + X$ et $1 + X + 0X^2$ sont égaux ? La réponse est oui car d'après la deuxième définition ces deux polynômes correspondent à la suite $(1, 1, 0, 0, \ldots)$. Néanmoins, penser à la première définition est plus intuitif. Pour multiplier $(1 + X)$ par X, on devine que le resultat va être $X+X^2$, ce qui est plus intuitif que si l'on vous dit, que la multiplication de la suite $(1, 1, 0, 0, \ldots)$ par $(0, 1, 0, 0, \ldots)$ est $(0, 1, 1, 0, 0, \ldots)$.

En résumé, la définition rigoureuse est la deuxième, mais la première est la plus mnémotechnique.
Pour l'instant les polynômes à coefficients dans A ne forment qu'un ensemble. On veut les munir d'une structure d'anneau. Pour cela, il faut définir une addition et une multiplication.

Définition 81. *Soit A un anneau. On définit les lois d'addition et de multiplication sur $A[X]$ par les formules suivantes. Si (a_n) et (b_n) sont des suites presque nulles, la somme (c_n) et la multiplication (d_n) des suites (a_n) et (b_n) sont les suites définies par:*

- $c_n = a_n + b_n$
- $d_n = \sum_{i=0}^{n} a_i b_{n-i}$

Bien sûr, les opérations d'addition et de multiplication ont été choisies sur les suites de sorte que lorsque l'on écrit ces suites sous la forme $a_0 + a_1X + \dots$, alors on peut développer la somme et le produit comme on s'y attend. Faisons une petite vérification pour s'en convaincre.

Exercice 55.
a)Écrire les suites correspondant aux polynômes $1 + X$ et $2 + 3X$ de $\mathbb{Z}[X]$. Faire le produit des suites en utilisant la définition.
b)Calculer le produit des polynômes de la manière usuelle et vérifier que l'on obtient bien le même résultat que précédemment.

Correction 55.
a)$1 + X$ correspond à la suite $(1, 1, 0, 0, \dots)$ et $2 + 3X$ à $(2, 3, 0, \dots)$. Le produit donne la suite $(2, 5, 3, 0, \dots)$.
b)Le produit donne $2 + 5X + 3X^2$ qui correspond bien à la suite ci-dessus.

Proposition 82. *L'ensemble $A[X]$ muni des opérations $+$ et $.$ précédentes est un anneau pour lesquels les éléments 0 et 1 sont respectivement les suites $(0, 0 \dots)$ et $(1, 0, 0, \dots)$.*

Démonstration. L'associativité de l'addition se vérifie aisément: si $(a_n), (b_n)$ et c_n sont des suites presques nulles alors $((a_n) + (b_n)) + (c_n)$ est la suite dont le n^{eme} terme est $(a_n + b_n + c_n)$. De même pour la somme $(a_n) + ((b_n) + (c_n))$. Donc on a bien l'associativité $((a_n) + (b_n)) + (c_n) = (a_n) + ((b_n) + (c_n))$.
De même, on vérifie en calculant le n^{eme} terme de chacune des suites se trouvant de part et d'autre de l'égalité que:

- $(a_n) + (b_n) = (b_n) + (a_n)$
- $(0, 0, \dots) + (a_n) = (a_n)$

- $(a_n)+(-a_n)=(0)$, ce qui montre que $(-a_n)$ est l'inverse de (a_n) pour le $+$.
- $((a_n)(b_n))(c_n)=(a_n)((b_n)(c_n))$
- $(1,0,\dots)(a_n)=(a_n)(1,0,\dots)=(a_n)$
- $(a_n)((b_n)+(c_n))=(a_n)(b_n)+(a_n)(c_n)$

ce qui constitue la liste des vérifications à faire pour avoir une structure d'anneau. ■

Exercice 56. Montrer que A est un sous-anneau de $A[X]$. Plus précisément, montrer que $A \to A[X]$, $a \mapsto (a,0,0,\dots) = a + 0X + 0X^2 + \dots$ est un morphisme d'anneaux injectif.

Correction 56. Il faut reprendre la liste des vérifications à effectuer pour voir qu'on a bien un morphisme d'anneaux. C'est une suite de vérifications fastidieuses et faciles que nous vous épargnons. Pour l'injectivité, il est évident que le seul élément s'envoyant sur le polynôme nul est l'élément nul.

Définition 83. *On dira qu'un polynôme de la forme $a + 0X + \dots$ est un polynôme constant. D'après l'exercice précédent, les polynômes constants forment un sous-anneau isomorphe à A, l'isomorphisme envoyant un élément $a \in A$ sur le polynôme constant $a + 0X + \dots$.*

Définition 84. *On appelle degré d'un polynôme $P = \sum a_n X^n$ le plus grand entier n tel que a_n soit non nul. Le coefficient a_n correspondent s'appelle le coefficient dominant. Par convention, le polynôme nul est de degré $-\infty$.*

Exemple: *Les polynômes de degré 0 sont les polynômes constants non nuls.* Quelle est la propriété universelle de $A[X]$? Elle est reliée à la notion de fonction polynômiale. Vous avez appris lors des années précédentes à évaluer des polynômes. Par exemple, on évalue le polynôme $2+X+X^3$ en $X=2$ et on trouve $2+2+8=12$. Autrement dit en faisant $X=2$, vous remplacez un polynôme de $\mathbb{R}[X]$ par un réel, ce qui vous donne donc une fonction evaluation au point 2, $ev_2 : \mathbb{R}[X] \to \mathbb{R}$, $P \mapsto P(2)$. On peut vérifier que cette fonction est un morphisme d'anneaux. Comment généraliser et définir un morphisme d'anneaux $A[X] \to B$? Intuitivement, vous allez dire comment envoyer A dans B par un morphisme f, puis évaluer X et lui donner une valeur $b \in B$. Alors un polynôme $a_0 + a_1X + \dots + a_nX^n$ sera envoyé sur $f(a_0) + f(a_1)b + \dots + f(a_n)b^n$. La proposition suivante dit qu'effectivement, c'est bien comme cela que l'on se donne un morphisme d'anneaux $A[X] \to B$.

Théorème 85. ***Propriété universelle de*** $A[X]$**.** *Il est équivalent de se donner*

- *un morphisme d'anneaux* $\varphi : A[X] \to B$
- *un morphisme d'anneaux* $f : A \to B$ *et un élément* $b \in B$.

Plus précisément, le morphisme d'anneaux φ *défini par le couple* (f, b) *est défini par la formule* $\varphi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} f(a_i) b^i$. *Réciproquement,* φ *définit le couple* (f, b)*:* f *est la restriction de* φ *aux polynômes constants et* b *est l'image de* X.

Démonstration. Supposons que φ soit donné. Alors $b = \varphi(X)$ est bien défini. Pour définir f, regardons le morphisme $A \to A[X]$, $a \mapsto a + 0X + \dots$. La composition $f : A \to A[X] \to B$ est bien un morphisme d'anneaux comme composé de morphismes d'anneaux. On a donc bien défini un couple (f, b) à partir de φ. Montrons réciproquement que le couple (f, b) définit un morphisme d'anneaux. Pour cela, on définit φ par la formule $\varphi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} f(a_i) b^i$. On doit vérifier que φ est bien un morphisme d'anneaux, c'est à dire que si $P = \sum a_i X^i$ et $Q = \sum c_i X^i$ sont deux polynômes, alors

- $\varphi(P + Q) = \varphi(P) + \varphi(Q)$
- $\varphi(PQ) = \varphi(Q)\varphi(Q)$
- $\varphi(1) = 1$

Le troisième point est vrai car $\varphi(1) = f(1) = 1$. Le premier l'est également car les deux termes valent $\sum (f(a_i) + f(c_i)) b^i$. Le deuxième point enfin est vrai car les deux côtés de l'égalité valent $\sum d_i b^i$ où $d_i = \sum_{j+k=i} f(a_j) f(c_k)$.

■

4.2 Polynômes et fonctions polynômiales. Zéro des polynômes

Au polynôme $X + X^2 \in \mathbb{R}[X]$ est associé la fonction de $\mathbb{R}$ dans $\mathbb{R}$: $x \mapsto x + x^2$. De même, à un polynôme de $A[X]$ est associé une fonction de A dans A

Définition 86. *Soit* A *un anneau et* $P = a_0 + \dots + a_n X^n \in A[X]$ *un polynôme. On appelle fonction polynômiale associée à* P *et on note* $\tilde{P}$ *la fonction* $A \to A$, $x \mapsto a_0 + \dots a_n x^n$.

Considérons $A = \mathbb{Z}/2\mathbb{Z}$ et $P = X(X + \dot{1}) = X + X^2$. Regardons la fonction polynômiale associée $\tilde{P} : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Elle envoie $\dot{0}$ sur $\dot{0}$ et

$\dot{1}$ sur $\dot{1} + \dot{1} = \dot{2} = \dot{0}$. Autrement dit, la fonction est la fonction nulle. Le polynôme P est-il nul ? Non, car la suite de coefficients $(\dot{0}, \dot{1}, \dot{1}, \dot{0}, \dot{0}, \dots)$ n'est pas nulle et un polynôme n'est qu'une suite de coefficients ! Néanmoins, lorsque l'anneau est un corps infini (par exemple $A = \mathbb{R}$ ou $A = \mathbb{C}$), on peut identifier les polynômes et les fonctions polynômiales comme on le montre dans la feuille d'exercices (exercice 6). Sur $\mathbb{Z}$, il n'y a pas de problème non plus.

ExoTD 6.
a)*Si A est un corps contenant un nombre infini d'éléments. La fonction $A[X] \to A^A$, définie par $P \mapsto \tilde{P}$ est un morphisme d'anneaux injectifs (en particulier, on peut assimiler polynômes et fonctions polynômiales).*
b)*Peut on généraliser dans l'identification entre polynômes et fonctions polynômiales sans les hypothèses sur A ?*

correcTD 6.
c)*D'après un exercice précédent, si on est sur un anneau intègre et si P est un polynôme non nul, $\tilde{P}$ est une fonction ayant un nombre de zéros au plus égal au degré de P. La fonction nulle ayant un nombre infini de zéros, $\tilde{P}$ n'est pas la fonction nulle. Donc le noyau du morphisme est réduit au polynôme nul, le morphisme est injectif.*
d)*Non, on ne peut généraliser car le cours donne l'exemple du polynôme $X^2 + X$ dans $\mathbb{Z}/2\mathbb{Z}[X]$ qui n'est pas nul mais tel que la fonction polynômiale associée est nulle.*

En résumé, sur les corps ou les anneaux usuels, ($\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$), vous n'avez pas trop à vous soucier de la différence entre polynômes et fonctions polynômiales. En revanche, si vous travaillez avec des anneaux un peu plus exotiques ($\mathbb{Z}/n\mathbb{Z}$), il faut faire la différence. Ceux et celles qui se sentent plus à l'aise ainsi peuvent se restreindre à ces cas où l'on peut sans problème identifier polynômes et fonctions. La différence ne sera pas importante pour la suite du cours. Nous noterons d'ailleurs $P(2)$ la valeur du polynôme en 2, plutôt que $\tilde{P}(2)$ qui serait plus rigoureux.
Sur l'anneau $\mathbb{Z}$, une technique importante était l'existence de divisions, ce qui était à la base de la détermination des idéaux de $\mathbb{Z}$. De même, dans l'anneau $A[X]$, on va pouvoir utiliser des divisions par des polynômes unitaires, ce qui s'avèrera une technique importante.

