Anneaux et corps

Table des matières

1 Anneaux et corps, premiers pas

Dans ce paragraphe nous introduisons quelques notions générales liées à la structure d'anneau. Nous définirons les corps et après un bref rappel sur les anneaux de polynômes à une indéterminée nous étudierons les anneaux $\mathbb{Z}/n\mathbb{Z}$ pour obtenir des résultats d'arithmétique.

1.1 Notions générales

Définition 1.1

Un **anneau** A est un groupe commutatif, dont la loi est noée $+$ et l'élément neutre 0, muni d'une multiplication $(x, y) \mapsto xy$ ayant les propriétés suivantes :

- ◇ la multiplication est associative : pour tous x, y, z dans A nous avons $(xy)z = x(yz)$, élément noté simplement xyz ;
- ◇ la multiplication est distributive par rapport à l'addition : pour tous x, y, z dans A nous avons

$$x(y+z) = xy + xz \qquad \text{et} \qquad (x+y)z = xz + yz;$$

- ◇ il y a un élément unité, noté 1 ou 1_A : pour tout x dans A, nous avons $x\,1 = 1\,x = x$.

Si la multiplication est commutative, c'est-à-dire si $xy = yx$ pour tous x, y dans A, on dit que l'anneau A est **commutatif**.

Proposition 1.1

Si A est un anneau, alors
- pour tous $x \in A$, $x\,0 = 0\,x = 0$ et $(-1)\,x = -x$;
- l'élément unité est unique.

Démonstration. En effet d'après la distributivité nous avons

$$x = (1+0)\,x = 1\,x + 0\,x = x + 0\,x$$

par suite, en ajoutant $-x$ (rappelons que A muni de la loi $+$ est un groupe) de part et d'autre de l'égalité, nous obtenons $0 = 0\,x$. Un raisonnement analogue conduit à $0\,x = x$.

Puisque $x + (-1)x = (1 + (-1))x = 0\,x = 0$ nous avons $(-1)\,x = -x$.

Enfin si u est un élément unité, alors $ux = x$ pour tout $x \in A$ d'où $u = u\,1 = 1$. □

Il existe des anneaux non commutatifs, comme l'anneau des matrices carrées $n \times n$, $n \geq 2$, à coefficients réels.

Dans la suite le terme anneau signifiera anneau commutatif. De plus, nous supposerons toujours que $1 \neq 0$.

Définition 1.2

Soit A un anneau. Un *sous-anneau* de A est un sous-groupe additif B de A tel que
- $1 \in B$,
- $\forall\, x,\, y \in B,\, xy \in B$.

Si B est un sous-anneau de A, alors B est un anneau pour la multiplication définie dans A.

Exemple 1. Les groupes $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis du produit des nombres, sont des anneaux. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ et $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$.

Exemple 2. L'ensemble $\mathbb{R}[X]$ des polynômes à coefficients réels est un anneau ; l'élément 0 est le polynôme nul et l'élément unité est le polynôme constant 1.

Exemple 3. L'ensemble $\mathbb{Z}[X]$ des polynômes à coefficients entiers est un sous-anneau de $\mathbb{R}[X]$.

Exemple 4. L'*anneau des entiers de Gauss*

$$\mathbb{Z}[\mathbf{i}] = \{a + b\mathbf{i} \mid a \in \mathbb{Z},\, b \in \mathbb{Z}\}.$$

Montrons que $\mathbb{Z}[\mathbf{i}]$ est un sous-anneau de $\mathbb{C}$.

Pour tous a, b, c, $d \in \mathbb{Z}$, la somme

$$(a + b\mathbf{i}) + (c + d\mathbf{i}) = (a + c) + (b + d)\mathbf{i}$$

appartient à $\mathbb{Z}[\mathbf{i}]$ et l'opposé $-a - b\mathbf{i}$ aussi. Ainsi $\mathbb{Z}[\mathbf{i}]$ est un sous-groupe additif de $\mathbb{C}$. Considérons le produit

$$(a + b\mathbf{i}) + (c + d\mathbf{i}) = (ac - bd) + (ad + bc)\mathbf{i};$$

la partie réelle et la partie imaginaire sont des entiers. Il en résulte que ce produit appartient à $\mathbb{Z}[\mathbf{i}]$. Enfin $1 = 1 + 0\,\mathbf{i}$ appartient à $\mathbb{Z}[\mathbf{i}]$. Finalement $\mathbb{Z}[\mathbf{i}]$ est un sous-anneau de $\mathbb{C}$.

Exemple 5. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ est un anneau.

Exemple 6. *Anneau produit.* Si A et B sont des anneaux, nous définissons la multiplication dans $A \times B$ en posant

$$\forall x, \forall x' \in A, \forall y, y' \in B, (x, y)(x', y') = (xx', yy').$$

Alors le groupe additif $A \times B$ est un anneau d'élément unité $(1_A, 1_B)$, appelé anneau produit de A et B. Dans un anneau produit, on ajoute et on multiplie composante par composante.

1.1.1 Multiple, diviseur, élément inversible

Définitions 1.1

Soit A un anneau.

- ◇ Soient a, $b \in A$. On dit que a divise b, ou que b est un multiple de a, s'il existe $q \in A$ tel que $b = aq$. Cela se note $a \mid b$.
- ◇ Un élément $a \in A$ est *inversible* s'il existe $a' \in A$ tel que $aa' = 1$.

L'ensemble des éléments inversibles de A est noté A^*.

Si un élément est inversible, son inverse est unique. En effet, s'il exsite a', $a'' \in A$ tels que $aa' = a''a = 1$, alors

$$a' = 1a' = (a''a)a' = a''(aa') = a''1 = a''.$$

L'inverse d'un élément inversible a se note a^{-1}.

- ◇ Si $a \in A$ est inversible, alors tout élément de A est multiple de a. En effet, si a est inversible, alors pour tout $x \in A$, nous avons $x = x1 = (xa^{-1})a$, *i.e.* x est multiple de a.
- ◇ 0 n'est pas inversible. En effet, si 0 était inversible, alors 1 serait multiple de 0 donc nous aurions $1 = 0$.

Remarque 1. Si B est un sous-anneau de A, un élément de B peut être inversible dans A sans être inversible dans B : par exemple, l'entier 2 est inversible dans $\mathbb{Q}$ mais pas dans $\mathbb{Z}$.

Proposition 1.2

Soit A un anneau. L'ensemble A^* des éléments inversibles de A est un groupe pour la multiplication ; l'élément neutre est 1.

Démonstration. Soient a, b dans A^* ; alors $(ab)(b^{-1}a^{-1}) = 1$, d'où ab appartient à A^*. D'une part 1 appartient à A^* et d'autre part a^{-1} a pour inverse a, donc a^{-1} appartient à A^*. La multiplication étant associative A^* est un groupe multiplicatif. □

Proposition 1.3

Soient A et B des anneaux. Nous avons $(A \times B)^* = A^* \times B^*$.

Démonstration. Soit $(a,b) \in A \times B$. Pour tous $(x,y) \in A \times B$, nous avons $(a,b)(x,y) = (ax, by)$. Pour que (a,b) soit inversible il faut et il suffit qu'il existe $x \in A$ et $y \in B$ tels que $ax = 1_A$ et $by = 1_B$ ce qui signifie $(a,b) \in A^* \times B^*$. □

Définition 1.3

Un *corps* est un anneau $\Bbbk$ dont tous les éléments non nuls sont inversibles, autrement dit $\Bbbk^* = \Bbbk \smallsetminus \{0\}$.

Proposition 1.4

Soit $\Bbbk$ un corps. Pour tous x, $y \in \Bbbk$ nous avons

$$xy = 0 \iff (x = 0 \text{ ou } y = 0)$$

Démonstration. Si x ou y est nul, alors $xy = 0$. Réciproquement, soient x, $y \in \Bbbk$ tels que $xy = 0$; si $x \neq 0$, alors x est inversible et nous avons $0 = x^{-1}0 = x^{-1}xy = y$. □

Exemples 1.

- ◇ Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
- ◇ Le groupe des inversibles de l'anneau $\mathbb{Z}$ est $\mathbb{Z}^* = \{1, -1\}$. En effet, 1 et -1 sont leur propre inverse et si $a \in \mathbb{Z}$ est inversible, alors a divise 1 donc $a = \pm 1$.
- ◇ Dans l'anneau de polynômes $\mathbb{R}[X]$ les éléments inversibles sont les polynômes constants non nuls : le groupe $\left(\mathbb{R}[X]\right)^*$ est isomorphe à $\mathbb{R}^*$.
- ◇ Déterminons les éléments inversibles de l'anneau $\mathbb{Z}[\mathbf{i}]$ des entiers de Gauss. Remarquons d'abord que pour tout $z = a + b\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$, la quantité $|z|^2 = a^2 + b^2$ est un entier positif ou nul. Soit z un élément inversible de $\mathbb{Z}[\mathbf{i}]$; il existe $z' \in \mathbb{Z}[\mathbf{i}]$ tel que $zz' = 1$; par suite $1 = |zz'| = |z|\,|z'|$ et $1 = |z|^2\,|z'|^2$. Puisque $|z|^2$ et $|z'|^2$ sont des entiers positifs ou nuls, nous en déduisons que $|z|^2 = 1$. En posant $z = a + \mathbf{i}b$, il vient $a^2 + b^2 = 1$ avec a, b dans $\mathbb{Z}$ donc ou bien $a = \pm 1$ et $b = 0$, ou bien $a = 0$ et $b = \pm 1$. Ainsi z est l'un des nombres 1, -1, $\mathbf{i}$ ou $-\mathbf{i}$. Réciproquement, ces éléments de $\mathbb{Z}[\mathbf{i}]$ sont inversibles dans $\mathbb{Z}[\mathbf{i}]$ (les éléments $\mathbf{i}$ et $-\mathbf{i}$ sont inverses l'un de l'autres). Nous avons donc
$$\left(\mathbb{Z}[\mathbf{i}]\right)^* = \{1, -1, \mathbf{i}, -\mathbf{i}\}.$$
- ◇ Montrons que $2 + 3\mathbf{i}$ divise $5 + \mathbf{i}$ dans l'anneau $\mathbb{Z}[\mathbf{i}]$.
Puisque $\mathbb{Z}[\mathbf{i}]$ est un sous-anneau de $\mathbb{C}$, calculons le quotient $\frac{5+\mathbf{i}}{2+3\mathbf{i}}$:
$$\frac{5+\mathbf{i}}{2+3\mathbf{i}} = \frac{(5+\mathbf{i})(2-3\mathbf{i})}{(2+3\mathbf{i})(2-3\mathbf{i})} = \frac{(5+\mathbf{i})(2-3\mathbf{i})}{2^2+3^2} = \frac{13-13\mathbf{i}}{13} = 1-\mathbf{i}.$$
Nous avons $5 + \mathbf{i} = (2 + 3\mathbf{i})(1 - \mathbf{i})$ donc $5 + \mathbf{i}$ est multiple de $2 + 3\mathbf{i}$ dans l'anneau $\mathbb{Z}[i]$.

1.2 Morphismes

Définition 1.4

Soient A et B des anneaux. Une application $f\colon A \to B$ est un morphisme d'anneaux si

$$\forall\, x, y \in A, \quad f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_A) = 1_B.$$

Un morphisme d'anneaux est donc un morphisme de groupes compatible avec les multiplications et envoyant l'élément unité sur l'élément unité.

Exemples 2.

- ◇ La conjugaison

$$\mathbb{Z}[\mathbf{i}] \to \mathbb{Z}[\mathbf{i}] \qquad\qquad z \mapsto \overline{z}$$

est un morphisme d'anneaux.

- ◇ Soit $a \in \mathbb{R}$. À tout polynôme $P \in \mathbb{R}[X]$, associons $P(a)$ sa valeur en a. Nous définissons ainsi une application

$$\upsilon\colon \mathbb{R}[X] \to \mathbb{R}, \qquad\qquad P \mapsto P(a).$$

Si P et Q sont des polynômes, nous avons évidemment $(P+Q)(a) = P(a)+Q(a)$ et $(PQ)(a) = P(a)Q(a)$; de plus, le polynôme constant 1 a pour valeur 1. L'application υ est donc un morphisme d'anneaux.

- ◇ Concrétisons la notion de morphisme d'anneaux sur un autre exemple. Essayons de déterminer les morphismes d'anneaux f de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$. Pour l'image de 0 et de 1 nous n'avons pas le choix : par définition $f(0) = 0$ et $f(1) = 1$. Mais alors

$$f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 0, \qquad f(3) = f(2) + f(1) = 0 + 1 = 1.$$

En continuant ainsi nous montrons par récurrence que $f(n) = \underbrace{1+1+\ldots+1}_{n \text{ fois}}$ pour n positif. Si n est pair, alors $f(n) = 0$ et si n est impair, alors $f(n) = 1$. D'autre part pour un nombre négatif l'égalité

$$f(n) + f(-n) = f(n-n) = f(0) = 0$$

montre que $f(-n) = -f(n)$, c'est-à-dire que $f(-n) = 0$ si n est pair et $f(-n) = -1 = 1$ si n est impair. Nous pouvons vérifier que nous avons ainsi bien défini un morphisme d'anneaux. Nous pouvons généraliser l'étude précédente :

Théorème 1.1

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

Démonstration. L'unicité se démontre exactement comme dans l'exemple. Nous n'avons pas le choix pour $f(1)$, puis pour $f(2)$, $f(3)$, …, $f(n)$ et $f(-n)$. De plus ce raisonnement montre que

nécessairement $f(n) = n \times 1$ et $f(-n) = -n \times 1$. Il y a donc 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'anneaux. Nous avons bien $f(1) = 1$ et $f(0) = 0$ par les formules. Vérifions que $f(x + y) = f(x) + f(y)$:
- ◇ d'une part $f(x + y) = (x + y) \cdot 1 = x \cdot 1 + y \cdot 1$,
- ◇ d'autre part $f(x) + f(y) = x \cdot 1 + y \cdot 1$

d'où $f(x + y) = f(x) + f(y)$. Nous pouvons de même montrer que $f(xy) = f(x)f(y)$ et $f(-x) = -f(x)$. □

Proposition 1.5

Soit $f\colon A \to B$ un morphisme d'anneaux. Pour tout élément x inversible dans A, $f(x)$ est inversible dans B et $(f(x))^{-1} = f(x^{-1})$. Le morphisme f définit un morphisme de groupes

$$A^* \to B^*, \qquad x \mapsto f(x)$$

Démonstration. Soit $x \in A^*$. Nous avons

$$1_B = f(1_A) = f(xx^{-1}) = f(x)f(x^{-1});$$

par suite $f(x)$ et $f(x^{-1})$ sont inverses l'un de l'autre dans B. Puisque $f(xy) = f(x)f(y)$ pour tous x, y dans A^*, l'application

$$A^* \to B^*, \qquad x \mapsto f(x)$$

est un morphisme de groupes de A^* dans B^*. □

1.2.1 Idéal

Définition 1.5

Soit A un anneau. Un *idéal* de A est un sous-groupe additif $\mathcal{I}$ de A ayant la propriété suivante

$$\forall\, a \in \mathcal{I},\ \forall\, x \in A,\ xa \in \mathcal{I}.$$

Un idéal est donc un sous-groupe pour l'addition qui est stable par multiplication par un élément quelconque de l'anneau.

Exemples 3.
- ◇ Soit A un anneau. Alors $\{0\}$ et A sont des idéaux de A.
- ◇ L'ensemble $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Proposition-Définition 1.1

Soit A un anneau.
- ◇ Pour tout $a \in A$, l'ensemble $\{ax \,|\, x \in A\}$ des multiples de a est un idéal de A noté aA ou (a). On dit que aA est l'*idéal engendré par* a.
- ◇ Pour tous a, $b \in A$, nous avons l'équivalence : $aA \subset bA \iff b \,|\, a$.

Démonstration. Pour tous x, $y \in A$, nous avons $xa + ya = (x+y)a$ et $-xa = (-x)a$. Puisque $0 = 0\,a$ est multiple de a, l'ensemble aA est un sous-groupe additif de A. Soient $b \in aA$ et $x \in A$. Il existe $u \in A$ tels que $b = au$ d'où $bx = a(ux)$ appartient à aA.

Si $aA \subset bA$, alors a appartient à bA donc a est multiple de b. Réciproquement, si b divise a, alors tout multiple de a est multiple de b, par conséquent $aA \subset bA$. □

Définition 1.6

Soient A un anneau et $\mathcal{I}$ un idéal de A. S'il existe $a \in \mathcal{I}$ tel que $\mathcal{I} = aA$, on dit que l'idéal $\mathcal{I}$ est principal.

Proposition 1.6

Tout idéal de l'anneau $\mathbb{Z}$ est principal.

Démonstration. Un idéal est un sous-groupe additif et les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$. □

Proposition 1.7

Soit $f\colon A \to B$ un morphisme d'anneaux.
Le noyau de f est un idéal de A distinct de A.
L'image de f est un sous-anneau de B.

Démonstration. Comme f est un morphisme de groupes, $\ker f$ est un sous-groupe additif de A. Soit $a \in \ker f$. Pour tout $x \in A$, nous avons

$$f(ax) = f(a)f(x) = 0\,f(x) = 0;$$

il en résulte que ax appartient à $\ker f$. Ainsi $\ker f$ est un idéal de A. Puisque $f(1_A) = 1_B$, nous avons : 1_A n'appartient pas à $\ker f$; en particulier $\ker f \neq A$.

L'image de f est un sous-groupe additif de B qui contient $f(1) = 1$. De plus, pour tous éléments $u = f(x)$ et $v = f(y)$ appartenant à $\operatorname{im} f$, $uv = f(xy)$ appartient à $\operatorname{im} f$. L'image de f est donc un sous-anneau de B. □

Proposition 1.8

- ◇ Un anneau A est un corps si et seulement si les idéaux de A sont $\{0\}$ et A.
- ◇ Soient $\Bbbk$ un corps et B un anneau. Tout morphisme d'anneaux $\Bbbk \to B$ est injectif.

Démonstration.

◇ Supposons que l'anneau A soit un corps. Soit $\mathcal{I}$ un idéal de A tel que $\mathcal{I} \neq \{0\}$. Il existe $a \in \mathcal{I}$, $a \neq 0$. L'élément a est inversible d'où $a^{-1}a = 1$, donc 1 appartient à $\mathcal{I}$. Par suite, pour tout $x \in A$, nous avons $x = x\,1 \in \mathcal{I}$ donc $\mathcal{I} = A$.

Réciproquement supposons que les seuls idéaux de A soient $\{0\}$ et A et soit $a \in A$, $a \neq 0$. L'idéal aA n'est pas réduit à $\{0\}$ (il contient a) ; par conséquent $aA = A$. Il s'en suit que 1 appartient à aA. Il existe donc $a' \in A$ tel que $1 = aa'$, autrement dit a est inversible.

- ◇ Soit $f\colon \Bbbk \to B$ un morphisme d'anneaux. Puisque $\ker f$ est un idéal de $\Bbbk$ distinct de $\Bbbk$ nous avons $\ker f = \{0\}$, *i.e.* f est injectif.

□

1.3 Anneau quotient

Soient A un anneau et $\mathcal{I}$ un idéal de A tel que $\mathcal{I} \neq A$.

Puisque $\mathcal{I}$ est un sous-groupe additif de A, nous pouvons former le groupe quotient $A/\mathcal{I}$. Soit $p\colon A \to A/\mathcal{I}$ la projection canonique. Soient x, x', y, y' des éléments de A tels que $p(x) = p(x')$ et $p(y) = p(y')$. Nous avons

$$x - x' \in \mathcal{I}, \qquad y - y' \in \mathcal{I}, \qquad xy - x'y' = (x - x')y + x'(y - y').$$

Comme $\mathcal{I}$ est un idéal, les produits $(x - x')y$ et $x'(y - y')$ appartiennent à $\mathcal{I}$, donc aussi leur somme $xy - x'y'$. Ainsi nous avons $p(xy) = p(x'y')$. Il s'en suit que $p(xy)$ ne dépend que des classes $p(x)$ et $p(y)$. Nous pouvons donc définir une multiplication dans $A/\mathcal{I}$ en posant

$$\forall\, \alpha, \beta \in A/\mathcal{I},\ \alpha\beta = p(xy) \text{ si } \alpha = p(x) \text{ et } \beta = p(y)$$

Proposition-Définition 1.2

Soient A un anneau et $\mathcal{I}$ un idéal de A différent de A. La multiplication définie ci-dessus sur le groupe quotient $A/\mathcal{I}$ fait de $A/\mathcal{I}$ un anneau. La projection canonique $p\colon A \to A/\mathcal{I}$ est un morphisme d'anneaux surjectif et $\ker p = \mathcal{I}$. On dit que $A/\mathcal{I}$ est *l'anneau quotient de A par l'idéal $\mathcal{I}$*.

Démonstration. Nous savons que p est un morphisme de groupes. Pour tous x, $y \in A$, nous avons par définition $p(x)p(y) = p(xy)$. Par conséquent pour tout $z \in A$ il vient

$$p(x)(p(y)p(z)) = p(x)p(yz) = p(x(yz)) = p(xy)p(z) = (p(x)p(y))p(z)$$

et

$$p(x)(p(y) + p(z)) = p(x)p(y + z) = p(x(y + z)) = p(xy + xz) = p(xy) + p(xz) = p(x)p(y) + p(x)p(z).$$

Nous avons aussi $p(1)p(x) = p(1\,x) = p(x)$. Puisque tout élément du groupe $A/\mathcal{I}$ s'écrit $p(x)$ où $x \in A$, ces égalités montrent que la multiplication dans $A/\mathcal{I}$ est associative, distributive par rapport à l'addition et que $p(1)$ est l'élément unité. La multiplication dans A étant commutative, celle dans $A/\mathcal{I}$ l'est aussi. Enfin comme $\mathcal{I} \neq A$, 1 n'appartient pas à $\mathcal{I}$ et comme $\ker p = \mathcal{I}$ nous obtenons $p(1) \neq 0$, *i.e.* $1_A \neq 0_A$. □

Pour calculer dans l'anneau quotient $A/\mathcal{I}$ nous calculons dans A et nous passons aux classes en appliquant le morphisme $A \to A/\mathcal{I}$. Comme pour les groupes quotients nous avons le théorème fondamental suivant :

Théorème 1.2: (Théorème de passage au quotient)

Soit $f\colon A \to B$ un morphisme d'anneaux. Soit $\mathcal{I}$ un idéal de A tel que $\mathcal{I} \subset \ker f$. Soit $p\colon A \to A/\mathcal{I}$ la projection canonique. Il existe un unique morphisme d'anneaux $\overline{f}\colon A/\mathcal{I} \to B$ tel que $\overline{f} \circ p = f$.

- ◇ Le morphisme $\overline{f}$ est injectif si et seulement si $\mathcal{I} = \ker f$.
- ◇ Les morphismes f et $\overline{f}$ ont même image. En particulier, $\overline{f}$ est surjectif si et seulement si f est surjectif.

Démonstration. Nous savons qu'il existe un unique morphisme de groupes $\overline{f}\colon A/\mathcal{I} \to B$ tel que $\overline{f} \circ p = f$. Montrons que $\overline{f}$ est un morphisme d'anneaux. Soient α et β dans $A/\mathcal{I}$; alors $\alpha = p(x)$ et $\beta = p(y)$ avec x, $y \in A$. Puisque p est un morphisme d'anneaux, nous avons $\alpha\beta = p(xy)$, puis

$$\overline{f}(\alpha\beta) = \overline{f}(p(xy)) = f(xy)$$

et

$$\overline{f}(\alpha)\overline{f}(\beta) = \overline{f}(p(x))\overline{f}(p(y)) = f(x)f(y)$$

comme f est un morphisme d'anneaux, $\overline{f}(\alpha\beta) = \overline{f}(\alpha)\overline{f}(\beta)$.

La dernière propriété découle du théorème de passage au quotient pour les groupes. □

En appliquant le théorème à l'idéal $\ker f$ de A, nous obtenons l'énoncé suivant :

Corollaire 1.1

Soit $f\colon A \to B$ un morphisme d'anneaux. Il existe un unique morphisme d'anneaux $\overline{f}\colon A/\ker f \to B$ tel que $\overline{f} \circ p = f$.
Le morphisme $\overline{f}$ est injectif.
Si f est surjectif, alors $\overline{f}$ est un isomorphisme.

Exemple 7. Soit $f\colon \mathbb{R}[X] \to \mathbb{C}$ le morphisme d'anneau définie par

$$\forall\, P \in \mathbb{R}[X], \quad f(P) = P(\mathbf{i}).$$

Nous avons $f(X) = \mathbf{i}$, $f(1) = 1$ et $f(X^2+1) = \mathbf{i}^2 + 1 = 0$.

- ◇ Montrons que le noyau de f est l'idéal $(X^2+1)\mathbb{R}[X]$ engendré par le polynôme X^2+1.
  - Soit P un élément de $(X^2+1)\mathbb{R}[X]$, autrement dit soit P un multiple de X^2+1. Écrivons P sous la forme $P = (X^2+1)Q$ avec $Q \in \mathbb{R}[X]$. Nous avons

$$f(P) = \underbrace{f(X^2+1)}_{0} f(Q) = 0 f(Q) = 0;$$

ainsi P appartient à $\ker f$. Nous en déduisons que $(X^2+1)\mathbb{R}[X]$ est inclus dans $\ker f$.

- Soit P un élément de $\ker f$. Alors $P(\mathbf{i}) = 0$. Le nombre complexe $\mathbf{i}$ est racine de P qui est à coefficients réels ; par suite $\overline{\mathbf{i}} = -\mathbf{i}$ est aussi racine de P. Par conséquent P est un multiple de $(X - \mathbf{i})(X + \mathbf{i}) = (X^2 + 1)$, *i.e.* le polynôme P appartient à $(X^2 + 1)\mathbb{R}[X]$.

◇ Notons $p\colon \mathbb{R}[X] \to \mathbb{R}[X]/(X^2+1)$ la projection canonique. D'après le Corollaire 1.1 il existe un morphisme d'anneaux $\overline{f}\colon \mathbb{R}[X]/(X^2+1) \to \mathbb{C}$ injectif tel que

$$\forall\, R \in \mathbb{R}[X] \quad \overline{f}(p(R)) = R(\mathbf{i}).$$

◇ Le morphisme f est surjectif car pour tous réels a et b nous avons $f(a+bX) = a+b\mathbf{i}$. Ainsi $\overline{f}$ est un isomorphisme d'anneaux, autrement dit les anneaux $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{C}$ sont isomorphes. Puisque $\mathbb{C}$ est un corps, l'anneau quotient $\mathbb{R}/(X^2+1)$ est un corps.
Le corps $\mathbb{R}[X]/(X^2+1)$ est une construction des nombres complexes à partir de $\mathbb{R}$.

1.4 Anneau $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier au moins égal à 2.

Puisque $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ différent de $\mathbb{Z}$, nous avons un anneau quotient $\mathbb{Z}/n\mathbb{Z}$. La projection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ associe à tout entier k sa classe $\overline{k}$ modulo n. Cette projection canonique

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad\qquad k \mapsto \overline{k}$$

est un morphisme d'anneaux. En particulier, nous avons

$$\forall\, \overline{k},\, \overline{l} \in \mathbb{Z}/n\mathbb{Z}, \quad \overline{k}\,\overline{\ell} = \overline{k\ell}.$$

Exemple 8. Dans l'anneau $\mathbb{Z}/6\mathbb{Z}$ nous avons $\overline{2}\,\overline{3} = \overline{6} = \overline{0}$: un produit de facteurs non nuls peut donc être nul. En voici une conséquence : pour tout $x \in \mathbb{Z}/6\mathbb{Z}$ nous avons

$$(x-2)(x-3) = x^2 - 5x = x(x-5).$$

C'est une expression polynomiale non identiquement nulle, de degré 2 et ayant quatre racines : $\overline{0}$, $\overline{2}$, $\overline{3}$ et $\overline{5}$.

1.4.1 Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Proposition 1.9

Pour tout entier $k \in \mathbb{Z}$, l'élément $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier à n.

Démonstration. Soit $k \in \mathbb{Z}$. Nous avons les équivalences :

$$\begin{aligned}
k \text{ est premier à } n &\iff \exists\, u,\, v \in \mathbb{Z},\, ku + nv = 1 \text{(théorème de Bezout)} \\
&\iff \exists\, u \in \mathbb{Z},\, ku \equiv 1 \bmod n \\
&\iff \exists u \in \mathbb{Z},\, \overline{k}\,\overline{u} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z} \\
&\iff \overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}.
\end{aligned}$$

□

Pour calculer l'inverse d'un élément inversible $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, nous écrivons une relation de Bezout entre les entiers k et n et nous en prenons la congruence modulo n. Illustrons cette méthode par un exemple.

Exemple 9. Dans l'anneau $\mathbb{Z}/20\mathbb{Z}$ les inversibles sont

$$\overline{1}, \qquad \overline{3}, \qquad \overline{7}, \qquad \overline{11} = -\overline{9}, \qquad \overline{13} = -\overline{7}, \qquad \overline{17} = -\overline{3}, \qquad \overline{19} = -\overline{1}.$$

Le groupe des inversibles $\left(\mathbb{Z}/20\mathbb{Z}\right)^*$ compte huit éléments : $\left(\mathbb{Z}/20\mathbb{Z}\right)^* = \{ \pm\overline{1}, \pm\overline{3}, \pm\overline{7}, \pm\overline{9}\}$

Calculons l'inverse $\overline{9}$. Nous avons la relation de Bezout $9 \times 9 - 4 \times 20 = 1$ d'où $9 \times 9 \equiv 1 \mod 20$ et $\overline{9}\,\overline{9} = \overline{1}$. Ainsi $(\overline{9})^{-1} = \overline{9}$.