Définition 87. *On appelle polynôme unitaire un polynôme de degré n dont le coefficient dominant a_n est inversible.*

Exemple: *Les polynômes unitaires de $\mathbb{Z}[X]$ sont ceux dont le coefficient dominant vaut 1 ou -1. Si A est un corps, tout polynôme non nul de $A[X]$ est unitaire.*

Définition-Proposition 88. ***Existence d'une division par des polynômes unitaires.*** *Soit A un anneau et $Q \in A[X]$ un polynôme unitaire. Soit P un polynôme quelconque. Alors il existe deux polynômes R et $S \in A[X]$ tels que $P = QS + R$ avec $deg(R) < deg(Q)$.*

La démonstration consiste à reproduire avec moult indices ce que l'on fait sur des exemples. Donc contentons nous d'un exemple. Faisons ainsi la division de $P = X^3 + X^2$ par $Q = 2X^2 + 1$ dans $\mathbb{R}[X]$. Le terme le plus grand est en X^3. Il suffit de multiplier Q par $\frac{1}{2}X$ pour avoir le même terme dominant que P. Donc on commence, par écrire la division $P = \frac{1}{2}XQ + R_1$. On trouve facilement que $R_1 = P - \frac{1}{2}XQ_1 = X^2 - \frac{X}{2}$. En pratique, on trouve R_1 en posant la division:

$$\begin{array}{c|c} X^3 + X^2 & 2X^2 + 1 \\ X^2 - \frac{X}{2} & \hline \\ & \frac{1}{2}X \end{array}$$

On a obtenu le reste en faisant la multiplication $\frac{1}{2}X.(2X^2+1) = X^3 + \frac{1}{2}$ des deux termes se trouvant sur la droite de la division. On a changé le signe et ajouté le résultat ainsi obtenu $-X^3 - \frac{1}{2}$ à la quantité en haut à gauche. Et on a marqué le résultat du calcul juste dessous. Bref, tout se passe comme pour une division usuelle avec les entiers. Continuons la division. Il s'agit d'éliminer le terme de plus haut degré du reste, ie. d'éliminer X^2. Pour avoir un terme en X^2, il suffit de multiplier le diviseur $2X^2 + 1$ par $\frac{1}{2}$. On continue donc la division de la façon suivante.

$$\begin{array}{c|c} X^3 + X^2 & 2X^2 + 1 \\ X^2 - \frac{X}{2} & \hline \\ -\frac{X}{2} - \frac{1}{2} & \frac{1}{2}X + \frac{1}{2} \end{array}$$

On ne peut plus continuer la division puisque le degré du reste est trop petit. On s'arrête donc et on a le résultat: $X^3 + X^2 = (2X^2 + 1)(\frac{X}{2} + \frac{1}{2}) + \frac{-X-1}{2}$ qui est la division cherchée.

Exercice 57.
a)Effectuer la division de $X^2 + 3$ par $X + 1$
b)Effectuer la division de $X^5 + X^2 + 3$ par $-X^3 + 1$
c)Effectuer la division de $X^2 + 3$ par $X^3 + 1$
d)Effectuer dans $\mathbb{Z}[X]$ la division de $X^2 + 3$ par $2X + 1$.

Correction 57.
a) $X^2+3=(X-1)(X+1)+4$
b) $X^5+X^2+3=-X^2.(-X^3+1)+(2X^2+3)$
c) $X^2+3=0.(X^3+1)+(X^2+3)$
d) Impossible car le coefficient dominant 2 n'est pas inversible dans $\mathbb{Z}$.

Utilisons maintenant ces techniques de division pour caractériser les points a qui annulent un polynôme.

Corollaire 89. *Soit A un anneau et $P \in A[X]$ et $a \in A$. Alors P s'annule en a ssi $X-a$ divise P.*

Démonstration. Si $X-a$ divise P: $P=(X-a)Q$. En faisant $X=a$, on trouve $P(a)=0.Q(a)=0$. Donc P s'annule en a. Réciproquement, si P s'annule en a. Effectuons la division de P par $X-a$: $P=(X-a)Q+R$. Le degré de R doit être plus petit que celui de $(X-a)$ donc R est une constante. Maintenant, l'évaluation au point $X=a$ donne $0=P(a)=0.Q+R$. Donc $R=0$ et $X-a$ divise P. ∎

Exercice 58.
a) Soit A un anneau intègre, $P \in A[X]$ et $a_1,\dots,a_k \in A$ des éléments distincts. Si $P(a_i)=0$ pour tout i, alors le produit $(X-a_1)\dots(X-a_n)$ divise P.
b) Un polynôme non nul de degré n sur un anneau intègre A admet au plus n racines.
c) Donner un polynôme de degré n sur un anneau non intègre ayant plus de n racines.

Correction 58.
a) On raisonne par récurrence sur $k \geq 1$. Pour $k=1$, effectuons la division de P par $X-a_1$: $P=Q(X-a_1)+R$ où R est un polynôme de degré au plus 0, c'est à dire une constante. En évaluant cette égalité au point $X=a_1$, on trouve $0=P(a_1)=R$. On a donc bien $X-a_1$ divise P. Supposons maintenant l'hypothèse vraie au rang $k-1$ et supposons que $P(a_i)=0$ pour $i \leq k$. Par hypothèse de récurrence $P=(X-a_1)(X-a_2)\dots(X-a_{k-1})Q$. Évaluons cette expression en $X=a_k$. On trouve $0=P(a_k)=(a_k-a_1)(a_k-a_2)\dots(a_k-a_{k-1})Q(a_k)$. Aucun des termes a_k-a_i n'est nul, donc puisqu'on est dans un anneau intègre, il faut que $Q(a_k)=0$, ce qui implique par hypothèse de récurrence que $X-a_k$ divise Q: $Q=(X-a_k)R$. En reportant dans l'expression de P, on trouve $P=$

$(X-a_1)(X-a_2)\dots(X-a_{k-1})(X-a_k)R$, qui établit ainsi la divisibilité voulue.
b)Si P de degré n admettait $n+1$ racines distinctes $a_1,\dots,a_{n+1}$, alors $P=(X-a_1)(X-a_2)\dots(X-a_{n+1})R$ d'après la première question. Or cette égalité est impossible car le degré du terme de droite ne peut être égal au degré n du terme de gauche.
c)Prenons l'anneau $A=\mathbb{Z}/4\mathbb{Z}[T]$. Le polynôme non nul $\dot{2}X$ admet pour racines les éléments $X=2T$, $X=2T^2$, $X=2T^3$ ...

4.3 Arithmétique des polynômes

On a vu dans la section précédente que l'on pouvait faire des divisions par des polynômes unitaires et obtenir ainsi un quotient et un reste. De ce point de vue, cela ressemble à ce qui passe avec des nombres entiers. Continuons l'analogie avec les entiers. On peut décomposer un entier en produit de nombres premiers, on dit encore en produit de nombres irréductibles quand on travaille dans $\mathbb{Z}$. Est-ce que l'on peut de même décomposer un polynôme en produit de polynômes irréductibles. Qui sont alors ces polynômes irréductibles, ces briques élémentaires intervenant dans la décomposition ?

4.3.1 Irréductibilité dans $\mathbb{R}[X],\mathbb{C}[X],\mathbb{Q}[X],\mathbb{Z}[X]$

Nous éssayons dans cette section de comprendre qui sont sont les polynômes irréductibles dans les cas de $\mathbb{C}[X],\mathbb{R}[X],\mathbb{Z}[X]$ et $\mathbb{Q}[X]$. Pour comprendre qui sont ces irréductibles, il faut au regard de la définition d'irréductibilité commencer par comprendre qui sont les éléments inversibles.

Proposition 90. ***Description des inversibles de*** $\mathbb{C}[X],\mathbb{R}[X],\mathbb{Q}[X]$**.** *Si k est un corps, les éléments inversibles de $k[X]$ sont les constantes non nulles.*

Démonstration. Si $a\in k$ est une constante non nulle, elle admet un inverse $\frac{1}{a}$ dans k. Le polynôme $\frac{1}{a}=\frac{1}{a}+0X+0X^2+\dots$ est un inverse de a, donc le polynôme constant a est inversible. Montrons qu'il n'y a pas d'autres inversible que ces polynômes constants non nuls. Les autres polynômes possibles sont le polynôme nul, ou un polynôme P de degré strictement positif. Le polynôme nul n'est pas inversible. Un polynôme P de degré >0 n'est pas non plus inversible. En effet, si Q est un polynôme quelconque, le produit PQ ne peut être égal à 1 car le degré de PQ est $deg(P)+deg(Q)$, qui ne peut pas valoir $deg(1)=0$ car $deg(P)$ est positif strictement. ∎

Proposition 91. *Les éléments inversibles de $\mathbb{Z}[X]$ sont les constantes $+1$ et -1.*

Démonstration. Il est évident que 1 et -1 sont inversibles. Réciproquement, la même démonstration que ci-dessus montre qui si P est inversible, son degré vaut 0, ce qui signifie que P est une constante non nulle. Mais l'inverse Q de P est alors également une constante de $\mathbb{Z}$ puisque $deg(Q) = deg(P) + deg(Q) = deg(PQ) = deg(1) = 0$. Donc P est une constante inversible dans $\mathbb{Z}$. Et on sait que les inversibles de $\mathbb{Z}$ sont les nombres 1 et -1. ■

Exercice 59.
a)Quels sont les polynômes inversibles dans la liste suivante sur $\mathbb{Q}[X]$: $1 + 3X + X^2, 5 + X, 4$?
b)Même question sur $\mathbb{Z}[X]$.

Correction 59.
a)Seule la constante 4 est inversible
b)Aucun n'est inversible.

Maintenant que nous avons compris qui sont les inversibles, nous pouvons comprendre qui sont les polynômes irréductibles.