De même, puisque $7 \times 3 \equiv 1 \mod 20$ (en effet $7 \times 3 - 1 \times 20 = 1$), nous avons $\overline{7}\,\overline{3} = \overline{1}$; par suite $\overline{7}$ et $\overline{3}$ sont inverses l'un de l'autre. Il en résulte que $-\overline{7}$ et $-\overline{3}$ sont aussi inverses l'un de l'autre.

Remarque 2. Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ nous avons :

$$a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \iff a \text{ est un générateur du groupe additif } \mathbb{Z}/n\mathbb{Z}.$$

En effet, nous avons le :

Lemme 1.1

Soit C_n un groupe cyclique à n élément. Soit a un générateur de C_n. Pour tout $q \in \mathbb{Z}$ l'ordre de a^q est $\frac{n}{\mathrm{pgcd}(n,q)}$.

Démonstration. Soit $q \in \mathbb{Z}$. Pour tout entier $k \in \mathbb{Z}$ nous avons les équivalences :

$$\begin{aligned}
\left(a^q\right)^k = 1 &\iff a^{kq} = 1 \\
&\iff kq \text{ est multiple de } n \text{ car } a \text{ est d'ordre } n \\
&\iff kq \text{ est multiple de } \mathrm{ppcm}(n,q) \\
&\iff kq \text{ est multiple de } \frac{nq}{\mathrm{pgcd}(n,q)} \\
&\iff k \text{ est multiple de } \frac{n}{\mathrm{pgcd}(n,q)}
\end{aligned}$$

□

Nous en déduisons le :

Lemme 1.2

Soit C_n un groupe cyclique à n éléments. Soit a un générateur de C_n. Alors a^q engendre C_n si et seulement si q et n sont premiers entre eux.

Démonstration. Les générateurs de C_n sont d'ordre n. D'après le Lemme 1.1 l'ordre de a^q est égal à n si et seulement si $\mathrm{pgcd}(n,q) = 1$. □

Finalement, le Lemme 1.2 assure donc que $\overline{k}$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier à n.

1.4.2 Le théorème des restes chinois

Proposition 1.10

Soit G un groupe. Pour tout $a \in \mathrm{G}$ il existe un unique morphisme $f\colon \mathbb{Z} \to \mathrm{G}$ tel que $f(1) = a$; il est défini par : $\forall\, k \in \mathbb{Z}, \quad f(k) = a^k$.

Exemple 10. L'application $f\colon \mathbb{Z} \to \mathbb{R}^*$ définie par $f(k) = 2^k$ est un morphisme de groupes.

Démonstration. Soit $a \in \mathrm{G}$. Soit $f\colon \mathbb{Z} \to \mathrm{G}$ l'application définie en posant $f(k) = a^k$ quel que soit $k \in \mathbb{Z}$. Alors pour tous k, $\ell \in \mathbb{Z}$, nous avons

$$f(k+\ell) = a^{k+\ell} = a^k a^\ell = f(k)f(\ell).$$

Ainsi f est un morphisme tel que $f(1) = a$. Si $g\colon \mathbb{Z} \to \mathrm{G}$ est un morphisme tel que $g(1) = a$, alors pour tout $k \in \mathbb{N}$, nous avons

$$g(k) = g(\underbrace{1+1+\ldots+1}_{k \text{ fois}}) = \underbrace{g(1)g(1)\ldots g(1)}_{k \text{ fois}} = \underbrace{a\,a\,\ldots\,a}_{k \text{ fois}} = a^k.$$

Alors $g(-k) = \big(g(k)\big)^{-1} = \big(a^k\big)^{-1} = a^{-k}$ d'où $g(k) = a^k$ quel que soit $k \in \mathbb{Z}$. □

Notons $p\colon \mathbb{Z} \to {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ la projection canonique ; pour tout $k \in \mathbb{Z}$, nous avons $p(k) = \overline{k}$. Supposons que $f\colon {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to \mathrm{G}$ soit un morphisme de groupes. Alors

$$f \circ p\colon \mathbb{Z} \to {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to \mathrm{G}$$

est un morphisme ; si nous posons $a = f \circ p(1) = f(\overline{1})$ nous avons d'après la Proposition 1.10

$$\forall \overline{k} \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, \quad f(\overline{k}) = f \circ p(k) = a^k.$$

Puisque $\overline{n} = \overline{0}$ dans ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, nous en déduisons que $f(\overline{n}) = f(\overline{0})$, *i.e.* $a^n = a^0 = 1$.

Ainsi si $f\colon {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to \mathrm{G}$ est un morphisme de groupes, l'élément $a = f(\overline{1})$ doit satisfaire la condition $a^n = 1$, autrement dit l'ordre de a doit être un diviseur de n.

Nous allons voir que cette condition est suffisante pour définir un tel morphisme f.

Proposition 1.11

Soit G un groupe. Soit $a \in \mathrm{G}$ tel que $a^n = 1$. Il existe un unique morphisme $f\colon {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to \mathrm{G}$ tel que $f(\overline{1}) = a$; il est défini par

$$\forall\, \overline{k} \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, \quad f(\overline{k}) = a^k.$$

Démonstration. La Proposition 1.10 assure l'existence d'un morphisme $g\colon \mathbb{Z} \to \mathrm{G}$ tel que $g(1) = a$. Nous avons $g(n) = a^n = 1$ d'où $n \in \ker g$. Comme $\ker g$ est un sous-groupe de $\mathbb{Z}$, nous avons l'inclusion $n\mathbb{Z} \subset \ker g$. Le théorème de passage au quotient assure que le morphisme g définit un morphisme

$f = \overline{g}\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}$ tel que $f \circ p = g$ où $p\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la projection canonique. Nous avons $f(\overline{1}) = f \circ p(1) = g(1) = a$; ainsi pour tout $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ nous avons $f(\overline{k}) = f \circ p(k) = g(k) = a^k$. Supposons que $h\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}$ est un (autre) morphisme tel que $h(\overline{1}) = a$. Alors $h \circ p(1) = a = f \circ p(1)$ donc $h \circ p = f \circ p$. Puisque p est surjective, nous obtenons $h = f$. □

Soient p et q des entiers au moins égaux à 2. Puisque pq est multiple de p la Proposition 1.11 assure l'existence d'un morphisme de groupes surjectif

$$r_p\colon \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \qquad \overline{x}_{[pq]} \mapsto \overline{x}_{[p]}.$$

Pour tous entiers x et y, nous avons, par définition des anneaux quotients, $\overline{x}_{[pq]}\overline{y}_{[pq]} = \overline{xy}_{[pq]}$ et $\overline{x}_{[p]}\overline{y}_{[p]} = \overline{xy}_{[p]}$ d'où

$$r_p(\overline{x}_{[p]}\overline{y}_{[p]}) = \overline{xy}_{[p]} = r_p(\overline{x}_{[p]})r_p(\overline{y}_{[p]}).$$

Ainsi r_p est un morphisme d'anneaux.

Théorème 1.3

Soient p et q des entiers au moins égaux à 2.
Si p et q sont premiers entre eux, l'application $f\colon \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ définie par

$$\forall\, k \in \mathbb{Z}, \quad f(\overline{k}_{[pq]}) = (\overline{k}_{[p]}, \overline{k}_{[q]}) = \Big(r_p(\overline{k}_{[pq]}), r_p(\overline{k}_{[pq]})\Big)$$

est un isomorphisme d'anneaux.

Démonstration. Les applications $r_p\colon \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ et $r_q\colon \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ étant des morphismes d'anneaux, f est un morphisme d'anneaux (la somme et le produit dans un anneau se font composante par composante).

Déterminons le noyau de f. Pour tout élément $x = \overline{k}_{[pq]}$ appartenant à $\mathbb{Z}/pq\mathbb{Z}$ nous avons

$$\begin{aligned}
f(x) = 0 &\iff \overline{k}_{[p]} = \overline{0}_{[p]} \text{ et } \overline{k}_{[q]} = \overline{0}_{[q]} \\
&\iff k \text{ est multiple de } p \text{ et } q \\
&\iff k \text{ est multiple de } \mathrm{ppcm}(p, q) = pq \\
&\iff \overline{k}_{[pq]} = \overline{0}_{[pq]} \\
&\iff x = 0.
\end{aligned}$$

Ainsi f est injectif. Les ensembles de départ et d'arrivée de f comptent tous deux pq éléments, l'application f est donc bijective. □

Corollaire 1.2

Soient C_p un groupe cyclique à p éléments et C_q un groupe cyclique à q éléments. Le groupe $\mathrm{C}_p \times \mathrm{C}_q$ est cyclique si et seulement si p et q sont premiers entre eux.

Démonstration. Puisque tout groupe cyclique à n éléments est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ nous pouvons supposer que $\mathrm{C}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{C}_q = \mathbb{Z}/q\mathbb{Z}$. Supposons p et q premiers entre eux. D'après le théorème des restes chinois le groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$; en particulier $\mathrm{C}_p \times \mathrm{C}_q$ est cyclique.

Réciproquement supposons que p et q ne soient pas premiers entre eux. Leur ppcm δ est donc strictement inférieur à pq. Pour tout $(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ nous avons

$$\delta(x, y) = (\delta x, \delta y) = (0, 0)$$

car δ est multiple de p et de q. Ainsi, tout élément du groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est d'ordre un diviseur de δ. Par suite le groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ne contient pas d'élément d'ordre pq ; en particulier ce groupe n'est pas cyclique. □

Dans le théorème pour expliciter l'isomorphisme réciproque nous devons, pour tout couple $(\overline{a}_{[p]}, \overline{b}_{[q]}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ trouver un entier $x \in \mathbb{Z}$ tel que $f(\overline{x}_{[pq]}) = (\overline{a}_{(p]}, \overline{b}_{[q]})$, c'est-à-dire

$$x \equiv a \bmod p \text{ et } x \equiv b \bmod q$$

Système d'équations ($x \equiv a$ mod n, $x \equiv b$ mod p)
Soient n et p des entiers premiers entre eux.
Nous cherchons les entiers $x \in \mathbb{Z}$ qui sont congrus à a modulo n et à b modulo p.

◇ *Calcul d'une solution.*
Nous écrivons une relation de Bezout entre n et p :

$$nu + pv = 1 \text{ avec } u, v \in \mathbb{Z}.$$

Posons $\alpha = pv$ et $\beta = nu$. Nous avons alors

$$\alpha \equiv \begin{cases} 1 \bmod n \\ 0 \bmod p \end{cases} \qquad \beta \equiv \begin{cases} 0 \bmod n \\ 1 \bmod p \end{cases}$$

Nous en déduisons que

$$\alpha a \equiv \begin{cases} a \bmod n \\ 0 \bmod p \end{cases} \qquad \beta b \equiv \begin{cases} 0 \bmod n \\ b \bmod p \end{cases}$$

Ainsi l'entier $x_0 = \alpha a + \beta p$ est une solution du système d'équations.

◇ *Calcul de toutes les solutions.*
Pour tout entier $x \in \mathbb{Z}$ nous avons les équivalences

$$\begin{cases} x \equiv a \bmod n \\ x \equiv b \bmod p \end{cases} \iff x \equiv x_0 \bmod n \text{ et } x \equiv x_0 \bmod p$$
$$\iff x - x_0 \text{ est multiple de } n \text{ et de } p$$
$$\iff x - x_0 \text{ est multiple de } np$$

car n et p étant premiers entre eux, nous avons $\mathrm{ppcm}(n, p) = np$. Les solutions sont donc les entiers x de la forme $x_0 + knp$ avec $k \in \mathbb{Z}$.

Exemple 11. Trouver les entiers x tels que

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 2 \bmod 21 \end{cases}$$

- ◇ *Calcul d'une solution.*
  Nous avons la relation de Bezout $8 \times 8 - 21 \times 3 = 1$ et les congruences

$$-63 \equiv \begin{cases} 1 \bmod 8 \\ 0 \bmod 21 \end{cases} \qquad \text{et} \qquad 64 \equiv \begin{cases} 0 \bmod 8 \\ 1 \bmod 21 \end{cases}$$

  L'entier $x_0 = -63 \times 3 + 64 \times 2 = -61$ est donc solution.
- ◇ *Calcul de toutes les solutions.*
  Pour qu'un entier x soit solution il faut et il suffit que x soit congru à -61 modulo 8 et modulo 21, c'est-à-dire que $x + 61$ soit multiple de 8 et de 21. Puisque $\operatorname{ppcm}(8, 21) = 8 \times 21 = 168$, les solutions sont les entiers de la forme $-61 + 168k$ avec $k \in \mathbb{Z}$.

Exemple 12. L'isomorphisme d'anneaux $f\colon \mathbb{Z}/77\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ du théorème chinois est défini par $f(\overline{k}_{[77]}) = (\overline{k}_{[7]}, \overline{k}_{[11]})$. Cherchons l'isomorphisme réciproque. Nous avons la relation de Bezout $2 \times 11 - 3 \times 7 = 1$, d'où

$$22 = 2 \times 11 \equiv \begin{cases} 1 \bmod 7 \\ 0 \bmod 11 \end{cases} \qquad \text{et} \qquad -21 = -3 \times 7 \equiv \begin{cases} 0 \bmod 7 \\ 1 \bmod 11 \end{cases}$$

Pour tous entiers x et y il vient $f(\overline{22x - 21y}_{[77]}) = (\overline{x}_{[7]}, \overline{y}_{[11]})$ donc

$$f^{-1}(\overline{x}_{[7]}, \overline{y}_{[11]}) = \overline{22x - 21y}_{[77]}.$$

Corollaire 1.3

Soient p et q des entiers premiers entre eux. L'isomorphisme des restes chinois définit un isomorphisme entre les groupes $\left(\mathbb{Z}/pq\mathbb{Z}\right)^*$ et $\left(\mathbb{Z}/p\mathbb{Z}\right)^* \times \left(\mathbb{Z}/q\mathbb{Z}\right)^*$

$$\left(\mathbb{Z}/pq\mathbb{Z}\right)^* \xrightarrow{\simeq} \left(\mathbb{Z}/p\mathbb{Z}\right)^* \times \left(\mathbb{Z}/q\mathbb{Z}\right)^*$$

Démonstration. La Proposition 1.5 assure que l'isomorphisme d'anneaux

$$f\colon \mathbb{Z}/pq\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

définit un morphisme de groupes

$$f^*\colon \left(\mathbb{Z}/pq\mathbb{Z}\right)^* \xrightarrow{\simeq} \left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right)^*$$

L'isomorphisme réciproque f^{-1} définit évidemment la bijection réciproque de f^* ; ainsi f^* est un isomorphisme de groupes. Or d'après la Proposition 1.3 nous avons $\left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right)^* = \left(\mathbb{Z}/p\mathbb{Z}\right)^* \times \left(\mathbb{Z}/q\mathbb{Z}\right)^*$ d'où le résultat. □

1.4.3 La fonction d'Euler

Nous nous proposons de répondre à la question suivante : combien l'anneau $\mathbb{Z}/n\mathbb{Z}$ compte-t-il d'éléments inversibles ? Autrement dit combien y a-t-il d'entiers k compris entre 1 et n premiers à n ?

Définition 1.7

Soit n un entier au moins égal à 2. Nous notons $\varphi(n)$ le nombre d'entiers k premiers à n et tels que $1 \leq k \leq n$. La fonction φ s'appelle la *fonction d'Euler*.

Proposition 1.12

- ◇ Le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ possède $\varphi(n)$ éléments.
- ◇ Pour tout entier a premier à n, nous avons $a^{\varphi(n)} \equiv 1 \bmod n$.
- ◇ Tout groupe cyclique à n éléments possède $\varphi(n)$ générateurs.

Démonstration.
- ◇ Le premier point découle de la Proposition 1.9.
- ◇ Le deuxième point vient du résultat général suivant [1] : dans un groupe G à N éléments nous avons $x^N = 1$ pour tout $x \in \mathrm{G}$. Ainsi pour tout entier a premier à n, la classe $\overline{a}$ de a modulo n est un élément du groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, d'où $\overline{a}^{\varphi(n)} \equiv 1 \bmod n$.
- ◇ Le troisième point découle de la Remarque 2.

□

Exemples 4. Nous avons bien sûr $\varphi(1) = 1$ mais aussi

$$\varphi(5) = \#\{1, 2, 3, 4\} = 4, \qquad \varphi(9) = \#\{1, 2, 4, 5, 7, 8\} = 6, \qquad \varphi(10) = \#\{1, 3, 7, 9\} = 4.$$

L'énoncé suivant donne un moyen de calculer $\varphi(n)$.

Proposition 1.13

- ◇ Si p est un nombre premier, alors
  - $\varphi(p) = p - 1$,
  - pour tout entier $r \geq 2$, $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.
- ◇ Si n et m sont des entiers positifs premiers entre eux, alors

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Démonstration.
- ◇ Soit p un nombre premier. Tout entier k compris entre 1 et $p-1$ est premier à p, d'où la première égalité.
  Soit r un entier au moins égal à 2. Les entiers premiers à p^r sont ceux qui ne sont pas multiples de p. Comptons donc les multiples de p compris entre 1 et p^r : ce sont les entiers kp, où

1. Cette propriété est un corollaire du théorème de Lagrange qui assure que si G est un groupe fini et si H est un sous-groupe de G, alors le cardinal de H divise le cardinal de G et $[\mathrm{G} : \mathrm{H}] = \frac{\mathrm{Card(G)}}{\mathrm{Card(H)}}$.

$1 \leq k \leq p^{r-1}$; ainsi il y a p^{r-1} multiples de p entre 1 et p^r. Nous en déduisons qu'il y a $p^r - p^{r-1}$ entiers non multiples de p compris entre 1 et p^r.

◇ Soient m et n des entiers premiers entre eux. L'isomorphisme d'anneaux

$$f\colon \mathbb{Z}/nm\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

des restes chinois définit un isomorphisme de groupes

$$f^*\colon \left(\mathbb{Z}/nm\mathbb{Z}\right)^* \xrightarrow{\simeq} \left(\mathbb{Z}/n\mathbb{Z}\right)^* \times \left(\mathbb{Z}/m\mathbb{Z}\right)^*$$

Par conséquent les groupes $\left(\mathbb{Z}/nm\mathbb{Z}\right)^*$ et $\left(\mathbb{Z}/n\mathbb{Z}\right)^* \times \left(\mathbb{Z}/m\mathbb{Z}\right)^*$ ont le même nombre d'éléments. Finalement à partir de

$$\text{Card}\left(\mathbb{Z}/nm\mathbb{Z}\right)^* = \varphi(nm), \qquad \text{Card}\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \varphi(n), \qquad \text{Card}\left(\mathbb{Z}/m\mathbb{Z}\right)^* = \varphi(m),$$

nous obtenons $\varphi(nm) = \varphi(n)\varphi(m)$.

□

Calcul de $\varphi(n)$

Pour calculer $\varphi(n)$ nous décomposons n en facteurs premiers

$$n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

où les p_i sont des nombres premiers deux à deux distincts et où $n_i \geq 1$. Puisque chaque facteur $p_i^{n_i}$ est premier avec le produit des autres facteurs nous avons l'égalité

$$\varphi(p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}) = \varphi(p_1^{n_1})\varphi(p_2^{n_2}) \dots \varphi(p_k^{n_k}).$$

Exemples 5. ◇ Nous avons : $\varphi(63) = \varphi(3^2 \times 7) = \varphi(3^2)\varphi(7) = (3^3 - 3)(7 - 1) = 36$.

◇ Pour tout entier $r \geq 1$, nous avons $\varphi(2^r) = 2^{r-1}$.

1.5 Le corps $\mathbb{F}_p$

Soit p un nombre premier. L'anneau $\mathbb{Z}/p\mathbb{Z}$ compte p éléments et $\varphi(p) = p - 1$ inversibles. Puisque 0 n'est pas inversible, nous avons nécessairement $\left(\mathbb{Z}/p\mathbb{Z}\right)^* = \left(\mathbb{Z}/p\mathbb{Z}\right) \smallsetminus \{0\}$. Ainsi, tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible, autrement dit l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Proposition 1.14

Soit n un entier au moins égal à 2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Démonstration. Nous avons vu que si n est un nombre premier, alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Réciproquement, supposons que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont donc inversibles. Soit d un diviseur de n tel que $1 \leq d < n$. Il existe un entier $q \geq 1$ tel que $dq = n$; par

suite nous avons $\overline{d}\,\overline{q} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$. L'entier d n'étant pas multiple de n, sa classe $\overline{d}$ modulo n n'est pas nulle. Comme $\mathbb{Z}/n\mathbb{Z}$ est un corps, nous en déduisons que $\overline{q} = \overline{0}$. Ainsi q est multiple de n. Étant donné que $1 \leq q \leq n$, nous obtenons $q = n$ d'où $d = 1$. Cela montre que les seuls diviseurs positifs de n sont 1 et n. □

Notation. Pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ se note $\mathbb{F}_p$.

Exemples 6. Nous avons :

$$\mathbb{F}_2 = \{\overline{0}, \overline{1}\}, \qquad \mathbb{F}_3 = \{\overline{0}, \overline{1}, -\overline{1}\}, \qquad \mathbb{F}_5 = \{\overline{0}, \pm\overline{1}, \pm\overline{2}\}.$$

Rappelons l'énoncé suivant :

Théorème 1.4: (Théorème de Fermat)

Soit p un nombre premier. Pour tout entier $a \in \mathbb{Z}$, nous avons $a^p \equiv a \bmod p$.

Pour le démontrer nous avons besoin de la :

Proposition 1.15

Soit p un nombre premier.
Pour tout entier k tel que $0 < k < p$, nous avons $\binom{p}{k} \equiv 0 \bmod p$.

Démonstration du Théorème 1.4. Commençons par le cas $a \geq 0$ et raisonnons par récurrence.

Si $a = 0$, alors la formule est vraie.

Supposons que a soit un entier positif tel que $a^p \equiv a \bmod p$. La formule du binôme assure que

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{k}a^{p-k} + \ldots + \binom{p}{p-1}a + 1.$$

La Proposition 1.15 assure que les coefficients $\binom{p}{1}$, $\binom{p}{2}$, …, $\binom{p}{p-1}$ sont tous congrus à 0 modulo p ; par suite

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

En utilisant l'hypothèse de récurrence, nous en déduisons que $(a+1)^p \equiv a + 1 \bmod p$. La formule est donc vraie quel que soit l'entier $a \geq 0$.

Supposons que a soit un entier négatif tel que $a^p \equiv a \bmod p$. D'après ce qui précède nous avons

$$(-1)^p a^p = (-a)^p \equiv -a \bmod p.$$

Si $p > 2$, alors p est impair donc $(-1)^p = -1$ et par conséquent $a^p \equiv a \bmod p$. Si $p = 2$, alors $(-1)^2 a^2 \equiv a^2 \bmod 2$ et $-1 \equiv 1 \bmod 2$. Il en résulte que $-a \equiv a \bmod 2$, d'où $a^2 \equiv a \bmod 2$. □

Corollaire 1.4

Pour tout élément $x = \overline{a} \in \mathbb{F}_p$ nous avons $x^p = x$.

Proposition 1.16

Dans $\mathbb{F}_p$ les propriétés suivantes sont satisfaites :
- ◇ pour tout $x \in \mathbb{F}_p$ nous avons $px = 0$;
- ◇ pour tout $x \in \mathbb{F}_p$ nous avons $x^p = x$ et pour tout $x \in \mathbb{F}_p \smallsetminus \{0\}$ nous avons $x^{p-1} = 1$.

Il est difficile de décider si un grand entier n est premier (tester directement si n a un diviseur premier inférieur à n n'est bien sûr pas raisonnable). Nous pouvons penser à utiliser la propriété de Fermat :

si n est premier, alors pour tout entier a premier à n, nous avons $a^{n-1} \equiv 1 \bmod n$.

Mais cette condition nécessaire n'est pas suffisante : prenons en effet le nombre $n = 561 = 3 \times 11 \times 17$. Pour tout entier a premier à n, a est premier à 3, 11 et 17 ; par suite

$$a^2 \equiv 1 \bmod 3, \qquad a^{10} \equiv 1 \bmod 11, \qquad a^{16} \equiv 1 \bmod 17.$$

Puisque $\operatorname{ppcm}(2, 10, 16) = 80$ nous en déduisons que a^{80} est congru à 1 modulo 3, modulo 11 et modulo 17. Il en résulte que $a^{80} - 1$ est multiple de $\operatorname{ppcm}(3, 11, 17) = n$; autrement dit $a^{80} \equiv 1 \bmod n$.

Comme $n - 1 = 560 = 80 \times 7$ est multiple de 80, nous avons $a^{n-1} \equiv 1 \bmod n$. L'entier n passe donc avec succès le test ci-dessus mais il n'est pas premier [2].

2 Polynômes

Dans ce paragraphe nous expliquons les propriétés générales des anneaux de polynômes (à une indéterminée). Puis nous montrons que les polynômes à coefficients dans un corps ont toutes les propriétés arithmétiques des entiers : existence d'une division euclidienne, du pgcd et d'une décomposition en « facteurs premiers ».

2.1 Polynômes à coefficients dans un anneau

Soit A un anneau.

Un *polynôme* à coefficients dans A est une expression

$$a_0 + a_1 X + \ldots + a_n X^n$$

où $n \in \mathbb{N}$ et les a_i sont des éléments de A.

Nous notons $A[X]$ l'ensemble des polynômes à coefficients dans A. Nous ajoutons et nous multiplions les polynômes comme d'habitude : cela fait de $A[X]$ un anneau.
- ◇ Le polynôme dont tous les coefficients sont nuls s'appelle le *polynôme nul* et se note 0.
- ◇ Si $P = a_0 + a_1 X + \ldots + a_n X^n \in A[X]$ n'est pas nul, le plus grand entier n tel que $a_n \neq 0$ s'appelle le *degré* de P et se note $\deg P$ (par convention le degré du polynôme nul est $-\infty$).
- ◇ Un polynôme est *unitaire* si son monôme non nul de plus grand degré a pour coefficient 1.

2. Un tel entier n est appelé un nombre de Carmichaël

◇ Les éléments de A s'identifient aux polynômes constants : A est un sous-anneau de $A[X]$.

Proposition 2.1: (Propriété caractéristique d'un anneau de polynômes)

Soit $f\colon A \to B$ un morphisme d'anneaux. Soit b un élément de B. Il existe un unique morphisme d'anneaux $F\colon A[X] \to B$ tel que $F(X) = b$ et $\forall\, a \in A$, $F(a) = f(a)$.

Démonstration. Puisqu'on veut que F soit un morphisme d'anneaux nous devons poser, pour tout polynôme $\sum_{k=0}^{n} a_k X^k \in A[X]$:

$$F\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} F(a_k)F(X)^k = \sum_{k=0}^{n} f(a_k)b^k.$$

Nous vérifions que l'application F ainsi définie est un morphisme d'anneaux. □

Changement d'anneaux

Soit $f\colon A \to B$ un morphisme d'anneaux. Puisque B est un sous-anneau de $B[X]$, considérons f comme un morphisme (encore noté f) $A \to B[X]$: pour tout $a \in A$, $f(a)$ est le polynôme constant $f(a) \in B$.

D'après la propriété précédente il existe un unique morphisme d'anneaux $F\colon A[X] \to B$ tel que $F(X) = X$ et $F(a) = f(a)$ pour tout $a \in A$. Pour tout polynôme $\sum_{i=0}^{n} a_i X^i \in A[X]$ nous avons

$$F\Big(\sum_{i=0}^{n} a_i X^i\Big) = \sum_{i=0}^{n} f(a_i)X^i.$$

Réduction modulo p

Soit p un nombre premier. Considérons le morphisme canonique $f\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ pour faire un changement d'anneau. Nous obtenons le morphisme d'anneaux $F\colon \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$, appelé *réduction modulo p* et défini par

$$F\Big(\sum_{i=0} a_i X^i\Big) = \sum_{i=0} \overline{a_i} X^i \in \mathbb{Z}/p\mathbb{Z}[X]$$

où pour tout $a \in \mathbb{Z}$, $\overline{a}$ désigne la classe de a dans $\mathbb{Z}/p\mathbb{Z}$.

Fonction polynôme

Soient A un anneau et $P \in A[X]$. Pour tout $a \in A$, l'élément $P(a) \in A$ s'appelle la *valeur* de P en a. L'application $A \to A$ qui à tout $x \in A$ associe $P(x)$ s'appelle la fonction polynôme associée à P.

Un élément $a \in A$ tel que $P(a) = 0$ s'appelle une *racine* de P.

Nous avons le résultat immédiat suivant :

Proposition 2.2

Soit $a \in A$. L'application $A[X] \to A$ qui, à tout polynôme $P \in A[X]$, associe $P(a)$ est un morphisme d'anneaux.

2.1.1 Anneau intègre

Définition 2.1

Soit A un anneau. On dit que A est *intègre* si pour tous x, $y \in A$, nous avons l'implication :

$$xy = 0 \Rightarrow (x = 0 \text{ ou } y = 0).$$

Exemples 7.
- ◇ L'anneau $\mathbb{Z}$ est intègre mais $\mathbb{Z}/15\mathbb{Z}$ n'est pas intègre car dans cet annneau nous avons $\overline{3} \neq 0$, $\overline{5} \neq 0$ et $\overline{3} \cdot \overline{5} = 0$.
- ◇ Tout corps est un anneau intègre.
- ◇ Tout sous-anneau d'un anneau intègre est intègre.

Proposition 2.3

Soit A un anneau intègre. Soient a et b deux éléments de A. Alors $aA = bA$ si et seulement s'il existe un élément inversible $u \in A^*$ tel que $b = au$.