Théorème 92. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.*

Démonstration. Montrons d'abord que tout polynôme P de degré un est irréductible, c'est à dire que si $P = QR$, alors soit Q soit R est inversible. Si $P = QR$, alors $1 = deg(P) = deg(Q) + deg(R)$. Donc ($deg(Q) = 1$ et $deg(R) = 0$) ou ($deg(Q) = 0$ et $deg(R) = 1$). Dans les deux cas, le polynôme de degré 0 est inversible d'après l'étude des inversibles ci-dessus.
Montrons maintenant qu'il n'y a pas d'autres irréductibles que les polynômes P de degré 1. Si P est de degré 0, il est inversible donc non irréductible par définition. Si P est de degré au moins deux, considérons un élément a tel que $P(a) = 0$. On sait qu'un tel élément existe toujours puisque l'on travaille sur les complexes. D'après la section précédente, on peut écrire $P = (X - a)Q$. Le degré de Q est égal à $deg(P) - 1$, donc est strictement positif. On a donc une décomposition de P en produit de deux non inversibles, ce qui montre que P n'est pas irréductible. ■

Pour trouver une décomposition en polynômes irréductibles d'un polynôme non constant, la démonstration précédente dit comment faire. Si le polynôme P est de degré 1, il est irréductible et la décomposition est $P = P$. Sinon, P admet une racine a et on peut écrire $P = (X - a)P_1$. Si P_1 est de degré 1, on a la décomposition cherché. Sinon, on trouve une racine b de P_1 et on écrit $P_1 = (X - b)P_2$, d'òu $P = (X - a)(X - b)P_2$. Si P_2 est irréductible, on a la décomposition cherchée. Sinon, on continue avec une racine c de P_2 et ainsi de suite. Puisque le degré de P_i baisse à chaque étape, l'algorithme s'arrête. On a donc démontré:

Théorème 93. *Tout polynôme non constant de $\mathbb{C}[X]$ admet une décomposition en produit de polynômes irréductibles.*

Lorsque l'on travaille sur $\mathbb{R}$, on ne peut pas procéder de la même façon que sur $\mathbb{C}$. Sur $\mathbb{C}$, tout polynôme admet une racine. En revanche, sur $\mathbb{R}$, un polynôme comme $X^2 + 1$ est sans racine. Le fait que ce polynôme soit sans racine se traduit algébriquement par le fait que le discriminant est positif. En fait dans $\mathbb{R}[X]$, il y a deux types de polynômes irréductibles, ceux de degré 1 et ceux de degré 2 sans racine, comme l'affirme le théorème suivant:

Théorème 94. *Un polynôme P de $\mathbb{R}[X]$ est irréductible ssi l'une des deux conditions suivantes est vérifiée:*

- *P est de degré 1*
- *P est de degré 2 et son discriminant Δ est positif.*

Démonstration. Si P est de degré 1, la même démonstration que sur $\mathbb{C}$ montre qu'il est irréductible. Si P est de degré deux sans racine. Montrons que P est irréductible. Par l'absurde. Supposons que $P = QR$ se décompose en produit de non inversibles. Alors Q et R sont de degré un. Mais tout polynôme $aX + b$ de degré un admet une racine, à savoir $-\frac{b}{a}$, donc Q admet une racine. Par conséquent, P admet également une racine. Contradiction. Le polynôme P est donc irréductible.
Montrons maintenant qu'il n'y a pas d'autres polynômes irréductibles que ceux là. Si P est constant, il est soit nul, soit inversible donc non irréductible. Si P est de degré deux avec une racine a, la décomposition $P = (X - a)Q$ montre que P n'est pas irréductible. Enfin supposons P de degré $d \geq 3$. Si P admet une racine réelle, la même démonstration que dans le cas du degré deux montre que P n'est pas irréductible. Si P est de degré au moins trois sans racine réelle, il admet une racine complexe non réelle a. D'où l'écriture $P = (X - a)Q$ dans $\mathbb{C}[X]$. Mais le conjugué $\bar{a}$ est aussi une racine de P. Donc $0 = P(\bar{a}) = (\bar{a} - a)Q(\bar{a})$. Puisque $\bar{a} - a \neq 0$, il faut $Q(\bar{a}) = 0$, donc

$X - \bar{a}$ divise Q: $Q = (X - \bar{a})R$. On obtient $P = (X - a)(X - \bar{a})R$. Le polynôme $S = (X - a)(X - \bar{a})$ est dans $\mathbb{R}[X]$. Le polynôme R était à priori dans $\mathbb{C}[X]$. Mais comme $R = \frac{P}{S}$, il est en fait dans $\mathbb{R}[X]$. On a donc une décomposition $P = RS$ dans $\mathbb{R}[X]$ qui montre que P n'est pas irréductible sur $\mathbb{R}$. ■

Voici en exercice deux points utilisés dans la démonstration sans justification.

Exercice 60.
a)Est-ce que la conjuguaison complexe $\mathbb{C} \to \mathbb{C}$, $z = a + ib \mapsto \bar{z} = a - ib$ est un morphisme d'anneaux ?
b)Montrer que si $P \in \mathbb{R}[X]$ admet une racine a, alors le conjugué $\bar{a}$ vérifie lui aussi $P(\bar{a}) = 0$.
c)Montrer que $P = (X - a)(X - \bar{a})$ est un polynôme réel.

Correction 60.
a)Oui. Quand on écrit les vérifications à faire pour un morphisme d'anneaux, on s'aperçoit que cela revient à vérifier les formules $\overline{1} = 1$, $\bar{z}_1 + \bar{z}_2 = \overline{z_1 + z_2}$ et $\bar{z}_1\bar{z}_2 = \overline{z_1 z_2}$. Et ces formules se vérifient immédiatement.
b)Soit $P = \sum a_i X^i$. On a $0 = P(a) = \overline{P(a)} = \overline{\sum a_i a^i} = \sum a_i \overline{a}^i$ d'après les formules de la première question et puisque les a_i sont réels. Mais cette derniere expression est simplement $P(\bar{a})$ qui est donc bien nul.
c)Son polynôme conjugué $\overline{P}$ obtenu en changeant tous les coefficients par leur conjugué est $\overline{P} = (X - \bar{a})(X - a) = P$. Donc P est réel puisque $\overline{P} = P$. (Autre méthode possible on calcule simplement: $P = X^2 - 2Re(a) - |a|^2$ où Re désigne la partie réelle et $|\ |$ le module. Il est alors clair sous cette forme que P est un polynôme réel).

Exercice 61.
a)Calculer une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{C}$
b)Même question sur $\mathbb{R}$.

Correction 61.
a)Si on multiplie P par $X - 1$, on trouve $X^5 - 1$. Les racines de ce polynôme sont les racines cinquièmes de l'unité à savoir $r, r^2, r^3, r^4, r^5 = 1$ où $r = e^{\frac{2i\pi}{5}}$. Donc $P.(X - 1) = (X - r)(X - r^2)(X - r^3)(X - r^4)(X - 1)$. Comme on est dans un anneau intègre, on peut simplifier par $X - 1$ et on trouve $P = (X - r)(X - r^2)(X - r^3)(X - r^4)$ qui est la décomposition voulue.
b)Pour obtenir la décomposition dans $\mathbb{R}$, il faut regrouper les termes deux

à deux avec le conjugué. Le conjugué de r est r^4 et celui de r^2 est r^3. On a l'égalité $(X-r)(X-r^4) = X^2 - 2cos(\frac{\pi}{5})X + 1$ et $(X-r^2)(X-r^3) = X^2 - 2cos(2\frac{\pi}{5})X + 1$. La décomposition sur $\mathbb{R}$ est donc $P = (= X^2 - 2cos(\frac{\pi}{5})X + 1)(X^2 - 2cos(2\frac{\pi}{5})X + 1)$.

Pour $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, il est plus difficile de dire qui sont les irréductibles. Nous n'allons pas pouvoir donner un critère simple pour vérifier si un polynôme est irréductible. En revanche, nous allons donner un algorithme pour décomposer un polynôme en produit d'irréductibles. Commençons par le cas de $\mathbb{Z}[X]$. Regardons d'abord le cas des polynômes constants.

Proposition 95. *Soit $p \in \mathbb{Z}$. La constante p vu comme polynôme de $\mathbb{Z}[X]$ est irréductible ssi p est un nombre premier au signe près.*

Démonstration. Si p est un nombre premier ou l'opposé d'un nombre premier, écrivons $p = qr$. Puisque p est un polynôme de degré 0, q et r doivent aussi être des polynômes de degré 0, c'est à dire des constantes de $\mathbb{Z}$. Mais dans $\mathbb{Z}$, p est irréductible donc la seule possibilité est que q ou r soit égal à 1 ou -1. Comme 1 et -1 sont inversibles dans $\mathbb{Z}[X]$, cela signifie que p est irréductible.
Réciproquement, si p n'est pas premier au signe près, on peut écrire $p = qr$ avec q et r différents de 1 et -1. Cette écriture est une décomposition de p qui montre que p n'est pas irréductible. ■

Proposition 96. *Si un polynôme $P = \sum a_i X^i$ de $\mathbb{Z}[X]$ est irréductible, alors le pgcd de ses coefficients est* 1.

Démonstration. Procédons par contraposée. Soit d le pgcd des a_i et supposons que le pgcd soit différent de 1. Alors on peut écrire $P = d.Q$, avec $Q = \frac{a_0}{d} + \frac{a_1}{d}X + \cdots + \frac{a_n}{d}X^n$, ce qui montre que P n'est pas irréductible. ■

Exercice 62. Soit $P \in \mathbb{Z}[X]$ un polynôme de degré au plus un. Discuter l'irréductibilité de ce polynôme.

Correction 62. Si P est nul ou une constante inversible, il n'est pas irréductible par définition de l'irréductibilité. Si P est une constante ni nulle, ni inversible, P est irréductible par le cours ssi p est un nombre premier. Il reste à considérer le cas où $P = aX + b$ est de degré 1. Si a et b ne sont pas premiers entre eux et ont un pgcd non trivial d, la décomposition

$P = d(\frac{a}{d}X + \frac{b}{d})$ montre que P n'est pas irréductible. Si a et b sont premiers entre eux, montrons que P est irréductible. Soit $P = QR$ une décomposition. Puisque P est de degré 1, il faut que Q et R soient de degré 0 et 1, par exemple par symétrie Q de degré 0 et R de degré 1. Donc Q est une constante c. On obtient donc $aX + b = c(dX + e)$, ce qui montre que c divise à la fois a et b. Donc c vaut plus ou moins 1 puisque $pgcd(a, b) = 1$. Donc Q est inversible dans $\mathbb{Z}[X]$. Toute décomposition de P en facteurs contient un facteur inversible, ce qui prouve que Q est irréductible.

L'exercice suggère que la méthode pour décomposer un polynôme $P \in \mathbb{Z}[X]$ en irréductibles commence de la façon suivante. On commence par casser en morceaux en factorisant le pgcd des coefficients du polynôme. Par exemple, pour $6X^2+6X+12$, le pgcd en question est six et on commence par casser le polynôme sous la forme $2.3.(X^2+X+2)$. Le polynôme non constant dans le produit est tel que le pgcd de ses coefficients vaut 1. Formellement, on introduit la notion de contenu d'un polynôme.

Définition 97. *Soit $P \in \mathbb{Z}[X]$. On appelle contenu de P et on note $ct(P)$ le pgcd des coefficients de P.*

Exercice 63.
a)Soit $P \in \mathbb{Z}[X]$. Vérifier que P est divisible (dans $\mathbb{Z}[X]$) par le contenu $ct(P)$.
b)Montrer que si l'on écrit $P = ct(P)Q$, alors $ct(Q) = 1$.

Correction 63.
a)Écrivons $P = \sum a_i X^i$ et $ct(P) = pgcd(a_i)$. On a l'égalité $P = ct(P).\sum \frac{a_i}{ct(P)} X^i$, ce qui montre que P est divisible par $ct(P)$ puisque les $\frac{a_i}{ct(P)}$ sont des entiers.
b)Pour voir que Q est de contenu égal à 1, raisonnons par l'absurde. Supposons $ct(Q) \neq 1$. Alors en écrivant $Q = ct(Q)\sum b_i X^i$, et en reportant dans l'expression de P, on obtient $P = ct(P)ct(Q)\sum b_i X^i = \sum (ct(P)ct(Q)b_i)X^i$, ce qui montre que tous les coefficients de P sont divisibles par $ct(P)ct(Q)$. Cela contredit le fait que le plus grand diviseur commun aux coefficients est $ct(P)$.

Une fois que l'on a écrit P sous la forme $a_1 \dots a_n Q$ où $ct(Q) = 1$, il faut ensuite décomposer Q. On essaie donc de trouver une décomposition $Q = RS$ où R et S sont non inversibles. L'exercice suivant montre alors que R et S ne sont pas des constantes.

Exercice 64. Montrer que si $Q \in \mathbb{Z}[X]$ est tel que $ct(Q) = 1$, et si $Q = RS$ est une décomposition en produit de non inversibles, alors ni R ni S ne sont des constantes.