Démonstration. Supposons qu'il existe un élément inversible $u \in A^*$ tel que $b = au$. Puisque $b = au$, nous avons l'inclusion $bA \subset aA$. Comme u est inversible, nous avons $a = bu^{-1}$ d'où $aA \subset bA$. Finalement $aA = bA$.

Réciproquement supposons que $aA = bA$. Il existe u, $v \in A$ tels que $b = ua$ et $a = vb$. Si a ou b est nul, alors $a = b = 0$ et $b = a \times 1$. Si $a \neq 0$ et $b \neq 0$, alors $b = uvb$, c'est-à-dire $b(1 - uv) = 0$. Puisque A est intègre nous en déduisons que $1 = uv$ donc u et v sont inversibles. □

Proposition 2.4

Soit A un anneau intègre.
- ◇ L'anneau $A[X]$ est intègre.
- ◇ Pour tous polynômes non nuls P, $Q \in A[X]$ nous avons l'égalité $\deg(PQ) = \deg P + \deg Q$.

Démonstration. Soient P et Q des polynômes non nuls à coefficients dans A. Soit $a_n X^n$ le monôme de plus grand degré de P ; soit $a_p X^p$ le monôme de plus grand degré de Q. Puisque $a_n \neq 0$ et $b_p \neq 0$ nous avons $a_n b_p \neq 0$. Ainsi le monôme de plus grand degré de PQ est $a_n b_p X^{n+p}$. Il en résulte que $PQ \neq 0$ et $\deg(PQ) = n + p = \deg P + \deg Q$. □

Dans la suite nous considèrerons uniquement des polynômes sur un anneau intègre.

2.1.2 Division euclidienne

Proposition-Définition 2.1

Soit A un anneau intègre. Soit $B \in A[X]$ un polynôme dont le coefficient dominant est inversible dans A (donc $B \neq 0$).
Pour tout polynôme $U \in A[X]$ il existe un unique polynôme $Q \in A[X]$ et un unique polynôme $R \in A[X]$ tel que

$$U = BQ + R \text{ et } (R = 0 \text{ ou } \deg R < \deg B).$$

Le polynôme Q s'appelle le *quotient* et R s'appelle le *reste* de la division de U par B.

Remarques 1.
- ◇ Le reste de la division de U par B est nul si et seulement si U est multiple de B.
- ◇ Nous pouvons toujours faire la division euclidienne par un polynôme unitaire.
- ◇ Si $\Bbbk$ est un corps et si $B \in \Bbbk[X]$ est non nul, nous pouvons toujours faire la division euclidienne par B dans $\Bbbk[X]$.

Démonstration. Posons $B = b_n X^n + b_{n-1}X^{n-1} + \ldots + b_0$, où $b_n \in A^*$, ainsi $\deg B = n$. Soit $U \in A[X]$.
Si $U = 0$ ou si $\deg U < n$, nous prenons $Q = 0$ et $R = U$.

Supposons $U \neq 0$ et $\deg U > n$. Raisonnons par récurrence sur $p = \deg U$. Posons $U = \sum_{k=0}^{p} u_k X^k$.
Le monôme de degré p dans $V = u_p(b_n^{-1})X^{p-n}B$ est

$$u_p(b_n^{-1})X^{p-n}b_n X^n = u_p X^p$$

Dans la différence $U - V$ ce monôme disparait ; le polynôme $U - V$ est donc de degré strictement inférieur à p. Par hypothèse de récurrence il existe Q_1 et R dans $A[X]$ tels que $U - V = BQ_1 + R$, $R = 0$, ou $\deg R < n$. Il vient $U = B(u_p(b_n^{-1})X^{n-p} + Q_1) + R$ ce qui assure l'existence des polynômes Q et R de l'énoncé.

Montrons l'unicité de Q et R. Raisonnons par l'absurde : supposons que $U = BQ + R = BQ_1 + R_1$ avec $R_1 = 0$ ou $\deg R_1 < \deg B$. Alors, en soustrayant, nous avons $B(Q - Q_1) = R_1 - R$. Si $Q \neq Q_1$, nous avons $Q - Q_1 \neq 0$ d'où

$$\deg(R - R_1) = \deg(B(Q - Q_1)) = n + \deg(Q - Q_1) \geq n.$$

Mais R et R_1 sont nuls ou de degré strictement inférieurs à n : si $R - R_1$ n'était pas nul, il serait de degré strictement inférieur à n, ce qui n'est pas vrai. Nous avons donc $R = R_1$ et puisque $B \neq 0$, il vient $Q - Q_1 = 0$. Ainsi Q et R sont uniques. □

Corollaire 2.1

Soit A un anneau intègre. Soit $a \in A$. Pour tout polynôme $U \in A[X]$ il existe un unique polynôme $Q \in A[X]$ tel que $U = (X - a)X + U(a)$.

Démonstration. Soient Q et R le quotient et le reste de la division de U par le polynôme unitaire $X - a$. Nous avons $U = (X - a)Q + R$; par suite $U(a) = 0\,Q(a) + R(a) = R(a)$. Le polynôme R étant nul ou de degré 0 il est constant donc $R = R(a) = U(a)$. □

Corollaire 2.2

Soit $U \in A[X]$. Un élément $a \in A$ est une racine de U si et seulement si U est multiple de $X - a$.

Proposition 2.5

Soient A un anneau intègre et $P \in A[X]$ un polynôme non nul. Le nombre de racines de P est au plus égal au degré de P.

Démonstration. Nous raisonnons par récurrence sur le degré de P.

- ◇ Si P n'a pas de racine, le résultat est vrai.
- ◇ Supposons que P a (au moins) une racine $a \in A$. Il existe $Q \in A[X]$ tel que $P = (X - a)Q$. Un élément $x \in A$ est donc racine de P si et seulement si $x = a$ ou si x est racine de Q. Puisque $P \neq 0$, nous avons $Q \neq 0$. Par hypothèse de récurrence Q compte au plus $\deg Q$ racines. Par conséquent P compte au plus $1 + \deg Q = \deg P$ racines.

□

Exemple 13. Montrons que l'anneau quotient $\mathbb{Z}[X]/(X^2+1)\mathbb{Z}[X]$ est isomorphe à l'anneau des entiers de Gauss $\mathbb{Z}[\mathbf{i}]$.

Soit $f\colon \mathbb{Z}[X] \to \mathbb{Z}[\mathbf{i}]$ le morphisme d'anneaux tel que $f(X) = \mathbf{i}$. Pour tout polynôme $P \in \mathbb{Z}[X]$ nous avons $f(P) = P(\mathbf{i})$.

- ◇ Soit $P \in \ker f$. Dans $\mathbb{Z}[X]$ la division de P par $X^2 + 1$ s'écrit $P = (X^2 + 1)Q + R$, où Q, R désignent deux éléments de $\mathbb{Z}[X]$ tels que $R = 0$ ou $\deg R \leq 1$. Nous avons
$$0 = P(\mathbf{i}) = (\mathbf{i}^2 + 1)Q(\mathbf{i}) + R(\mathbf{i}) = R(\mathbf{i}).$$
Posons $R = a + bX$ où a, b désignent deux éléments de $\mathbb{Z}$. Nous obtenons $0 = R(\mathbf{i}) = a + b\mathbf{i}$; par suite $a = b = 0$ et finalement $R = 0$. Ainsi P est multiple de $X^2 + 1$.
Réciproquement, si P est multiple de $X^2 + 1$, alors $P(\mathbf{i}) = 0$ et P appartient à $\ker f$. Le noyau de f est donc l'idéal $(X^2 + 1)\mathbb{Z}[X]$.
- ◇ L'application f est surjective car pour tout $a + b\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$ le polynôme $a + bX$ appartient à $\mathbb{Z}[X]$ et $f(a + bX) = a + b\mathbf{i}$.
Le morphisme f définit donc un isomorphisme d'anneaux
$$\overline{f}\colon \mathbb{Z}[X]/(X^2+1)\mathbb{Z}[X] \xrightarrow{\simeq} \mathbb{Z}[\mathbf{i}]$$
tel que
$$\overline{f}(\overline{P}) = P(\mathbf{i}) \qquad \forall\, P \in \mathbb{Z}[X]$$
où $\overline{P}$ désigne la classe de P dans l'anneau quotient. Nous avons $f^{-1}(a + b\mathbf{i}) = \overline{a + bX}$ pour tous a, $b \in \mathbb{Z}$.

2.2 Anneau $\mathbb{k}[X]$

Dans ce paragraphe $\mathbb{k}$ est un corps.

2.2.1 Idéal de $\mathbb{k}[X]$

Soit $\mathcal{I}$ un idéal de l'anneau $\mathbb{k}[X]$.

Si $\mathcal{I} = \{0\}$, alors $\mathcal{I} = 0\,\mathbb{k}[X]$.

Supposons $\mathcal{I} \neq \{0\}$; alors il existe dans $\mathcal{I}$ des polynômes non nuls. Soit D un polynôme de plus petit degré parmi les polynômes non nuls de $\mathcal{I}$.

Soit $P \in \mathcal{I}$. Divisons P par D : il existe $Q \in \mathbb{k}[X]$ et $R \in \mathbb{k}[X]$ tels que $P = DQ + R$, $R = 0$ ou $\deg R < \deg D$. Puisque $\mathcal{I}$ est un idéal et D est un élément de $\mathcal{I}$, nous obtenons : DQ appartient à $\mathcal{I}$. Comme de plus P appartient à $\mathcal{I}$, nous avons : $R = P - DQ$ appartient à $\mathcal{I}$. Le polynôme D étant de plus petit degré parmi les polynômes non nuls de $\mathcal{I}$ nous en déduisons que $R = 0$. Finalement P est multiple de D.

Cela montre que $\mathcal{I}$ est inclus dans l'ensemble des multiples de D. Mais comme D appartient à $\mathcal{I}$, tous les multiples de D appartiennent à $\mathcal{I}$. Finalement $\mathcal{I} = D\mathbb{k}[X]$ est l'idéal engendré par D.

Supposons que Δ soit un (autre) polynôme tel que $\mathcal{I} = \Delta\mathbb{k}[X]$; alors D et Δ sont multiples l'un de l'autre. Il existe donc un élément $a \in \mathbb{k}^*$ tel que $\Delta = aD$.

Nous pouvons donc énoncer le :

Théorème 2.1

Soit $\mathcal{I}$ un idéal de l'anneau $\mathbb{k}[X]$.

- ◇ Il existe un polynôme $D \in \mathbb{k}[X]$ tel que $\mathcal{I} = D\mathbb{k}[X]$, autrement dit $\mathcal{I}$ est l'idéal principal engendré par D.
- ◇ Si D et Δ sont des polynômes qui engendrent $\mathcal{I}$, alors il existe $a \in \mathbb{k}^*$ tel que $D = a\Delta$.

2.2.2 Pgcd

Soient a, $b \in \mathbb{k}[X]$. Posons

$$\mathcal{I} = \{AU + BV \,|\, U, V \in \mathbb{k}[X]\} = A\mathbb{k}[X] + B\mathbb{k}[X].$$

La somme de deux éléments de $\mathcal{I}$ appartient à $\mathcal{I}$, de même que l'opposé de tout élément de $\mathcal{I}$. Puisque 0 appartient à $\mathcal{I}$, $\mathcal{I}$ est un sous-groupe additif de $\mathbb{k}[X]$. De plus, tout multiple d'un élément de $\mathcal{I}$ est dans $\mathcal{I}$; il s'en suit que $\mathcal{I}$ est un idéal de $\mathbb{k}[X]$.

Supposons que A et B soient non tous deux nuls. Alors $\mathcal{I} \neq \{0\}$. Le Théorème 2.1 assure l'existence d'un polynôme $D \neq 0$ tel que $\mathcal{I} = D\mathbb{k}[X]$. Parmi tous les polynômes aD, où $a \in \mathbb{k}^*$ il y en a un et un seul qui est unitaire : nous l'obtenons en multipliant D par l'inverse du coefficient de son monôme de plus grand degré.

Ceci nous conduit à définir la notion suivante.

Définitions 2.1

Soient A, $B \in \mathbb{k}[X]$ des polynômes non tous deux nuls. Le polynôme unitaire $D \in \mathbb{k}[X]$ tel que $A\mathbb{k}[X] + B\mathbb{k}[X] = D\mathbb{k}[X]$ s'appelle le *pcgd* de A et B et se note $\text{pgcd}(A, B)$.
Si $\text{pgcd}(A, B) = 1$, on dit que A et B sont *premiers entre eux*.

Proposition 2.6

Nous avons les propriétés suivantes :
- ◇ $\text{pgcd}(A, B)$ divise A et B ;
- ◇ si $P \in \mathbb{k}[X]$ divise A et B, alors P divise $\text{pgcd}(A, B)$.

Comme dans l'anneau des entiers, nous avons une relation de Bezout et un théorème de Gauss.

Théorème 2.2: (Théorèm de Bezout)

Soient A, $B \in \mathbb{k}[X]$ des polynômes non tous deux nuls.
- ◇ Il existe des polynômes U, $V \in \mathbb{k}[X]$ tels que $AU + BV = \text{pgcd}(A, B)$.
- ◇ Les polynômes A et B sont premiers entre eux si et seulement s'il existe U, $V \in \mathbb{k}[X]$ tels que $AU + BV = 1$ (relation de Bezout).

Démonstration. Comme $\text{pgcd}(A, B)$ appartient à $A\mathbb{k}[X] + B\mathbb{k}[X]$ il existe U, V dans $\mathbb{k}[X]$ tels que $\text{pgcd}(A, B) = AU + BV$. Supposons qu'il existe U et V dans $\mathbb{k}[X]$ tels que $AU + BV = 1$. Alors 1 appartient à l'idéal $A\mathbb{k}[X] + B\mathbb{k}[X] = \text{pgcd}(A, B)\mathbb{k}[X]$; il en résulte que cet idéal est l'anneau $\mathbb{k}[X]$ tout entier. Nous avons $\text{pgcd}(A, B)\mathbb{k}[X] = 1\,\mathbb{k}[X]$ d'où $\text{pgcd}(A, B) = 1$. □

Théorème 2.3: (Théorèm de Gauss)

Soient A, B et $C \in \mathbb{k}[X]$ des polynômes non nuls. Si A divise BC et si A et B sont premiers entre eux, alors A divise C.

Démonstration. Supposons $\text{pgcd}(A, B) = 1$. Alors il existe U, V dans $\mathbb{k}[X]$ tels que $AU + BV = 1$. En multipliant par C, nous obtenons $ACU + BCV = C$. Si A divise BC, alors A divise BCV et comme A divise ACU, nous en déduisons que A divise C. □

2.2.3 Calcul du pgcd

Comme pour l'anneau $\mathbb{Z}$, nous utilisons l'algorithme d'Euclide.
Soient A, B deux éléments de $\mathbb{k}[X]$. Supposons $B \neq 0$.
Effectuons les divisions euclidiennes :

$$
\begin{array}{lll}
A = BQ_1 + R_1, & 0 \leq \deg R_1 < \deg B & \\
A = R_1Q_2 + R_2, & 0 \leq \deg R_2 < \deg R_1 & \\
\vdots, & \vdots & R_{n-2} = R_{n-1}Q_n + R_n, \quad 0 \leq \deg R_n < \deg R_{n-1} \\
R_{n-1} = R_nQ_{n+1} + 0 &
\end{array}
$$

Les restes non nuls successifs ont des degrés qui diminuent strictement, par suite le dernier reste est nul.