Correction 64. Par contraposée on va montrer que si $R = r$ est une constante, alors R est inversible. En effet, si $S = \sum s_i X^i$, $Q = \sum (r s_i) X^i$. Le nombre r divise tous les coefficients de s, donc leur pgcd, qui est 1. Donc r vaut plus ou moins 1 et $R = r$ est inversible.

Par symétrie entre R et S dans l'écriture $Q = RS$, on peut supposer que $deg(R) \leq deg(S)$, donc que $0 < deg(R) \leq deg(Q)/2$. La méthode pour trouver un R possible qui divise Q est la suivante. On va établir une liste finie $R_1, \ldots, R_s$ de polynômes et on va montrer que si R divise S, il est forcément dans la liste $\{R_1, \ldots, R_s\}$. On va ensuite essayer de diviser Q par chacun des R_i de notre liste. Si aucun des R_i ne divise Q, cela voudra dire que Q est irréductible et on aura fini. Sinon, on trouve un R_i qui divise Q, on pose $R = R_i$ et l'expression $Q = RS$ définit S. Mais alors décomposer Q revient à décomposer R et S. On recommence alors la même manipulation avec R et S à la place de Q: soient ils sont irréductibles, soit on les casse en deux. Comme le degré de R et de S est strictement plus petit que celui de Q, l'algorithme s'arrête au bout d'un nombre fini d'étapes. Par exemple, quand les polynômes sont de degré au plus un, on a vu comment conclure en exercice.
Reste à savoir comment trouver cette liste de R_i. A quoi peut ressembler un polynôme R de degré d divisant Q ? Choisissons des entiers $x_0, \ldots, x_d$ au hasard. Par exemple $x_0 = 0, \ldots, x_d = d$ (mais un autre choix conviendrait aussi). Si $Q = RS$ alors $Q(0) = R(0)S(0)$, donc $R(0)$ divise $Q(0)$. L'entier $Q(0)$ a un nombre fini de diviseurs donc il y a un nombre fini de choix possibles pour $R(0) = R(x_0)$. De même, il y a un nombre fini de choix possibles pour $R(x_1), \ldots, R(x_d)$. Admettons que je choisisse une valeur possible pour $R(x_0), \ldots, R(x_d)$. Alors le polynôme R est entièrement déterminé. En effet, on sait que si $x_0, \ldots, x_d$ sont des points de $\mathbb{R}$ et si $v_0, \ldots, v_d$ sont des valeurs associées aux x_i, il existe un unique polynôme d'interpolation $P \in \mathbb{R}[X]$ de degré d tel que $P(x_i) = v_i$. Donc puisqu'on a un nombre fini de choix possibles pour $R(0), \ldots, R(d)$, on a un nombre fini de choix possibles pour R.
Essayons de mettre la méthode en application.

Exercice 65. Considérons le polynôme de degré 4 $P = 5x^4 + 10x^3 - 5x^2 - 10x + 5 \in \mathbb{Z}[X]$.
a)Écrire P sous la forme $a_1 \ldots a_n Q$ où les a_i sont des entiers irréductibles et où Q est de contenu 1.
b)Soit R un polynôme de $\mathbb{Z}[X]$ divisant Q. Donner la liste des valeurs possibles pour $R(0)$.
c)Donner de même la liste des valeurs possibles pour $R(1)$ et $R(-1)$.

d)Faire la liste des polynômes de degré 1 susceptibles de diviser Q.
e)Faire la liste des polynômes de degré 2 susceptibles de diviser Q.
f)Trouver la décomposition de Q en produit d'irréductibles.
g)Trouver la décomposition de P en produit d'irréductibles.

Correction 65.
a)$P = 5(X^4 + 2X^3 - X^2 - 2X + 1)$.
b)Puisque $Q(0)$ vaut 1, $R(0)$ qui divise $Q(0)$ vaut 1 ou -1.
c)Pour la même raison, puisque $Q(1) = 1$ et $Q(-1) = 1$, on a $R(1)$ et $R(-1)$ qui valent 1 ou -1.
d)Les polynômes $aX + b$ de degré au plus 1 pouvant diviser Q doivent avoir pour valeur en 0 et 1 les valeurs 1 ou -1 ce qui donne les quatre possibilités 1, $-2X+1$,-1, $2X-1$. Mais aucun des polynômes de degré un de cette liste n'a une valeur possible en -1. Donc Q n'est pas divisible par un polynôme de degré 1.
e)Le polynôme $Q_0 = a+bX+cX^2$ qui vaut $-1, 1, 1$ en $-1, 0, 1$ est $1+X-X^2$. Donc $1 + X - X^2$ est un diviseur possible. En faisant varier les valeurs possibles de $Q(0), Q(1), Q(-1)$, on trouve les polynômes $Q_1 = X^2 + X - 1$, $Q_2 = -2X^2 + 1$,$Q_3 = 1$, ainsi que leurs opposés $-Q_0, -Q_1, -Q_2, -Q_3$.
f)Seul Q_2 (et $-Q_2$) divise Q. Et on trouve donc la factorisation $Q = Q_2.Q_2$.
g)$P = 5.(Q_2)^2$.

Nous savons donc maintenant décomposer un polynôme de $\mathbb{Z}[X]$ en produit d'irréductibles. Passons au dernier cas, celui de la décomposition des polynômes sur $\mathbb{Q}$. Quitte à multiplier un polynôme $P \in \mathbb{Q}[X]$ par une constante, on peut supposer $P \in \mathbb{Z}[X]$ et de contenu 1. Par exemple, pour $P = \frac{2}{3}X + \frac{2}{5}X^2$, en multipliant par $\frac{15}{2}$, obtient $5X + 3$ qui est bien dans $\mathbb{Z}[X]$ avec le pgcd des coefficients égal à 1. L'exercice suivant montre que cette petite manipulation est toujours possible.

Exercice 66. Soit $P = \sum \frac{a_i}{b_i} X^i \in \mathbb{Q}[X]$ un polynôme non inversible.
a)Montrer qu'il existe une constante $q \in \mathbb{Q}$ tel que $R = qP$ soit dans $\mathbb{Z}[X]$ de contenu 1.
b)Soit $R = R_1 \dots R_s$ une décomposition de R en irréductibles dans $\mathbb{Q}[X]$. Donner une décomposition de P.

Correction 66.
a)Commençons par choisir une constante q_1 (par exemple q_1 le produit des dénominateurs b_i tels que $Q_1 = q_1 P = \sum a_i \frac{q_1}{b_i} X^i$ soit dans $\mathbb{Z}[X]$. Soit c le contenu de Q_1. D'après l'exercice relatif à la factorisation du contenu d'un polynôme, on a $Q_1 = cR$, où $R = \sum \frac{a_i q_1}{c b_i} X^i$ est un polynôme de contenu

égal à 1. On a donc le résultat voulu avec $q = \frac{q_1}{c}$.
b)La décomposition de P se déduit de celle de R. Puisque la multiplication par un inversible ne change pas l'irréductibilité, qR_1 est irréductible dans $\mathbb{Q}[X]$ et on peut donc prendre la décomposition $P = (qR_1)R_2 \dots R_s$.

Comme les constantes sont inversibles dans $\mathbb{Q}[X]$, il est équivalent de savoir décomposer un polynôme P et de savoir décomposer le polynôme $R = qP$ comme le montre la deuxième question de l'exercice précédent. Donc on se pose la question de savoir décomposer dans $\mathbb{Q}[X]$ un polynôme P de $\mathbb{Z}[X]$ de contenu égal à un. Ce polynôme a à priori deux décompositions, l'une comme polynôme de $\mathbb{Z}[X]$ (que l'on sait calculer d'après ce qui précède) et l'autre dans $\mathbb{Q}[X]$. Remarquons tout de suite qu'il n'est pas évident que la décomposition reste la même lorsque l'on change les coefficients de l'anneau de polynômes. Par exemple $(X^2 + 1)$ est irréductible sur $\mathbb{R}[X]$ mais est réductible sur $\mathbb{C}[X]$ puisqu'il s'écrit $(X + i)(X - i)$. En revanche, pour un polynômes de $\mathbb{Z}[X]$ de contenu égal à un, sa décomposition est la même sur $\mathbb{Z}[X]$ et sur $\mathbb{Q}[X]$.

Théorème 98. *Soit $P \in \mathbb{Z}[X]$ un polynôme non constant de contenu égal à 1, et $P = P_1 \dots P_r$ une décomposition en irréductibles sur $\mathbb{Z}$. Alors les P_i sont irréductibles sur $\mathbb{Q}$ et l'expression $P = P_1 \dots P_r$ est donc également une décomposition en irréductibles sur $\mathbb{Q}$.*

Muni de ce théorème, on peut donc écrire la décomposition en irréductibles sur $\mathbb{Q}$ de tout polynôme. Mettons ce théorème en pratique avant d'en faire la démonstration.

Exercice 67. Décomposer en irréductibles le polynôme $Q = 5x^4 + 10x^3 - 5x^2 - 10x + 5 \in \mathbb{Q}[X]$. (On pourra se ramener à une décomposition sur $\mathbb{Z}$ faite dans un exercice précedent).

Correction 67. On a trouvé la décomposition sur $\mathbb{Z}[X]$: $Q = 5.(-2X^2 + 1)^2$. Le polynôme $(-2X^2 + 1)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$ d'après ce qu'on a vu dans le cours. La multiplication par 5 qui est un inversible de $\mathbb{Q}[X]$ ne change pas l'irréductibilité. Donc on a la décomposition: $Q = (-10X^2 + 5)(-2X^2 + 1)$ qui est la décomposition sur $\mathbb{Q}[X]$.

Pour démontrer le théorème, utilisons le lemme suivant, laissé en exercice.

Exercice 68. Soit $P, Q \in \mathbb{Z}[X]$ et $\lambda \in \mathbb{Z}$. Montrer que l'application contenu ct vérifie
a)$ct(\lambda P) = \lambda ct(P)$.

b)Montrer que si $P = \sum a_i X^i$ et $Q = \sum b_i X^i$ sont de contenu 1, alors $ct(PQ) = 1$.
c)$ct(P)ct(Q) = ct(PQ)$

Correction 68.
a)Si $a_1, \ldots, a_n$ sont les coefficients de P, ceux de λP sont $\lambda a_1, \ldots, \lambda a_n$. L'égalité proposée dit donc simplement que $pgcd(\lambda a_1, \ldots, \lambda a_n) = \lambda pgcd(a_1, \ldots, a_n)$. Mais cette dernière égalité est claire si on pense au pgcd comme les facteurs communs apparaissant dans les décompositions en facteurs premiers.
b)Supposons par l'absurde qu'un nombre premier d divise le contenu $ct(PQ)$. Puisque $ct(P) = 1$, il existe un nombre n tel que d ne divise pas a_n. On choisit un tel n minimum. De même, choisissons m minimum tel que d ne divise pas b_m. Le coefficient c_{m+n} devant le terme X^{m+n} du produit PQ est $\sum_{i=0\ldots m+n} a_i b_{m+n-i}$. Si i est plus petit que n, alors d divise a_i. Et si $i > n$, $m + n - i < m$ donc d divise b_{m+n-i}. Au final, tous les termes de la somme sont divisibles par d, sauf $a_n b_m$ qui n'est pas divisible par d puisque ni a_n ni b_m ne le sont. Donc c_{m+n} n'est pas divisible par d, ce qui contredit le fait que d divise le contenu $ct(PQ)$.
c)Écrivons $P = ct(P)P'$ et $Q = ct(Q)Q'$ où P' et Q' sont de contenu 1. Alors $PQ = ct(P)ct(Q)P'Q'$. Le contenu du polynôme à gauche du signe $=$ est $ct(PQ)$ tandis que le contenu du terme de droite est $ct(P)ct(Q)ct(P'Q') = ct(P)ct(Q)$ d'après les deux questions précédentes. On a donc l'égalité voulue.