Si P et Q sont des polynômes, alors pour simplifier posons

$$\mathcal{I}_{(P,Q)} = P\Bbbk[X] + Q\Bbbk[X].$$

Puisque A appartient à $\mathcal{I}_{(B,R_1)}$ nous avons l'inclusion $\mathcal{I}_{(A,B)} \subset \mathcal{I}_{(B,R_1)}$; de même $R_1 = A - BQ_1$ appartient à $\mathcal{I}_{(A,B)}$ d'où l'inclusion $\mathcal{I}_{(B,R_1)} \subset \mathcal{I}_{(A,B)}$. Finalement $\mathcal{I}_{(B,R_1)} = \mathcal{I}_{(A,B)}$. De proche en proche nous obtenons

$$\mathcal{I}_{(A,B)} = \mathcal{I}_{(B,R_1)} = \ldots = \mathcal{I}_{(R_{n-1},R_n)} = \mathcal{I}_{(R_n,0)} = R_n\Bbbk[X].$$

Ainsi $\operatorname{pgcd}(A,B)\Bbbk[X] = R_n\Bbbk[X]$; en particulier $\operatorname{pgcd}(A,B)$ divise R_n et R_n divise $\operatorname{pgcd}(A,B)$. Par conséquent il existe un élément $\lambda \in \Bbbk \setminus \{0\}$ tel que $\operatorname{pgcd}(A,B) = \lambda R_n$. Il en résulte :

Proposition 2.7

Soient A, B deux éléments de $\Bbbk[X]$. Supposons $B \neq 0$. Alors $\operatorname{pgcd}(A,B)$ s'obtient en divisant le dernier reste non nul par le coefficient de son monôme de plus grand degré.

2.3 Polynômes à coefficients dans $\mathbb{F}_p$

Rappelons que si p est un nombre premier, alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments. Les calculs dans l'anneau de polynômes $\mathbb{F}_p[X]$ présentent quelques particularités.

Proposition 2.8

Soient P et Q dans $\mathbb{F}_p[X]$. Nous avons les égalités

$$(P+Q)^p = P^p + Q^p \qquad \text{et} \qquad (P(X))^p = P(X^p).$$

Démonstration. Rappelons la formule du binôme (valable dans tout anneau commutatif) :

$$(P+Q)^p = \sum_{k=0}^{p} \binom{p}{k} P^k Q^{p-k}. \tag{2.1}$$

Pour tout entier k tel que $0 < k < p$ nous avons $\binom{p}{k} \equiv 0 \bmod p$[3]. Par suite la classe de $\binom{p}{k}$ dans $\mathbb{F}_p$ est égale à 0. Dans le membre de droite de (2.1) il ne reste donc que les premier et dernier termes ; nous obtenons donc $(P+Q)^p = P^p + Q^p$. Écrivons P sous la forme $\sum_{k=0}^{n} a_k X^k$. Élevons à la puissance p cette somme de monômes en appliquant la formule précédente

$$(P(X))^p = \sum_{k=0}^{n} (a_k)^p (X^k)^p = \sum_{k=0}^{n} (a_k)^p X^{k+p} = \sum_{k=0}^{n} a_k X^{k+p} = \sum_{k=0}^{n} (a_k)^p (X^p)^k = P(X^p)$$

(rappelons que pour tout a_k dans $\mathbb{F}_p$ nous avons $a_k^p = a_k$). □

Le polynôme unitaire de degré n est déterminé par n coefficients. Étant donné qu'il y a p éléments dans $\mathbb{F}_p$, il y a p^n polynômes unitaires de degré n dans $\mathbb{F}_p[X]$.

Exemples 8. ◇ Dans $\mathbb{F}_2[X]$ les coefficients possibles sont 0 et 1, par suite

- le seul polynôme de degré 0 est 1,
- les deux polynômes de degré 1 sont X et $X+1$,
- les quatre polynômes de degré 2 sont X^2, $X^2 + X = X(X+1)$, $X^2 + 1 = (X+1)^2$ et $X^2 + X + 1$.

- Dans $\mathbb{F}_5[X]$ nous avons $(X^2 + 3X - 1)^5 = X^{10} + 3X^5 - 1$.

Exemple 14. Soit P un élément de $\mathbb{F}_p[X]$. Pour tout entier $r \geq 1$ nous avons

$$(P(X))^{p^r} = P(X^{p^r}).$$

Il suffit en effet d'itérer l'égalité $(P(X))^p = P(X^p)$ en l'appliquant successivement aux polynômes $P_1(X) = P(X^p)$, $P_2(X) = P_1(X^p) = P(X^{p^2})$, etc.

Remarque 3. Considérons le polynôme $P = X^2 + X \in \mathbb{F}_2[X]$. Pour tout $a \in \mathbb{F}_2$, nous avons $a^2 = a$ donc $P(a) = a^2 + a = a + a = 0$. La fonction polynôme

$$\mathbb{F}_2 \to \mathbb{F}_2, \qquad a \mapsto P(a)$$

est donc nulle, alors que le polynôme P n'est pas nul (il est de degré 2).

Nous ne pouvons donc pas toujours identifier polynôme et fonction polynôme comme on le fait souvent lorsque les coefficients sont dans $\mathbb{R}$ ou dans $\mathbb{C}$: sur un corps fini, comme $\mathbb{F}_p$ par exemple, il faut au contraire bien distinguer le polynôme et la fonction polynôme associée.

Énonçons maintenant une propriété importante de $\mathbb{F}_p[X]$.

Proposition 2.9

Les racines du polynômes $(X^{p-1} - 1) \in \mathbb{F}_p[X]$ sont les éléments de $\mathbb{F}_p^*$ autrement dit

$$X^{p-1} - 1 = \prod_{a \in \mathbb{F}_p^*} (X - a).$$

3. De manière équivalente pour tout entier k tel que $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k}$ est un multiple de p.

En effet, par définition $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ d'où $p! = \binom{p}{k} k!(p-k)!$. Ainsi p divise $\binom{p}{k} k!(p-k)!$. Supposons que $1 \leq k \leq p-1$; alors p ne divise aucun entier compris entre 1 et k. Par suite le corollaire du Théorème de Gauss assure que p ne divise pas $k!$. Les inégalités $1 \leq p-k \leq p-1$ assurent que p ne divise pas non plus $(p-k)!$. D'après le même corollaire nous en déduisons que p ne divise pas $k!(p-k)!$. Il s'en suit que p divise $\binom{p}{k}$.

Démonstration. Pour tout $a \in \mathbb{F}_p^*$ nous avons $a^{p-1} = 1$, par suite a est racine de $X^{p-1}-1$. Ce polynôme étant de degré $p-1$, ses racines sont exactement les $p-1$ éléments de $\mathbb{F}_p^*$. □

Théorème 2.4: (Théorème de Wilson)

Soit $n \geq 2$ un entier. L'entier n est premier si et seulement si $(n-1)! \equiv -1 \bmod n$.

Démonstration. Supposons que n soit premier ; alors les polynômes $P = X^{n-1} - 1$ et $Q = \prod_{a \in \mathbb{F}_n^*} (X - a)$ sont égaux dans $\mathbb{F}_n[X]$. En notant $\overline{k}$ la classe modulo n d'un entier k nous avons

$$Q(0) = \prod_{a \in \mathbb{F}_n^*} (-a) = (-1)^{n-1} \prod_{a \in \mathbb{F}_n^*} a = (-1)^{n-1} \left(\overline{1}\,\overline{2} \ldots \overline{n-1} \right)$$

et $P(0) = -1$. Par conséquent $-1 \equiv (-1)^{n-1}(n-1)! \bmod n$.

Si $n = 2$ alors $(2-1)! = 1 \equiv -1 \bmod 2$.

Si $n \geq 3$, alors n est impair, $(-1)^{n-1} = 1$ et nous avons le résultat.

Réciproquement, raisonnons par l'absurde en supposant que $(n-1)! \equiv -1 \bmod n$ et n non premier. Il existe un entier q tel que q divise n et $1 < q < n$. Alors q divise $(n-1)!$ et comme $1 + (n-1)!$ est par hypothèse multiple de n, q divise $1 + (n-1)!$. Il en résule que q divise $\left(1 + (n-1)!\right) - (n-1)! = 1$: contradiction. □

2.4 Calcul des coefficients binomiaux modulo p

Écriture d'un entier en base b

Soit $b \geq 2$ un entier. Pour tout entier $n > 0$ écrivons les divisions par b en cascade :

$$\begin{array}{ll}
n = q_1 b + a_0 & 0 \leq a_0 < b \text{ et } \ 0 \leq q_1 < n \\
q_1 = q_2 b + a_1 & 0 \leq a_1 < b \text{ et } \ 0 \leq q_2 < q_1 \\
\vdots & \vdots \\
q_{r-1} = q_r b + a_{r-1} & 0 \leq a_{r-1} < b \text{ et } \ 0 \leq q_r < q_{r-1} \\
q_r = 0 b + a_r & 0 \leq a_r < b
\end{array}$$

Comme les quotients $q_1, q_2, \ldots$ sont positifs ou nuls et décroissent strictement il existe un entier $r \geq 0$ tel que $q_{r+1} = 0$. En remontant ces égalités nous obtenons

$$n = a_0 + a_1 b + a_2 b^2 + \ldots + a_r b^r \qquad \text{où } 0 \leq a_i < b \text{ pour tout } i.$$

C'est l'*écriture* de n en base b et les a_i sont les *chiffres* de n.

Si $b = 10$, nous retrouvons l'écriture décimale habituelle où les chiffres sont compris entre 0 et 9. L'écriture de b en base b est unique car si $n = x_0 + x_1 b + \ldots + x_s b^s$ avec $0 \leq x_0 < b$, alors x_0 est le

reste de la division de n par b d'où $x_0 = a_0$. Puis x_1 est le reste de la division de $\frac{n-a_0}{b}$ par b donc $x_a = a_1$ et de proche en proche $s = r$ et $x_i = a_i$ pour tout i.

Soit p un nombre premier.

Pour calculer les coefficients binomiaux $\binom{n}{m}$ modulo p nous commençons par écrire n et m en base p. Nous pouvons supposer que n et m ont le même nombre de chiffres en complétant par 0 :

$$\begin{aligned} n &= n_0 + n_1 p + n_2 p^2 + \ldots + n_r p^r \qquad 0 \leq n_i < p \\ m &= m_0 + m_1 p + m_2 p^2 + \ldots + m_r p^r \qquad 0 \leq m_i < p \end{aligned}$$

Proposition 2.10

Nous avons $\binom{n}{m} \equiv \prod_{i=0}^{r} \binom{n_i}{m_i} \bmod p$ où par convention $\binom{a}{b} = 0$ si $a < b$.

Démonstration. Dans $\mathbb{F}_p[X]$ nous avons

$$(1+X)^{n_i p^i} = \left((1+X)^{p^i}\right)^{n_i} = (1+X^{p^i})^{n_i}.$$

En effectuant le produit de ces égalités pour $i = 0, 1, \ldots, r$ nous obtenons

$$(1+X)^n = (1+X)^{n_0}(1+X^p)^{n_1} \ldots (1+X^{p^r})^{n_r}. \tag{2.2}$$

Développons le facteur $(1+X)^{n_i p^i}$ où $0 \leq i \leq r$:

$$(1+X)^{n_i p^i} = \sum_{k=0}^{n_i} \binom{n_i}{k} X^{k p^i}$$

Pour obtenir le terme en X^m dans le membre de droite de (2.2) il faut choisir dans chaque facteur un monôme $\binom{n_i}{k_i} X^{k_i p^i}$ de telle sorte que $0 \leq k_i \leq n_i$ et

$$X^m = \prod_{i=0}^{r} X^{k_i p^i} = X^{\sum_{i=0}^{r} k_i p^i},$$

c'est-à-dire $\sum_{i=0}^{r} k_i p^i = m$. Étant donné que $k_i \leq n_i < p$ ces entiers k_i doivent être les chiffres de m en base p. Si nous avons $m_i \leq n_i$ pour tout i, le coefficient de X^m dans les polynômes de (2.2) est donc $\binom{n}{m} = \prod_{i=0}^{r} \binom{n_i}{m_i} \bmod p$. S'il existe un entier i tel que $n_i < m_i$, ce coefficient est nul. Mais dans ce cas nous avons convenu que $\binom{n_i}{m_i} = 0$; par suite le produit $\prod_{i=0}^{r} \binom{n_i}{m_i}$ est également nul. □

Exemples 9. ◇ Calculons $\binom{19}{9}$ mod 3. Commençons par écrire 19 et 9 en base 3 :

$$19 = 1 + 0 \times 3 + 2 \times 3^2, \qquad 9 = 0 + 0 \times 3 + 1 \times 3^2.$$

Nous avons $\binom{19}{9} \equiv \binom{1}{0}\binom{0}{0}\binom{2}{1} \equiv 1 \times 1 \times 2 \equiv 2 \bmod 3$. Par suite $\binom{19}{9} \equiv 2 \bmod 3$.

◇ Calculons $\binom{29}{9}$ mod 3. Commençons par écrire 29 et 9 en base 3 :

$$29 = 2 + 0 \times 3 + 0 \times 3^2 + 1 \times 3^3, \qquad 9 = 0 + 0 \times 3 + 1 \times 3^2.$$

Il en résulte que $\binom{29}{9} \equiv \binom{2}{0}\binom{0}{0}\binom{0}{1}\binom{1}{0} \bmod 3$; comme $\binom{0}{1} = 0$ nous obtenons $\binom{29}{9} \equiv 0 \bmod 3$.

Exemple 15. Soient p un nombre premier, r un entier positif et k un entier tel que $0 < k < p$. Les écritures en base p de kp^r et de pr sont

$$kpr^r = 0 + 0 \times p + \ldots + k \times p^r \qquad pr^r = 0 + 0 \times p + \ldots + 1 \times p^r.$$

Par conséquent $\binom{kp^r}{p^r} \equiv \binom{0}{0}\binom{0}{0}\ldots\binom{k}{1} \bmod p$ et $\binom{kp^r}{p^r} \equiv k \bmod p$.

3 Anneaux principaux, anneaux euclidiens

Dans ce paragraphe nous introduisons la notion d'anneau principal où nous disposons, comme dans $\mathbb{Z}$, du pgcd et de la décomposition en « facteurs premiers ».

Nous définissons aussi les anneaux euclidiens qui sont pratiques pour les calculs.

Nous présenterons ensuite des exemples d'anneaux de nombres, analogues à l'anneau des entiers de Gauss.

3.1 Anneau principal

Définition 3.1

Un anneau A est *principal* s'il est intègre et si tout idéal de A est principal, c'est-à-dire de la forme aA où $a \in A$.

Exemples 10. ◇ L'anneau $\mathbb{Z}$ est principal.

◇ Pour tout corps $\Bbbk$ l'anneau de polynômes $\Bbbk[X]$ est principal.

◇ L'anneau $\mathbb{Z}[X]$ n'est pas principal.

Nous allons voir que dans un anneau principal nous possédons les outils essentiels de pgcd et de décomposition en facteurs premiers.

Définition 3.2

Soit A un anneau intègre. Soient a, b deux éléments de A. S'il existe un élément inversible $\varepsilon \in A^*$ tel que $a = b\varepsilon$, on dit que a et b sont *associés*.

La relation « a et b sont associés » est une relation d'équivalence sur A. Rappelons en effet que si a et b sont des éléments d'un anneau intègre A, alors nous avons les équivalences

$$aA \subset bA \iff b \,|\, a \text{ et } aA = bA \iff a = b\varepsilon \text{ où } \varepsilon \text{ est inversible}$$

Ainsi l'égalité $aA = bA$ est vraie si et seulement si a et b sont associés.

3.1.1 Pgcd

Si a et b sont des éléments d'un anneau A, alors l'ensemble $\{au+bv \,|\, u,\, v \in A\}$ est un idéal de A.

Définition 3.3

Soit A un anneau principal. Soient a, b deux éléments de A. Tout élément $d \in A$ tel que $dA = \{au+bv \,|\, u,\, v \in A\}$ s'appelle un *pgcd* de a et b et se note $\text{pgcd}(a,b)$. Si $\text{pgcd}(a,b)$ est un élément inversible de A, on dit que a et b sont *premiers entre eux*.

Si d est un pgcd de a et b, alors pour tout élément inversible ε, εd est un pgcd de a et b : le pgcd n'est donc défini qu'à un inversible près.

- ◇ Dans l'anneau $\mathbb{Z}$, les inversibles sont 1 et -1 ; par convention « le » pgcd est positif.
- ◇ Soit $\Bbbk$ un corps. Dans $\Bbbk[X]$ les inversibles sont les polynômes constants non nuls et le pgcd n'est défini qu'à multiplication près par un élément de $\Bbbk^*$. Par convention « le » pgcd est un polynôme unitaire.

Proposition 3.1

Soit A un anneau principal. Soient a, b et c des éléments de A.

- ◇ $\text{pgcd}(a,b)$ divise a et b. Si c divise a et b, alors c divise $\text{pgcd}(a,b)$.
- ◇ Il existe u, $v \in A$ tels que $au+bv = \text{pgcd}(a,b)$ (relation de Bezout).
- ◇ Si $a \,|\, bc$ et si a et b sont premiers entre eux, alors $a \,|\, c$ (théorème de Gauss).

Les démonstrations se font comme pour les polynômes à coefficients dans un corps.

3.1.2 Éléments irréductibles

Définition 3.4

Soit A un anneau intègre. Un élément $a \neq 0$ appartenant à A est *irréductible* si a n'est pas inversible et si pour tous u, $v \in A$ nous avons l'implication

$$a = uv \Rightarrow u \text{ ou } v \text{ est inversible}$$

Un élément a non nul et non inversible est irréductible si et seulement si ses seuls diviseurs sont des inversibles ou des éléments associés à a.

Exemples 11.

- ◇ Les éléments irréductibles de $\mathbb{Z}$ sont les $\pm p$ où p est un nombre premier.
- ◇ Soit $\Bbbk$ un corps. Un polynôme $P \in \Bbbk[X]$ de degré n est irréductible si et seulement si $n \geq 1$ et si les seuls diviseurs de P sont de degré 0 ou n.
  Tout polynôme de degré 1 est donc irréductible dans $\Bbbk[X]$.
- ◇ Dans l'anneau $\mathbb{Z}[\mathbf{i}]$ nous avons $(3+2\mathbf{i})(3-2\mathbf{i}) = 3^2+2^2 = 13$. Puisque $3+2\mathbf{i}$ et $3-2\mathbf{i}$ ne sont pas inversibles dans $\mathbb{Z}[\mathbf{i}]$, 13 n'est pas irréductible dans $\mathbb{Z}[\mathbf{i}]$ alors qu'il l'est dans le sous-anneau $\mathbb{Z}$ de $\mathbb{Z}[\mathbf{i}]$.

Proposition 3.2

Soit A un anneau principal. Soient a et p des éléments de A. Si p est irréductible, alors

$$\text{pgcd}(p,a) = \begin{cases} 1 \text{ si } p \text{ ne divise pas } a \\ \text{p si } p \,|\, a \end{cases}$$

Démonstration. Posons $d = \text{pgcd}(p,a)$. Si $p \,|\, a$, alors $\text{pgcd}(p,a) = p$. Supposons que d'une part p est irréductible, et que d'autre part p ne divise pas a. Puisque $p \,|\, d$, il existe u dans A tel que $p = du$ d'où d appartient à A^* ou u appartient à A^*. Remarquons que si u appartient à A^*, alors $p \,|\, d$ ce qui est impossible puisque p ne divise pas a. Il en résulte que d appartient à A^* ; cela signifie que p et a sont premiers entre eux, *i.e.* que 1 est un pgcd de a et p. □

Corollaire 3.1

Soit A un anneau principal. Soient a, b des éléments de A et p un irréductible de A. Si $p \,|\, ab$, alors $p \,|\, a$ ou $p \,|\, b$.

Démonstration. Supposons que p ne divise pas a. La Proposition 3.2 assure alors que p et a sont premiers entre eux ; d'après le Théorème de Gauss p divise donc b. □

3.1.3 Factorisation en produit d'irréductibles

Commençons par démontrer une propriété technique et utile.

Proposition 3.3

Soit A un anneau principal. Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de A tels que, pour tout n, a_{n+1} divise a_n. Il existe un entier N tel que, pour tout $k \geq N$, a_k et a_N sont associés.

Démonstration. Soit $\mathcal{I} = \{x \in A \,|\, \exists\, n \in \mathbb{N} \text{ tel que } a_n | x\}$.

Montrons que $\mathcal{I}$ est un idéal de A. En effet, soient x et y des éléments de $\mathcal{I}$. Il existe n tel que a_n divise x et il existe m tel que a_m divise y. Si par exemple $m \geq n$, alors par hypothèse a_m divise a_n d'où a_m divise x ; autrement dit a_m divise x et y donc a_m divise $x+y$. Il s'en suit que $x+y$ appatient à $\mathcal{I}$. Puisque a_n divise $-x$, $-x$ appartient à $\mathcal{I}$. Enfin 0 appartient à $\mathcal{I}$. Il en résulte que $\mathcal{I}$ est un sous-groupe additif de A. De plus, pour tout $a \in A$, a_n divise ax, ainsi $ax \in \mathcal{I}$. Finalement $\mathcal{I}$ est un idéal de A.

Remarquons que pour tout n, nous avons les inclusions : $a_nA \subset a_{n+1}A \subset \mathcal{I}$.

Puisque A est principal, il existe $\alpha \in A$ tel que $\alpha A = \mathcal{I}$. Étant donné que α appartient à $\mathcal{I}$, il existe un entier N tel que a_N divise α. Nous en déduisons les inclusions

$$a_nA \subset \mathcal{I} = \alpha A \subset a_NA.$$

Il en résulte que $\alpha A = \mathcal{I} = a_NA$. Pour tout entier $k \geq N$, il s'en suit $a_kA \subset \mathcal{I} = a_NA \subset a_kA$ d'où $a_kA = a_NA$: les éléments a_k et a_N sont associés. □

Proposition 3.4

Dans un anneau principal, tout élément non nul et non inversible a un diviseur irréductible.

Démonstration. Soit A un anneau principal. Soit $a \in A$ un élément non nul et non inversible. Si a est irréductible, le diviseur a convient.

Suppsons a non irréductible. Il existe a_1, $b_1 \in A^*$ tels que $a = a_1 b_1$. Si a_1 est irréductible, nous avons fini. Sinon il existe a_2, $b_2 \in A^*$ tel que $a_1 = a_2 b_2$. Supposons que ce processus de factorisation ne s'arrête pas et qu'on puisse construire des suites (a_n) et (b_n) d'éléments de A tels que, pour tout n,

$$a_n = a_{n+1} b_{n+1}, \qquad a_n \text{ non inversible}, \qquad b_n \text{ non inversible}$$

Pour tout n, a_{n+1} divise a_n et comme le quotient n'est pas inversible a_{n+1} et a_n ne sont pas associés : contradiction avec la Proposition 3.3. Il existe donc un entier ℓ tel que le diviseur a_ℓ soit irréductible. □

Proposition 3.5: (Factorisation en produit d'irréductibles)

Soit A un anneau principal. Soit $a \in A$ un élément non nul et non inversible. Il existe des irréductibles p_1, p_2, ..., p_k tels que $a = p_1 p_2 \dots p_k$. Cette factorisation est unique au sens suivant : si $p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$, avec q_i irréductibles, alors $k = \ell$; de plus quitte à changer l'ordre des facteurs p_i et q_i sont associés pour tout i.

Démonstration. Montrons tout d'abord l'existence de la factorisation. La Proposition 3.4 assure que a a un diviseur irréductible p_1 ; nous avons ainsi une factorisation $a = p_1 a_1$ avec $a_1 \in A$. Si a_1 est irréductible, nous avons fini. Sinon il existe un irréductible p_2 tel que $a_1 = p_2 a_2$ avec $a_2 \in A$. Supposons que ce processus ne s'arrête pas. Nous construisons alors une suite d'éléments $a_n \in A$ et d'irréductibles p_n tels que $a_n = p_{n+1} a_{n+1}$. Pour tout n, a_{n+1} divise a_n et n'est pas associé à a_n : contradiction. Par suite il existe un entier k tel que a_k est irréductible. Nous avons alors

$$a = p_1 a_1 = p_1 p_2 a_2 = \dots = p_1 p_2 \dots p_k a_k$$

et dans ce dernier produit, tous les termes sont irréductibles.

Soient $p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ des factorisations en produit d'irréductibles. L'irréductible p_1 divise $q_1 q_2 \dots q_\ell$ donc p_1 divise l'un des q_i. Quitte à réindicer les q_i nous pouvons supposer que p_1 divise q_1. Comme q_1 est irréductible, $q_1 = p_1 \varepsilon_1$ avec $\varepsilon_1 \in A^*$. En divisant chaque factorisation par p_1 il vient (si $k \geq 2$) $p_2 \dots p_k = \varepsilon_1 q_2 \dots q_\ell$. Supposons $k \leq \ell$. En continuant ainsi, on voit que pour tout $i \in \{1, \dots, k\}$, p_i et q_i sont associés. Si $k < \ell$, il existe un inversible ε tel que $1 = \varepsilon q_{k+1} \dots q_\ell$: impossible car les q_i ne sont pas inversibles. □

Notation. Si p_1 et p_2 sont des irréductibles associés, il existe $\varepsilon \in A^*$ tel que $p_2 = \varepsilon p_1$ donc $p_1 p_2 = \varepsilon p_1^2$. Plus généralement, regroupons les irréductibles associés qui apparaissent dans la décomposition de a. La factorisation prend la forme

$$a = \varepsilon q_1^{m_1} q_2^{m_2} \dots q_\ell^{m_\ell}$$

où les q_i sont des irréductibles deux à deux non associés, $m_i \geq 1$ et $\varepsilon \in A^*$.

- ◇ Pour tout i, on pose $\nu_{q_i}(a) = m_i$,
- ◇ si on remplace q_i par un associé q_i', alors $\nu_{q_i}(a) = \nu_{q_i'}(a)$ d'après l'unicité de la décomposition.

Corollaire 3.2

Soit A un anneau principal. Soient a, b, $c \in A$ des éléments non nuls et non inversibles tels que $ab = c^n$ avec $n \geq 1$. Si a et b sont premiers entre eux, il existe α, β des éléments de A et ε, $\varepsilon' \in A^*$ des inversibles tels que $a = \varepsilon\alpha^n$ et $b = \varepsilon'\beta^n$.

Démonstration. Posons $a = \varepsilon p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ et $b = \varepsilon' q_1^{m_1} q_2^{m_2} \dots q_\ell^{m_\ell}$ où ε, $\varepsilon' \in A^*$, où les p_i sont des irréductibles deux à deux non associés, de même que les q_j. Supposons a et b premiers entre eux. Alors aucun p_i n'est associé à un q_j ; par conséquent la décomposition de ab est

$$ab = (\varepsilon\varepsilon')p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} q_1^{m_1} q_2^{m_2} \dots q_\ell^{m_\ell}.$$

Puisque $ab = c^n$, l'unicité de la décomposition assure que chaque exposant $n_i = \nu_{p_i}(c^n) = n\nu_{p_i}(c)$ est multiple de n. De même chaque m_j est multiple de n. Autrement dit il existe des entiers positifs d_i et δ_j tels que $n_i = d_i n$ et $m_j = \delta_j n$. Alors $a = \varepsilon\big(p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}\big)^n$ et $b = \varepsilon'\big(q_1^{\delta_1} q_2^{\delta_2} \dots q_\ell^{\delta_\ell}\big)^n$. □

3.1.4 Anneau quotient d'un anneau principal

L'énoncé suivant permet de construire des corps :

Théorème 3.1

Soit A un anneau principal. Soit $a \in A$ un élément non nul et non inversible. Les propriétés suivantes sont équivalentes :

(i) a est irréductible ;
(ii) l'anneau quotient A/aA est un corps ;
(iii) l'anneau quotient A/aA est intègre.

Exemple 16. Nous retrouvons que pour tout entier $n \geq 2$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Démonstration. Notons $p\colon A \to A/aA$ la projection canonique.

(i) ⇒ *(ii)* Supposons que a soit irréductible.

Soit $\alpha \in A/aA$; soit $x \in A$ tel que $p(x) = \alpha$. Supposons que α soit non nul, c'est-à-dire que x ne soit pas un multiple de a. Puisque a est irréductible, x et a sont premiers entre eux ; il existe donc u, v dans A tels que $au + bx = 1$. En appliquant le morphisme p nous obtenons

$$1 = \underbrace{p(a)}_{0} p(u) + p(x)p(v) = \underbrace{p(x)}_{\alpha} p(v).$$

Ainsi $\alpha p(v) = 1$; en particulier α est inversible dans A/aA. Finalement tout élément non nul de A/aA est inversible donc A/aA est un corps.

$(ii) \Rightarrow (iii)$ découle du fait qu'un corps est un anneau intègre.

$(iii) \Rightarrow (i)$ Supposons que A/aA soit intègre. Soient u et v dans A tels que $a = uv$. Dans A/aA nous avons l'égalité $0 = p(a) = p(u)p(v)$, donc par exemple, $p(u) = 0$. Autrement dit, u est multiple de a : u s'écrit au' pour un certain u' dans A. Il en résulte que $a = uv = au'v$. Comme A est intègre, nous obtenons que $u'v = 1$. Ainsi v est inversible et a est irréductible.