Montrons le théorème à l'aide de ce lemme. On a donc $P \in \mathbb{Z}[X]$ de contenu 1 et $P = P_1 \ldots P_r$ une décomposition de P dans $\mathbb{Z}[X]$. On veut montrer que les P_i sont irréductibles dans $\mathbb{Q}[X]$. Par l'exercice précédent, $1 = ct(P) = ct(P_1) \ldots ct(P_r)$ donc le contenu de chaque P_i vaut 1. On est donc ramené à démontrer qu'un polynôme irréductible P de $\mathbb{Z}[X]$ de contenu 1 est irréductible sur $\mathbb{Q}[X]$. Décomposons un tel P sous la forme QR dans $\mathbb{Q}[X]$. On veut montrer que Q ou R est inversible, c'est à dire une constante. Mulitplions Q par un entier q (resp. R par r) de façon à obtenir un polynôme à coefficients entiers. On a l'égalité

$$qrP = (qQ)(rR).$$

En passant aux contenus, on a donc $qr.ct(P) = qr = ct(qQ)ct(rR)$. On peut donc diviser à gauche et à droite l'égalité précédente par $qr = ct(qQ)ct(rR)$ et on obtient:

$$P = \frac{qQ}{ct(qQ)} \frac{rR}{ct(rR)}$$

Cette égalité est une décomposition de P dans $\mathbb{Z}[X]$. Puisque P est irréductible dans $\mathbb{Z}[X]$, cela signifie que l'un des facteurs, par exemple le premier, vaut $+1$ ou -1. Mais si $\frac{qQ}{ct(qQ)}$ est une constante, Q est également une constante. ■

Si on se donne un polynôme $P \in \mathbb{Z}[X]$ de contenu 1, pour vérifier s'il est irréductible, vous devez à priori essayer de le décomposer en irréductibles. Si la décomposition trouvée est $P = P$, alors cela signifie que P est irréductible. Il existe un critère, appelé critére d'Eisenstein, qui permet parfois de vérifier plus rapidement l'irréductibilité sur $\mathbb{Z}$.

Exercice 69.
a)Critère d'Eisenstein. Soit $P = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ un polynôme de degré n et p un nombre premier. Supposons que p divise $a_0, \ldots, a_{n-1}$ mais pas a_n et que p^2 ne divise pas a_0. Montrer que P est irréductible.
b)Montrer qu'il existe dans $\mathbb{Z}[X]$ des polynômes irréductibles de tout degré strictement positif.

Correction 69.
a)Par l'absurde. Supposons P non irréductible et écrivons une décomposition $P = QR$ où $Q = \sum d_i X^i$, $R = \sum b_i X^i$ en produit de non inversibles. Tous les d_i ne sont pas divisibles par p sinon P (et donc a_n) serait divisible par P. Donc il existe un plus petit entier q tel que d_q ne soit pas divisible par p. De même, il existe un plus petit entier m tel que b_m ne soit pas divisible par p. Le coefficient c_{m+q} de X^{m+q} de P n'est donc pas divisible par p (c'est le même raisonnement que l'exercice où l'on montre que si P et Q sont de contenu 1, $ct(PQ) = 1$). Cela signifie donc que $m + q = deg(P) = deg(Q) + deg(R)$. Comme $m \leq \deg(R)$ et $q \leq deg(Q)$, la seule possibilité est $m = deg(R)$ et $q = deg(Q)$. Puisque Q et R sont de degré au moins 1 car non inversibles, $m > 0$ et $q > 0$. Par minimalité de m et q, on a donc d_0 et b_0 divisibles par p. Mais alors $a_0 = d_0 b_0$ est divisible par p^2. Contradiction.
b)D'après le point précédent, le polynôme $X^n + 2$ est irréductible pour tout n.

ExoTD 7. *Soit $P = \sum a_i X^i \in \mathbb{Z}[X]$, p un nombre premier et $\dot{P} = \sum \dot{a}_i X^i$ l'image $\overline{P}$ de P dans $\mathbb{Z}/p\mathbb{Z}[X]$.*
***c)**Comparer le degré de P et celui de $\overline{P}$. A quelle condition a-t-on égalité.*
***d)**Si $\dot{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et a même degré que P, montrer que $P \in \mathbb{Z}[X]$ est irréductible*
***e)**Décomposer $\bar{P} = X^3 + X^2 + X + \dot{1}$ sur $\mathbb{Z}/3\mathbb{Z}$.*
***f)**Montrer que $P = X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Z}$.*

correcTD 7.
g)$\deg(\overline{P}) \leq \deg(P)$ *avec égalité ssi p ne divise pas le coefficient dominant* a_n *de* P
h)*Par contraposée. Montrons que si* $P = QR$ *est réductible, alors* $\overline{P}$ *est réductible. On a* $\bar{P} = \bar{Q}\bar{R}$*. Pour montrer que* $\bar{P}$ *est réductible, il suffit au vu de cette décomposition de montrer que* $\bar{Q}$ *et* $\bar{R}$ *sont non inversibles, c'est à dire non constants. L'analyse des degrés des polynômes donne:*

$$\deg(P) = \deg(\bar{P}) = \deg(\bar{Q}) + \deg(\bar{R}) \leq \deg(Q) + \deg(R) = \deg(QR) = \deg(P)$$

Il faut donc que l'inégalité soit une égalité, ce qui se produit si $deg(\bar{Q}) = deg(Q)$ *et* $deg(\bar{R}) = deg(R)$*. Comme* Q *et* R *sont des polynômes non constants par hypothèse,* $\bar{Q}$ *et* $\bar{R}$ *sont également non constants.*
i)*Si* P *était réductible, il s'écrirait sous la forme* $P = QR$ *où* Q *et* $R = aX + b$ *sont de degré* 2 *et* 1*. En particulier,* P *aurait une racine* $\frac{-b}{a}$*. Donc pour montrer que* P *est irréductible il suffit de voir qu'il n'a pas de racine. Or* $P(\dot{0}) = \dot{1}$*,* $P(\dot{1}) = \dot{1}$ *et* $P(\dot{2}) = \dot{2}$*. Par suite* P *est sans racine donc irréductible.*
j)*L'image* $\bar{P}$ *de* P *est irréductible dans* $\mathbb{Z}/3\mathbb{Z}[X]$ *d'après la question précédente et a même degré que* P*. Donc* P *est irréductible d'après le deuxième point.*

4.3.2 Anneaux euclidiens, factoriels, principaux

Faisons le point. Nous avons vu dans chacun des anneaux $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$ comment écrire une décomposition en éléments irréductibles. Dans $\mathbb{Z}$, nous avons également décomposé les nombres en produits de nombres irréductibles. Pour $\mathbb{Z}$, cette décomposition était essentiellement unique, c'est à dire plus précisément unique à multiplication par des inversibles et permutation près. L'analogie entre $\mathbb{Z}$ et les anneaux de polynômes se poursuit. On dispose d'un théorème d'essentielle unicité pour la décomposition dans les anneaux de polynômes.

Théorème 99. *Soit* A *un anneau qui est soit un corps, soit* $\mathbb{Z}$*. Tout élément non nul et non inversible* $P \in A[X]$ *se décompose en produit d'éléments irréductibles et la décomposition est unique à l'odre des facteurs et multiplication par des inversibles près. Plus précisément, cela signifie que si* $P = p_1 \dots p_r = q_1 \dots q_s$ *sont deux décompositions, alors* $r = s$ *et, quitte à intervertir les* q_i*, on a* $p_i = \epsilon_i q_i$ *où* ϵ_i *est inversible.*

Définition 100. *factoriel Un anneau intègre vérifiant une décomposition comme ci-dessus, unique à l'ordre des facteurs et multiplication par des inversibles près est appelé un anneau factoriel.*

Le théorème précédent et son analogue sur $\mathbb{Z}$ se reformulent donc en:

Théorème 101. *Les anneaux $\mathbb{Z}$, $\mathbb{Z}[X]$, et $k[X]$ quand k est un corps sont factoriels.*

Le cas de $\mathbb{Z}[X]$ est à part. Le cas de $k[X]$ se démontre comme pour celui des entiers. Commençons donc par celui-ci. Si l'on relit la démonstration de l'unicité de la décomposition dans $\mathbb{Z}$, on voit que la clé de l'unicité est le corollaire 111, qui vient lui-même de la relation de Bezout, qui vient elle-même de la principalité de $\mathbb{Z}$, qui vient (enfin !) de l'existence d'une division. Si k est un corps, on a une division dans $k[X]$ et on peut donc refaire exactement le même jeu que dans $\mathbb{Z}$. Voici donc la démonstration telle qu'on aurait pu la présenter de façon générale.

Définition 102. *division euclidien Un anneau euclidien A est un anneau intègre muni d'une application $\delta : A \setminus 0 \to \mathbb{N}$ vérifiant la propriété suivante. Pour tout couple (a, b) d'éléments de A avec $b \neq 0$, il existe une division $a = bq + r$ avec $\delta(r) < \delta(b)$ ou $r = 0$.*

Exercice 70. Montrer que $\mathbb{Z}$ et $k[X]$ sont des anneaux euclidiens en donnant l'application δ correspondante.

Correction 70. Pour $\mathbb{Z}$, l'application δ est l'application valeur absolue. Pour $k[X]$, l'application δ est le degré des polynômes.

Proposition 103. *Les anneaux euclidiens sont principaux.*

Démonstration. Il suffit de relire la démonstration sur $\mathbb{Z}$ et de voir que la seule chose que l'on a utilisé pour démontrer que les idéaux de $\mathbb{Z}$ sont principaux est le fait que $\mathbb{Z}$ est euclidien. ■

Corollaire 104. *Tout idéal I de $k[X]$ est principal, ie. il existe un polynôme P tel que I est l'ensemble des multiples de P.*

Exercice 71. Démontrer le corollaire qui dit que tout idéal de $k[X]$ est principal en reprenant mot par mot la démonstration faite sur $\mathbb{Z}$ 36 et en faisant les adaptations là où elles sont nécéssaires.

Correction 71. Si $I = \{0\}$, on a évidemment I principal engendré par 0. Sinon, I contient un élément i non nul. Soit a un élément de I non nul de degré minimum. On va montrer que I est principal en montrant $I = (a)$. Il est d'abord clair que $I \supset (a)$ puisque I contient a et que (a) est le plus

petit idéal contenant a. Montrons réciproquement $I \subset (a)$. Soit donc $i \in I$. Il nous faut $i \in (a)$. On fait la division $i = aq + r$. L'élement $r = i - aq \in I$. Or $\deg(r) < \deg(a)$ et a est de degré minimal parmi les éléments non nuls de I, donc c'est que $r = 0$. D'où $i = aq$ c.a.d. l'appartenance recherchée $i \in (a)$.

De même que la démonstration de la principalité faite sur $\mathbb{Z}$ s'est adapté presque mot pour mot à $k[X]$, les énoncés suivants sont de simples adaptations de ce qui a été fait sur $\mathbb{Z}$. On donne les énoncés pour des polynômes, mais les énoncés se généralisent également en des énoncés sur les anneaux euclidiens. Puisque les démonstrations sont rigoureusement identiques à celles sur $\mathbb{Z}$, on les omet.

Définition 105. *Soit $P_1, \ldots, P_n$ une famille de polynômes de $A[X]$. Un polynôme $P \in A[X]$ est un pgcd des P_i si*

- *P divise chaque P_i*
- *P est maximal pour cette propriété au sens de la divisibilité, ie. si Q divise chaque P_i, alors Q divise P.*

Définition 106. *Soit $P_1, \ldots, P_n$ une famille de polynômes de $A[X]$. Un polynôme $P \in A[X]$ est un ppcm des P_i si*

- *P est un multiple de chaque P_i*
- *P est minimal pour cette propriété au sens de la divisibilité, ie. si Q est un multiple de chaque P_i, alors P divise Q.*

L'identification entre générateur d'un idéal et pgcd vraie sur $\mathbb{Z}$ est également vraie sur $k[X]$.

Proposition 107. *Soit P un générateur de l'idéal $(P_1, \ldots, P_n)$ ie. un polynôme tel que $(P) = (P_1, \ldots, P_n)$. Alors P est un pgcd des P_i.*

Exercice 72.
a)Si P est un pgcd des P_i dans $k[X]$, quels sont les autres pgcd des P_i.
b)Calculer $pgcd(5X^2 + 3, X^3 + X)$

Correction 72.
a)Un pgcd est défini à inversible près. Les inversibles de $k[X]$ sont les constantes non nulles. Les pgcd possibles sont donc les polynômes cP où $c \in k$ est une constante non nulle.
b)On procède comme avec les entiers. On fait une suite de divisions donnée par l'algorithme d'Euclide et le pgcd est le dernier reste non nul. Ici

- $X^3 + X = \frac{1}{5}X(5X^2 + 3) + \frac{2}{5}X$

- $5X^2 + 3 = \frac{25}{2}X(\frac{2}{5}X) + 3$
- $\frac{2}{5}X = 3.\frac{2}{15}X + 0$

Le pgcd est donc 3 ou encore 1 à inversible près. Les deux polynômes sont donc premiers entre eux.

La notion de ppcm est également lié à la notion d'idéal.

Proposition 108. *Soient $P_1, \ldots, P_n$ des éléments de $k[X]$ et P tel que $(P) = (P_1) \cap (P_2) \cdots \cap (P_n)$. Soit $Q \in k[X]$ alors Q est un multiple de chaque P_i ssi Q est un multiple de P. En particulier P est un ppcm des P_i.*

On remarquera que le ppcm n'est lui aussi défini qu'à multiplication par une constante non nulle près, tout comme le pgcd.

Définition 109. *Des éléments $P_1, \ldots, P_n$ de $k[X]$sont dits premiers entre eux si 1 est un pgcd des P_i.*

Comme dans $\mathbb{Z}$, la principalité des idéaux permet de caractériser les ensembles de nombres premiers entre eux par une égalité numérique.

Théorème 110. ***Théorème de Bezout.*** *Des éléments $P_1, \ldots, P_n$ de $k[X]$ sont premiers entre eux ssi il existe des polynômes Q_i tels que $\sum Q_i P_i = 1$*

Cette caractérisation de Bezout implique comme dans $\mathbb{Z}$ les corollaires suivants.

Corollaire 111. *Si P est premier avec Q et avec R, alors P est premier avec QR.*

Corollaire 112. ***Théorème de Gauss*** *Si P est premier avec Q et divise QR, alors P divise R.*

On a donc pu dérouler dans $k[X]$ exactement la même théorie que dans $\mathbb{Z}$, jusqu'au théorème de Gauss. On peut alors conclure la démonstration de l'unicité de la décomposition en reprenant également la démonstration faite sur $\mathbb{Z}$. Tout part au début de l'existence d'une division euclidienne, qui est commune à $\mathbb{Z}$ et $k[X]$. Le schéma pour démontrer que $k[X]$ est factoriel a donc été implicitement que tout anneau euclidien est principal, puis que tout anneau principal est factoriel.
Le cas de $\mathbb{Z}[X]$ est à part, puisque $\mathbb{Z}$ n'est pas un corps. L'exercice suivant montre que $\mathbb{Z}[X]$ n'est pas principal, ce qui exclut de traiter le cas $\mathbb{Z}[X]$ comme les autres cas.

Exercice 73. Montrer que $\mathbb{Z}[X]$ n'est pas euclidien en montrant que $(2, X)$ n'est pas principal.

Correction 73. Supposons par l'absurde qu'il existe un polynôme P tel que $(2, X) = (P)$. Cela implique que $2 \in (P)$, donc que P divise 2. Les diviseurs de 2 dans $\mathbb{Z}[X]$ sont $1, 2, -1, -2$. Si $P = 2$ ou -2, les multiples de P sont des polynômes dont tous les coefficients sont divisibles par 2. En particulier $X \in (P)$ aurait des coefficients divisibles par 2. Contradiction. La seule possibilité restante est donc $P = 1$ ou $P = -1$. Dans ce cas $(P) = \mathbb{Z}[X]$. On aura notre contradiction si on montre $(2, X) \neq \mathbb{Z}[X]$. Montrons pour cela $1 \notin (2, X)$. Un polynôme de $(2, X)$ s'écrit par définition $2A + XB$ où A et B sont dans $\mathbb{Z}[X]$. Il est alors clair que le terme constant d'un tel polynôme est divisible par 2, ce qui n'est pas le cas de 1. Donc $1 \notin (2, X)$ comme annoncé.

En revanche, on a quand même unicité de la décomposition, mais il faut un argument différent.

Exercice 74. Montrer en vous ramenant à un travail sur $\mathbb{Q}$ que la décomposition en facteurs irréductibles dans $\mathbb{Z}[X]$ est essentiellement unique.

Correction 74. Soit $P \in \mathbb{Z}[X]$ un polynôme et $P = a_1 \dots a_r P_1 \dots P_s = b_1 \dots b_t Q_1 \dots Q_u$ deux décompositions de P dans $\mathbb{Z}[X]$ où a_i et b_i sont dans $\mathbb{Z}$ tandis que les autres termes sont des polynômes non constants de contenu égal à 1. On veut démontrer l'unicité à permutation et au signe près, c'est à dire que $r = t, s = u$, $a_i = \epsilon_i b_i$, $P_i = \epsilon_i Q_i$ où ϵ_i est un signe ($+1$ ou -1). Le contenu de P est $a_1 \dots a_r = b_1 \dots b_t$. Le polynôme $\frac{P}{ct(P)} \in \mathbb{Z}[X]$ admet les deux décompositions $P_1 \dots P_s$ et $Q_1 \dots Q_u$. Ce sont aussi des décompositions sur $\mathbb{Q}[X]$ donc par unicité de la décomposition sur les rationnels, on a $s = u$ et quitte à réordonner les facteurs $P_i = \epsilon_i Q_i$. Enfin $a_1 \dots a_r$ et $b_1 \dots b_s$ sont deux décompositions dans $\mathbb{Z}$ de l'entier $ct(P)$ (défini au signe prés). Par unicité de la décomposition sur $\mathbb{Z}$, on obtient $r = s$ et $a_i = \epsilon_i b_i$ à permutation des a_i près.

Chapitre 5

$\mathbb{Z}[i]$ et le théorème des deux carrés

Objectif: Dans ce chapitre, on caractérise les entiers qui s'écrivent comme somme de deux carrés. Le point clé consiste à montrer qu'un certain anneau, en l'occurence $\mathbb{Z}[i]$, a des propriétés particulières.

5.1 $\mathbb{Z}[i]$ est un anneau euclidien

Définition 113. *Gauss On appelle entier de Gauss un complexe de la forme $a+bi$ où a et b sont des nombres entiers.*

Exercice 75. Vérifier que les entiers de Gauss forment un sous-anneau de l'anneau des nombres complexes.

Correction 75. Il est clair que 1 est un entier de Gauss, que le produit de deux entiers de Gauss est un entier de Gauss, et que la différence entre deux entiers de Gauss est un entier de Gauss. Donc les entiers de Gauss forment bien un sous-anneau de $\mathbb{C}$.

Une des propriétés importantes qui nous a permis de bien comprendre les anneaux $\mathbb{Z}$ et $k[x]$ a été l'existence d'une division. De même, $\mathbb{Z}[i]$ est muni d'une division euclidienne. Rappelons en la définition:

Définition 114. *Soit A un anneau et $N : A \setminus \{0\} \to \mathbb{N}$ une application. On appelle division euclidienne relativement à N la donnée d'une application $D : A \times (A \setminus \{0\}) \to A \times A$, qui à deux éléments a et $b \in A$, avec $b \neq 0$ associe un couple (q, r) tels que les deux conditions suivantes soient vérifiées:*

- $a = bq + r$

- $r = 0$ *ou* $N(r) < N(b)$.

On veut montrer que $\mathbb{Z}[i]$ est euclidien. Comment trouver le quotient q et le reste r d'une division $a = bq + r$? de deux entiers de Gauss a et b ? L'idée est la suivante. Pour trouver le quotient q, on fait la division $\frac{a}{b}$ comme nombres complexes. Le quotient $\frac{a}{b} = m + ni$ obtenu est un nombre complexe qui n'est pas en général un entier de Gauss, ie. m et n ne sont pas entiers. L'idée est de prendre pour q une approximation de $\frac{a}{b}$.

Proposition 115. *Soit $N : \mathbb{Z}[i] \to \mathbb{N}$, $a + bi \mapsto a^2 + b^2$ la restriction de la norme complexe à $\mathbb{Z}[i]$. Soient a, b deux entiers de Gauss et $q' = m' + n'i = \frac{a}{b}$ le complexe quotient. Soit $m, n \in \mathbb{Z}$ deux entiers tels que les valeurs absolues de $m' - m$ et $n' - n$ soient inférieures ou égales à $\frac{1}{2}$. Soit $q = m + ni$ et $r = a - qb$. Alors l'expression $a = bq + r$ est une division de a par b relativement à N. En particulier $\mathbb{Z}[i]$ est euclidien.*

Démonstration. On doit vérifier que $r = 0$ ou $N(r) < N(b)$. Si $r = 0$ il n'y a rien à dire. Sinon, on veut montrer $N(r) < N(b)$. Or $N(r) = N(a - bq) = N(b)N(\frac{a}{b} - q) = N(b)N((m' - m) + (n' - n)i) \leq N(b)(\frac{1}{4} + \frac{1}{4}) < N(b)$. ∎

Exercice 76. Faire la division de $2 + 15i$ par $1 + i$.

Correction 76.
a) $\frac{2+15i}{1+i} = \frac{(2+15i)(1-i)}{(1+i)(1-i)} = \frac{17+13i}{2}$. On peut donc prendre comme quotient $8+6i$. Le reste est alors $(2+15i)-(8+6i)(1+i) = i$. Une division possible est donc $2 + 15i = (8 + 6i)(1 + i) + i$. Le reste i est de norme 1 qui est bien inférieure à la norme 2 de $1 + i$.

Rappelons que l'on a démontré au chapitre précédent que euclidien implique principal implique factoriel. On a donc en particulier:

Théorème 116. *L'anneau $\mathbb{Z}[i]$ est factoriel.*

Au delà de la factorialité, la philosophie générale est que les anneaux euclidiens se comportent comme $\mathbb{Z}$ et $k[X]$.

Exercice 77. En relisant les démonstrations des énoncés correspondant pour les entiers, faites les modifications nécéssaires pour établir les énoncés suivants dans $\mathbb{Z}[i]$.
a)Montrer que si a divise bc et si a est premier avec b, alors a divise c.
b)Soit p un entier de Gauss irréductible et $q \in \mathbb{Z}[i]$ non divisible par p. Alors p et q sont premiers entre eux.
c)Montrer que si a divise bc et si a est irréductible, alors a divise b ou c.

Correction 77.
a)Si on relit le théorème de Bezout, on voit qu'il est vrai sur tout anneau principal, en particulier dans $\mathbb{Z}[i]$. On a donc une expression $1 = \lambda a + \mu b$ car a et b sont premiers entre-eux par hypothèse. D'où on tire $c = \lambda ac + \mu bc$. Puisque a divise ac et bc, il divise c.
b)C'est la même démonstration presque mot pour mot que pour les entiers: Soit $d = pgcd(p, q)$. On veut dire que d est inversible. Par définition du pgcd, on a l'égalité des idéaux $(d) = (p, q)$. L'élément p qui est dans le deuxième idéal est dans le premier et donc $p = d.\lambda$ pour un certain λ. En vertu de l'irréductibilité de p, soit d soit λ est inversible. Si c'est d, on a gagné. Il faut donc éliminer l'autre cas. Raisonnons par l'absurde. Supposons que λ est inversible, alors $(d) = (p)$. Mais alors q qui est dans (d) est aussi dans (p), donc divisible par p, ce qui est exclu par hypothèse.
c)Si a est irréductible. Soit a divise b et on a gagné. Sinon, a et b sont premiers entre eux d'après la question précédente. Et dans ce cas a divise c d'après la première question.

Exercice 78.
a)Faire la division de $25 + 3i$ par $3 + i$.
b)Trouver le pgcd de ces deux entiers de Gauss.

Correction 78.
a)$25 + 3i = (8 - 2i)(3 + i) + (-1 + i)$.
b)L'expression précédente montrer que les diviseurs communs à $25 + 3i$ par $3 + i$ coïncident avec les diviseurs communs à $3 + i$ et $-1 + i$. Donc $pgcd(5 + 3i, 3 + i) = pgcd(3 + i, -1 + i)$. En effectuant une division supplémentaire: $(3 + i) = (-1 - 2i)(-1 + i) + 0$, on voit que le pgcd est $-1 + i$.

Rappelons que la factorisation dans les anneaux factoriels n'est définie qu'à produit par des inversibles près. Par exemple, dans $\mathbb{Z}[i]$, un élément $e = abcd$ qui s'écrit comme produit de 4 irréductibles s'écrit aussi sous la forme $(ia)(ib)(ic)(id)$ puisque $i^4 = 1$. Les inversibles à l'aide desquels on peut changer la factorisation sont les suivants.

Proposition 117. *Soit $q = a + bi \in \mathbb{Z}[i]$. Les propositions suivantes sont équivalentes.*

- *q est inversible*
- *$N(q) = 1$*
- *$q \in \{1, -1, i, -i\}$.*

Démonstration. On adopte le schéma de démonstration $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.
Si q est inversible d'inverse r, alors $N(q)N(r) = N(qr) = N(1) = 1$.

Comme $N(q)$ et $N(r)$ sont des entiers positifs, la seule possibilité est $N(q) = N(r) = 1$.
Soit $q = a + bi$. Si $N(q) = a^2 + b^2 = 1$, la seule possibilité sachant que a et b sont entiers est que a et b aient pour valeur 1 ou -1, c'est à dire que $q \in \{1, -1, i, -i\}$.
Enfin, si $q \in \{1, -1, i, -i\}$, alors q est évidemment inversible: les inverses de $\{1, -1, i, -i\}$ étant respectivement $\{1, -1, -i, i\}$. ■

5.2 Décomposition en irréductibles dans $\mathbb{Z}[i]$

D'après la section précédente, $\mathbb{Z}[i]$ est factoriel, donc tout nombre se décompose de façon essentiellement unique en produit d'irréductibles. Dans cette section, on cherche à écrire explicitement une telle décomposition. La première question est de savoir qui sont les irréductibles de $\mathbb{Z}[i]$. On commence par une réponse partielle.

Proposition 118.
- *Soit $q = a + bi$. Si $N(q)$ est un nombre premier, alors q est irréductible dans $\mathbb{Z}[i]$.*
- *Si $p \in \mathbb{Z}$ est irréductible dans $\mathbb{Z}[i]$, alors c'est un nombre premier au signe près.*

Exemple 119. *L'entier de Gauss $2 + i$ est irréductible puisque sa norme 5 est un nombre premier. De même $1+i$ et $1-i$ sont irréductibles. En particulier, $2 = (1+i)(1-i)$ est une décomposition de 2 en produit d'irréductibles.*

Démonstration. Commençons par le premier point. Soit q un entier de Gauss tel que $N(q) = p$ est premier et $q = rs$ une factorisation. On veut montrer que l'un des deux termes r ou s est inversible. On a $p = N(q) = N(rs) = N(r)N(s)$. Comme la norme sur $\mathbb{Z}[i]$ est un entier positif et que p est premier, la seule possibilité est que $N(r) = 1$ et $N(s) = p$ (à échange de r et s près). Mais d'après la caractérisation des inversibles de $\mathbb{Z}[i]$, cela signifie que r est inversible. Donc q est irréductible.
Pour le deuxième point, on procède par contraposée. On veut montrer qu'un entier $p = qr$ non irréductible dans $\mathbb{Z}$ n'est pas non plus irréductible dans $\mathbb{Z}[i]$. Comme p n'est pas premier, on peut supposer que q et r sont différents de 1 et -1, donc ne sont pas de norme égale à 1. Ils sont donc non inversibles dans $\mathbb{Z}[i]$ et la décomposition non triviale $p = qr$ montre que p n'est pas irréductible dans $\mathbb{Z}[i]$. ■

La réciproque de la dernière affirmation de la proposition est elle vraie ? Un nombre premier de $\mathbb{Z}$ est il irréductible dans $\mathbb{Z}[i]$? Non, l'égalité $2 = (1+i)(1-i)$ de l'exemple précédent montre que 2 n'est pas irréductible. En revanche, j'affirme que 3 est irréductible dans $\mathbb{Z}[i]$. En effet supposons que 3 s'écrive $3 = uv$. On veut montrer que u ou v est inversible. Comme $N(3) = 9 = N(u)N(v)$. Si $N(u)$ ou $N(v)$ vaut 1, alors u ou v est inversible et on a gagné. Le seul cas qui nous embête et qu'il faut éliminer est donc celui où $N(u) = N(v) = 3$. Mais $N(u) = N(a+ib)$ est un entier de la forme a^2+b^2. Et on sait d'après l'exercice 79 qu'une somme de carrés n'est jamais congrue à trois modulo quatre. Donc le cas $N(u) = 3$ est impossible.

Exercice 79. Montrer qu'une somme de carrés $a^2 + b^2$ ne vaut jamais 3 dans $\mathbb{Z}/4\mathbb{Z}$.

Correction 79. Si $a \in \mathbb{Z}/4\mathbb{Z}$ vaut $\dot{0}, \dot{1}, \dot{2}, \dot{3}$, a^2 vaut $\dot{0}, \dot{1}, \dot{0}, \dot{1}$. De même b^2 ne peut valoir que $\dot{0}$ ou $\dot{1}$. Et donc a^2+b^2 ne peut valoir que $\dot{0}+\dot{0}, \dot{0}+\dot{1}$ ou $\dot{1}+\dot{1}$, et ainsi ne prend jamais la valeur $\dot{3}$.

En regardant attentivement la démonstration précédente, on remarque qu'elle se généralise. C'est ce que vous propose l'exercice suivant:

Exercice 80. Montrer que les nombres premiers de $\mathbb{Z}$ congrus à trois modulo quatre sont irréductibles dans $\mathbb{Z}[i]$.

Correction 80. Soit $x \equiv 3(4)$ un nombre premier. Supposons que x s'écrive $x = uv$. On veut montrer que u ou v est inversible. Comme $N(x) = x^2 = N(u)N(v)$. Si $N(u)$ ou $N(v)$ vaut 1, alors u ou v est inversible et on a gagné. Le seul cas qui nous embête et qu'il faut éliminer est donc celui où $N(u) = N(v) = x$. Mais $N(u) = N(a+ib)$ est un entier de la forme a^2+b^2. Et on sait d'après un exercice précédent qu'une somme de carrés n'est jamais congrue à trois modulo quatre. Donc le cas $N(u) = x$ est impossible.

Résumons nous. Si on prend $p \in \mathbb{Z}$, il arrive que p soit réductible dans $\mathbb{Z}[i]$, comme pour $p = 2$, et il arrive que p soit irréductible, par exemple si p est de la forme $3 + 4k$. Traitons un exemple supplémentaire, le cas $p = 5$. On remarque que 5 est somme de deux carrés, d'où l'égalité $5 = 1+4 = (1+2i)(1-2i)$ qui montre que 5 n'est pas irréductible. Les nombres 7 et 11 sont de la forme $3 + 4k$ donc irréductibles dans $\mathbb{Z}[i]$. Le nombre premier suivant pour lequel on ne sait s'il est irréductible est $p = 13$. Celui-ci n'est pas une somme de carrés, et on ne peut pas appliquer le même argument que pour 5. Mais en fait, on fait une variation du même argument en remarquant que 2.13 est un somme de carrés. Considérons l'égalité $2.13 = 1+25 = (1+5i)(1-5i)$

. Supposons un instant que 13 soit irréductible. Alors, puisque 13 divise le produit $(1+5i)(1-5i)$, il divise l'un des termes, par exemple $1+5i$, mais c'est impossible puisque $N(13)=169$ ne divise pas $N(1+5i)=26$. Donc 13 n'est pas irréductible et s'écrit comme un produit $13=uv$ de non inversibles. Puisque u et v ne sont pas de norme 1, la seule possibilité est $N(u)=N(v)=13$, donc u et v sont irréductibles car de norme un nombre premier. Donc la décomposition de 13 en facteurs premiers est de la forme $13=uv$. Au delà de ce raisonnement, on peut vérifier à la main l'existence des entiers de Gauss précédents u et v.

Exercice 81. Vérifiez qu'il existe des entiers de Gauss u et v tels que $13=uv$.

Correction 81. Il faut chercher $u=a+ib$ de norme 13 donc $a^2+b^2=13$ avec a et b entiers. Il faut donc $a=2,b=3$ ou $a=3,b=2$. Les candidats pour u et v sont donc $2+3i, 2-3i, 3+2i, 3-2i$. A tatons à l'aide de ces candidats, on trouve finalement $13=(2+3i)(2-3i)$.

La démonstration que l'on a faite pour 13 reposait sur le fait qu'un certain multiple de 13 est une somme de la forme 1+ un carré, ie. $2.13=1+5^2$. On peut généraliser cette remarque à tous les nombres de la forme $1+4k$.

Lemme 120. *Si p est un nombre premier congru à un modulo 4, alors il existe $\lambda\in\mathbb{Z}$ tel que $\lambda p=1+a^2$, où $a\in\mathbb{Z}$.*

Démonstration. On admet le point suivant de théorie des corps: les éléments de $\mathbb{Z}/p\mathbb{Z}$ non nuls forment un groupe pour la multiplication et ce groupe est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. En particulier un générateur g de ce groupe vérifie $g^{p-1}=1$ et $g^{\frac{p-1}{2}}\neq 1$. L'élément $g^{\frac{p-1}{2}}$ est un élément de carré égal à 1 et différent de 1, donc c'est -1. Notons $\dot{a}=g^{\frac{p-1}{4}}$. D'après ce qui précède, $\dot{a}^2=-1$ dans $\mathbb{Z}/p\mathbb{Z}$. Donc si $a\in\mathbb{Z}$ est un élément dans $\mathbb{Z}$ dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ est $\dot{a}$, l'égalité $\dot{a}^2=-1$ se traduit par l'existence d'un λ tel que $\lambda p=1+a^2$. ∎

Avec ce lemme, on peut généraliser le raisonnement qui montrait que 13 est un produit de deux irréductibles dans $\mathbb{Z}[i]$.

Proposition 121. *La décomposition dans $\mathbb{Z}[i]$ d'un nombre premier $p\in\mathbb{Z}$ de la forme $1+4k$ est de la forme $p=uv$.*

Démonstration. On sait d'après le lemme qu'un certain multiple $\lambda p=a^2+1^2=a^2+b^2$ est une somme de carrés. Donc $\lambda p=a^2+1^2=(a+i)(a-i)$.

Si p était irréductible, p diviserait l'un des facteurs de $(a+i)(a-i)$, par exemple $a+i$. On aurait alors $(a+i) = p(q+ri)$, et en particulier pour la partie imaginaire $i = pri$, c'est à dire $pr = 1$, ce qui est absurde pour des entiers avec $p > 1$. Donc p n'est pas irréductible et on peut l'écrire sous la forme $p = uv$ de deux éléments non inversibles. On veut montrer alors que u et v sont irréductibles et que $p = uv$ est la décomposition en irréductibles. En passant aux normes, $p = uv$ implique $p^2 = N(p) = N(u)N(v)$. Puisque u et v sont non inversibles, ils ne sont pas de norme 1. La seule possibilité est donc $N(u) = N(v) = p$. Les entiers de Gauss u et v sont donc irréductibles puisque leur norme est un nombre premier. ■

Un nombre premier différent de 2 est congru à 1 mod 4 ou à 3 mod 4. On peut donc finalement résumer l'étude précédente par le résultat suivant:

Théorème 122. *Soit $p \in \mathbb{Z}$ un nombre premier.*

- *si $p = 2$, alors p est réductible et sa décomposition est $2 = (1+i)(1-i)$.*
- *si $p \equiv 1(4)$, alors p est réductible et sa décomposition est $p = uv$ est un produit de deux irréductibles de norme p.*
- *Si $p \equiv 3(4)$, alors p est irréductible dans $\mathbb{Z}[i]$.*

Venons-en enfin à notre problème. Etant donné un entier de Gauss $q = a + bi$ non inversible ni nul, comment calculer sa décomposition en irréductibles ? On commence par chercher un élement e qui le divise. Pour cela, on remarque que si e divise q, alors il divise $q\overline{q} = a^2 + b^2$. Décomposons $q\overline{q} \in \mathbb{N}$ en produit de nombre entiers $p_1 \dots p_r$, puis décomposons chacun des p_i qui peuvent l'être en vertu du théorème précédent en produit de deux irréductibles. On obtient ainsi une expression de la forme $q\overline{q} = e_1 \dots e_s$. Nécessairement, l'un des e_i divise q, disons par exemple e_1. D'où $q = e_1 r_1$. On calcule r_1. Si l'un des e_i divise r_1, par exemple e_2, on écrit $q = e_1 e_2 r_2$ et on calcule r_2. On recommence avec r_2 et ainsi de suite. Au bout d'un nombre fini d'étapes, on se retrouve avec une décomposition de la forme $q = r_n e_1 e_2 \dots e_n$ avec r_n non divisible un e_i. Alors r_n est inversible. L'élément $e'_1 = r_n e_1$ est irréductible. La décomposition $q = e'_1 e_2 \dots e_n$ est la décomposition en irréductibles cherchée.
L'exercice suivant a pour but de justifier quelques une des affirmations précédentes.

Exercice 82. On reprend les notations du paragraphe suivant le théorème 122.
a)Justifier le fait que l'un des e_i divise q

b)Dire pourquoi au bout d'un nombre fini d'étapes, on obtient un r_n qui n'est plus divisible par l'un des e_i
c)Justifier le fait que r_n est inversible.
d)Justifier le fait que e'_1 est irréductible

Correction 82.
a)Les irréductibles divisant q sont aussi des irréductibles divisant $q\overline{q}$. Autrement dit, tout irréductible d divisant q se trouve être l'un des e_i. Comme q n'est pas inversible, il est divisible par au moins un d irréductible, d'où l'existence du e_i correspondant.
b)Les e_i sont irréductibles, donc de norme au moins 2 (puisque les éléments de norme 1 sont inversibles donc non irréductibles). Il s'ensuit que la norme de r_{n+1} est inférieure à la norme de r_n. La suite des normes des r_i est une suite d'entiers positifs strictement décroissante. Si le processus ne s'arrêtait pas, on aurait construit une suite infinie décroissante d'entiers strictement positifs, ce qui n'est pas possible.
c)Si r_n n'était pas inversible, il serait divisible par un élément irréductible d. Ce d diviserait aussi q, et donc par la première question, ce d serait l'un des e_i. Or par hypothèse r_n n'est pas divisible par un e_i. Il faut donc que r_n soit inversible.
d)Multiplier par un inversible ne change pas l'irréductibilité ou la non irréductibilité. Puisque r_n est inversible, e'_1 est comme e_1 un irréductible.

Exercice 83. Appliquer l'algorithme pour trouver la décomposition en irréductibles de $6+8i$ dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

Correction 83. $(6+8i)(6-8i) = 100 = 2^2.5^2 = (1+i)^2(1-i)^2(1+2i)^2(1-2i)^2$. On a $6+8i = (1+i)(7+i)$, $7+i = (1+3i)(1-2i)$, $1+3i = (1-2i)(-1+i)$. D'où au total la décomposition $6+8i = (1+i)(1-2i)^2(-1+i)$.

5.3 Le théorème des deux carrés.

Soit $n \in \mathbb{N}$ un entier et $n = n_1 \dots n_s$ sa décomposition en produit de nombre premiers. Chaque n_i vaut soit deux, soit est congru à 1 mod 4, soit est congru à 3 mod 4. On peut donc écrrire sa décomposition sous la forme

$$n = 2^r \prod_{p_i \equiv 1(4)} p_i^{s_i} \prod_{p_i \equiv 3(4)} p_i^{t_i}.$$

Théorème 123. *Un nombre entier différent de* 0 *et* 1 *est somme de deux carrés ssi dans la décomposition précédente les t_i sont des nombres pairs.*

Démonstration. Remarquons tout d'abord que si $n = a^2 + b^2$ est somme de deux carrés alors n est la norme d'un entier de Gauss, en l'occurence $a + bi$. La réciproque étant évidente, nous obtenons:

Lemme 124. *Un entier est somme de deux carrés ssi il est la norme d'un entier de Gauss.*

Supposons que $n_1, \ldots, n_k$ soient somme de deux carrés: $n_1 = N(u_1), \ldots, n_k = N(u_k)$. Alors la quantité $n_1 \ldots n_k = N(u_1) \ldots N(u_k) = N(u_1 \ldots u_k)$ est une somme de deux carrés puisque c'est une norme. Autrement dit, nous avons démontré le lemme suivant:

Lemme 125. *Si $n_1, \ldots, n_k$ sont somme de deux carrés, leur produit est également somme de deux carrés.*

Exercice 84. Écrire explicitement $40 = (1 + 4)(4 + 4)$ comme une somme de deux carrés.

Correction 84. $1 + 4 = (1 + 2i)(1 - 2i) = N(1 + 2i)$ et $4 + 4 = N(2 + 2i)$. Donc $40 = N(1+2i)N(2+2i) = N((1+2i)(2+2i)) = N(-2+6i) = 4^2+6^2$. C'est l'écriture voulue en somme de carrés.

Choisissons maintenant un nombre $n = 2^r \prod_{p_i \equiv 1(4)} p_i^{s_i} \prod_{p_i \equiv 3(4)} p_i^{t_i}$ avec t_i pair et montrons qu'il est somme de deux carrés. D'après le lemme, il suffit de démontrer que

- 2 est somme de deux carrés
- un premier congru à 1 mod 4 est somme de deux carrés.
- $p_i^{t_i}$ est somme de deux carrés si $p_i \equiv 3(4)$ et si t_i est pair.

Le premier point est évident: $2 = 1 + 1$ est une somme de carrés. Pour le troisième point, puisque t_i est pair, $p_i^{t_i} = 0^2 + (p_i^{\frac{t_i}{2}})^2$ est une somme de carrés. Enfin, si p_i est congru à 1 modulo 4, on sait par le théorème 122 que $p_i = uv$ est un produit de deux irréductibles de $\mathbb{Z}[i]$. Donc $N(p_i) = p_i^2 = N(u)N(v)$. Puisque $N(u)$ et $N(v)$ ne peuvent être égaux à 1, la seule possibilité est $N(u) = N(v) = p_i$. Donc p_i est une norme et c'est donc une somme de deux carrés.
Montrons maintenant réciproquement que si un nombre $n = a^2 + b^2$ différent de 0 et 1 est somme de deux carrés, les t_i apparaissant dans sa décomposition sont pairs. On procède par récurrence sur $n \geq 2$. C'est évident pour $n = 2$. Pour n quelconque, soit p_i un nombre premier congru à 3 mod 4. Si p_i ne divise pas n, on a $t_i = 0$ qui est donc pair. Sinon, p_i divise $n = a^2 + b^2 = (a + b_i)(a - bi)$ dans $\mathbb{Z}$, donc dans $\mathbb{Z}[i]$. Mais d'après

le théorème 122, p_i est irréductible dans $\mathbb{Z}[i]$. Donc p_i divise l'un des deux facteurs, par exemple $(a+bi)$: $(a+bi) = p_i q$. Mais alors on a aussi $(a-bi) = p_i \overline{q}$, d'où $n = p_i^2 q\overline{q}$. L'entier $q\overline{q}$ est une somme de carrés puisque c'est une norme, donc par hypothèse de récurrence, p_i apparait avec une puissance paire $2k$ dans sa décomposition irréductible. Il s'ensuit que p_i apparait avec la puissance paire $2k+2$ dans la décomposition de n. ■

Exercice 85.
a)Dire parmi les nombres suivants lesquels sont des sommes de 2 carrés: 108,134,980.
b)En vous inspirant de la démonstration du théorème des deux carrés et en écrivant chacun de leurs facteurs comme somme de deux carrés, écrire explicitement les nombres ci-dessus comme somme de deux carrés.

Correction 85.
a)$108 = 2^2.3^3$ n'est pas somme de 2 carrés car la puissance de 3 est impaire. $134 = 2.67$ n'est pas somme de 2 carrés car la puissance de 67 est impaire. $980 = 2^2.5.7^2$ est somme de carrés. Des égalités $4 = N(2)$, $5 = N(2+i)$, $7^2 = N(7)$, on tire, $980 = N(14.(2+i)) = N(28+14i)$. Donc $980 = 28^2+14^2$.