□

3.2 Polynômes irréductibles de $\Bbbk[X]$

Si $\Bbbk$ est un corps, l'anneau $\Bbbk[X]$ est principal (§2.2.1). Tout polynôme non nul $P \in \Bbbk[X]$ s'écrit $P = \lambda P_1^{n_1} P_2^{n_2} \dots P_k^{n_k}$ où λ désigne un élément de $\Bbbk^*$ et où les P_i sont des polynômes irréductibles unitaires deux à deux distincts. Cette factorisation est unique à l'ordre près des facteurs.

Nous présentons quelques résultats généraux sur les polynômes irréductibles dans $\Bbbk[X]$.

Proposition 3.6

Soit $\Bbbk$ un corps.
- ◇ Les polynômes de degré 1 sont irréductibles dans $\Bbbk[X]$.
- ◇ Soit $P \in \Bbbk[X]$ un polynôme de degré 2 ou 3. Le polynôme P est irréductible dans $\Bbbk[X]$ si et seulement s'il n'a pas de racine dans $\Bbbk$.

Démonstration. Les polynômes de degré 1 sont irréductibles.

Soit $P \in \Bbbk[X]$ de degré 2 ou 3. Si P a une racine $a \in \Bbbk$, il existe $Q \in \Bbbk[X]$ tel que $P = (X - a)Q$. Nous avons $\deg Q = (\deg P) - 1 > 0$; par suite P n'est pas irréductible.

Réciproquement, si P n'est pas irréductible, il existe des polynômes U et V dans $\Bbbk[X]$ tels que $P = UV$, $\deg U \geq 1$ et $\deg V \geq 1$. Puisque $\deg U + \deg V = \deg P \leq 3$, l'un des polynômes U ou V est de degré 1. Le polynôme P a donc une racine dans $\Bbbk$. □

Exemples 12.
- ◇ Le polynôme $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ car il est de degré 3 et n'a pas de racine dans $\mathbb{Q}$. Mais $X^3 - 2$ n'est pas irréductible dans $\mathbb{R}[X]$ car il est multiple de $X - \sqrt[3]{2}$.
- ◇ Le polynôme $X^4 + 1$ n'a pas de racine dans $\mathbb{R}$ mais il n'est pas irréductible dans $\mathbb{R}[X]$ car

$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$$

- ◇ Les polynômes $X^2 + X + 1$ et $X^3 + X^2 + 1$ sont irréductibles dans $\mathbb{F}_2[X]$ car ils sont de degré 2 et n'ont pas de racine dans $\mathbb{F}_2$.
- ◇ Soit $P \in \Bbbk[X]$ un polynôme de degré au moins 2. Si P a une racine dans $\Bbbk$, alors P n'est pas irréductible. En effet, si $a \in \Bbbk$ est une racine de P, nous avons $P = (X - a)Q$ où $Q \in \Bbbk[X]$ et $\deg Q > 0$.

Proposition 3.7

- ◇ Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- ◇ Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est négatif.

Démonstration. ◇ Tout polynôme $P \in \mathbb{C}[X]$ non constant a au moins une racine dans $\mathbb{C}$ (théorème de d'Alembert-Gauss). Par suite si $\deg P \geq 2$, alors P n'est pas irréductible dans $\mathbb{C}[X]$.

◇ Soit $P \in \mathbb{R}[X]$ un polynôme de degré au moins 2.
Si P a une racine réelle, alors P n'est pas irréductible.
Suppsons que P n'ait pas de racine réelle. Si $\alpha \in \mathbb{C}$ est une racine de P, alors le conjugué $\overline{\alpha}$ est aussi racine de P. Écrivons les racines complexes de P sous la forme α_1, $\overline{\alpha_1}$, α_2, $\overline{\alpha_2}$, …, α_k, $\overline{\alpha_k}$ où $k \geq 1$ et $\alpha_i \neq \overline{\alpha_i}$ pour tout i. Il existe un nombre réel $\lambda \neq 0$ tel que

$$\begin{aligned} P &= \lambda(X-\alpha_1)(X-\overline{\alpha_1})(X-\alpha_2)(X-\overline{\alpha_2})\dots(X-\alpha_k)(X-\overline{\alpha_k}) \\ &= \lambda(X^2+a_1X+b_1)(X^2+a_2X+b_2)\dots(X^2+a_kX+b_k) \end{aligned}$$

où a_i et b_i sont des nombres réels tels que $a_i^2 - 4b_i < 0$. Si P est irréductible dans $\mathbb{R}[X]$, il ne peut y avoir qu'un seul facteur dans le dernier produit ($k = 1$) donc P est de degré 2 et de discriminant strictement négatif.

□

Polynômes irréductibles de $\mathbb{F}_p[X]$

Pour tout entier $n \geq 0$ il n'y a qu'un nombre fini de polynômes de degré n dans $\mathbb{F}_p[X]$, donc un nombre fini de polynômes irréductibles de degré n. Nous pouvons les obtenir de proche en proche de la manière suivante (crible d'Eratosthène) :

- ◇ Nous écrivons la liste des polynômes de degré 1 : ils sont irréductibles ;
- ◇ dans la liste des polynômes de degré 2, nous supprimons ceux qui sont multiples d'un polynôme de degré 1 : il reste les polynômes irréductibles de degré 2 ;
- ◇ plus généralement dans la liste des polynômes de degré n nous supprimons ceux qui sont multiples d'un polynôme irréductible de degré inférieur à n : il reste les polynômes irréductibles de degré n.

Exemple 17. Le seul polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$ est X^2+X+1. Pour trouver les polynômes irréductibles de degré 4 dans $\mathbb{F}_2[X]$, il suffit d'écrire les polynômes de degré 4 qui n'ont pas de racine et de supprimer le polynôme $(X^2+X+1)^2 = X^4+X^2+1$. Voici la liste où nous avons souligné les trois polynômes irréductibles :

$$\underline{X^4+X^3+1}, \qquad X^4+X^2+1, \qquad \underline{X^4+X+1}, \qquad \underline{X^4+X^3+X^2+X+1}.$$

Sur les polynômes irréductibles de $\mathbb{Q}[X]$

Nous ne pouvons pas trouver les polynômes irréductibles de $\mathbb{Q}[X]$ par un crible analogue à celui que nous venons de décrire. Voici une condition commode d'irréductibilité utilisant le morphisme $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ de réduction modulo un nombre premier p. Commençons par un résultat préliminaire.

Lemme 3.1

Soient A et B des polynômes à coefficients dans $\mathbb{Z}$. Soit p un nombre premier. Supposons que tous les coefficients du polynôme AB sont multiples de p. Alors l'un au moins des polynômes A ou B a tous ses coefficients multiples de p.

Démonstration. Notons $f\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme de réduction modulo p. Pour tout polynôme $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ nous avons

$$f(P) = \overline{a_0} + \overline{a_1}X + \ldots + \overline{a_n}X^n$$

où $\overline{k}$ désigne la classe de k modulo p. Puisque tous les coefficients de AB sont multiples de p, le polynôme $f(AB)$ est nul. Étant donné que f est un morphisme d'anneaux nous avons l'égalité $f(A)f(B) = f(AB) = 0$. L'anneau $\mathbb{F}_p[X]$ étant intègre, l'un au moins des polynômes $f(A)$ ou $f(B)$ est nul. Si par exemple $f(A) = 0$, alors tous les coefficients de A sont multiples de p. □

Lemme 3.2

Soit $P \in \mathbb{Z}[X]$ un polynôme non nul. S'il existe des polynômes U, $V \in \mathbb{Q}[X]$ tels que $P = UV$, alors il existe des polynômes U_1, $V_1 \in \mathbb{Z}[X]$ tels que $P = U_1V_1$, $\deg U_1 = \deg U$ et $\deg V_1 = \deg V$.

Démonstration. Supposons que P s'écrive UV avec U, $V \in \mathbb{Q}[X]$. En chassant les dénominateurs des coefficients de U et de V, nous obtenons un entier $n > 0$ et des polynômes A, $B \in \mathbb{Z}[X]$ tels que $nP = AB$, $\deg A = \deg U$ et $\deg B = \deg V$.

Si $n > 1$, alors il existe un nombre premier q tel que q divise n. Puisque P est à coefficients entiers, le polynômes nP a tous ses coefficients multiples de q. Le Lemme 3.1 assure que le polynôme A, par exemple, a tous ses coefficients multiples de q. Divisons ces coefficients par q ce qui ne change pas les degrés de A et B : nous obtenons un polynôme $A_1 \in \mathbb{Z}[X]$ tel que $(n/q)P = A_1B$ et $\deg A_1 = \deg A$.

Si $\frac{n}{q} > 1$, nous continuons en divisant par un diviseur premier de $\frac{n}{q}$. Finalement nous obtenons deux polynômes U_1, $V_1 \in \mathbb{Z}[X]$ tels que $P = U_1V_1$, $\deg U_1 = \deg U$ et $\deg V_1 = \deg V$. □

Proposition 3.8

Soit $P \in \mathbb{Z}[X]$ un polynôme de degré non nul. Soit p un nombre premier qui ne divise pas le coefficient dominant de P. Si la réduction de P modulo p est un polynôme irréductible de $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Supposons que P s'écrive UV avec U, V dans $\mathbb{Q}[X]$. Nous devons montrer que U ou V est de degré 0. Le Lemme 3.2 assure l'existence de deux polynômes U_1, $V_1 \in \mathbb{Z}[X]$ tels que $P = U_1V_1$, $\deg U_1 = \deg U$ et $\deg V_1 = \deg V$.

En appliquant le morphisme $f\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ de réduction modulo p, nous obtenons dans $\mathbb{F}_p[X]$ l'égalité $f(P) = f(U_1)f(V_1)$. Soient a, u_1 et v_1 les coefficients dominants de P, U_1 et V_1. Nous avons $a = u_1v_1$. Par hypothèse p ne divise pas a, par conséquent p ne divise ni u_1, ni v_1. Ainsi les classes modulo p de u_1 et v_1 sont des éléments non nuls de $\mathbb{F}_p$. Nous en déduisons que $\deg f(U_1) = \deg U_1$, $\deg f(V_1) = \deg V_1$ et $\deg f(P) = \deg P$. Si le polynôme $f(P)$ est irréductible dans $\mathbb{F}_p[X]$, l'un des polynômes $f(U_1)$ ou $f(V_1)$ est de degré 0. Étant donné que $f(U_1)$ et $f(V_1)$ ont même degré que U et V, l'un des polynômes U ou V est de degré 0. □

Exemple 18. Soit $P = X^4 - 6X^3 + 2X^2 - 3X + 9$. C'est un polynôme unitaire à coefficients entiers. Sa réduction modulo 2 est $X^4 + X + 1$ qui, comme nous l'avons vu précédemment, est irréductible dans $\mathbb{F}_2[X]$. Par suite P est un polynôme irréductible de $\mathbb{Q}[X]$.

Exemple 19. Montrons que le polynôme $P = X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.

Supposons que $P = UV$ où U, $V \in \mathbb{Q}[X]$ sont de degré non nul. Étant donné que $X^4 + 1$ n'a pas de racine réelle, U et V n'ont pas de racine dans $\mathbb{Q}$. Il s'en suit que U et V sont de degré 2. La décomposition de P en irréductibles dans $\mathbb{R}[X]$ est

$$X^4 + 1 = (X^2 + 2\sqrt{2}X + 1)(X^2 - 2\sqrt{2}X + 1);$$

en particulier $X^2 + 2\sqrt{2}X + 1$ divise U. Ainsi il existe $\lambda \in \mathbb{R}^*$ tel que $U = \lambda(X^2 + 2\sqrt{2}X + 1)$. Le coefficient de X^2 dans U est un nombre rationnel ; par conséquent λ appartient à $\mathbb{Q}$. Mais alors $2\lambda\sqrt{2}$, le coefficient de X, n'appartient pas à $\mathbb{Q}$: contradiction. Nous en déduisons que P est un polynôme irréductible de $\mathbb{Q}[X]$.

Exemple 20. Montrons que pour tout nombre premier p, le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.

Soit p un nombre premier. Remarquons que pour tout $a \in \mathbb{F}_p^*$ l'un au moins des éléments -1, a ou $-a$ est un carré dans $\mathbb{F}_p$. En effet, si -1 et a ne sont pas des carrés, alors leur produit $-a$ est un carré.

- ◇ Supposons que -1 est un carré dans $\mathbb{F}_p$. En posant $-1 = \delta^2$ où $\delta \in \mathbb{F}_p$, il vient dans $\mathbb{F}_p[X]$ la factorisation
$$X^4 + 1 = X^4 - \delta^2 = (X^2 - \delta)(X^2 + \delta)$$
donc $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.
- ◇ Supposons que 2 est un carré dans $\mathbb{F}_p$: $2 = \alpha^2$ où $\alpha \in \mathbb{F}_p$. Alors dans $\mathbb{F}_p[X]$ nous avons la factorisation
$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1)^2 - (\alpha X)^2 = (X^2 + \alpha X + 1)(X^2 - \alpha X + 1)$$
donc $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.
- ◇ Enfin supposons que -2 est un carré dans $\mathbb{F}_p$: $-2 = \beta^2$ où $\beta \in \mathbb{F}_p$. Alors, comme ci-dessus, nous avons dans $\mathbb{F}_p[X]$
$$X^4 + 1 = (X^2 - 1)^2 + 2X^2 = (X^2 - 1)^2 - (\beta X)^2 = (X^2 + \beta X + 1)(X^2 - \beta X + 1)$$
donc $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.

Cet exemple montre les limites de l'énoncé précédent.

3.3 Anneau euclidien

Ce sont des anneaux où nous disposons d'une division euclidienne comme dans $\mathbb{Z}$ et $\Bbbk[X]$ où $\Bbbk$ est un corps. Nous devons nous donner un moyen de « mesurer » les restes.

Définition 3.5

Soit A un anneau intègre. L'anneau A est *euclidien* s'il existe une application $\vartheta : A \setminus \mathbb{N}$ ayant la propriété suivante : pour tout $a \in A$ et pour tout $b \in A \setminus \{0\}$ il existe q et r dans A tels que $a = bq + r$ et $(r = 0$ ou $\vartheta(r) < \vartheta(b))$.

Bien que nous ne demandons pas que q et r soient uniques, nous appelons ces éléments *quotient* et *reste*. La propriété essentielle d'un anneau euclidien est la suivante :

Théorème 3.2

Tout anneau euclidien est principal.

Démonstration. Soit A un anneau euclidien. Puisque A est intègre par hypothèse, nous devons montrer que tout idéal $\mathcal{I}$ de A est principal. Si $\mathcal{I} = \{0\}$, alors $\mathcal{I} = 0A$. Supposons désormais que $\mathcal{I} \neq \{0\}$. Alors $\vartheta(\mathcal{I} \setminus \{0\})$ est une partie non vide de $\mathbb{N}$; elle possède donc un plus petit élément $\vartheta(b)$ où $b \in \mathcal{I} \setminus \{0\}$. Puisque b appartient à $\mathcal{I}$, nous avons l'inclusion $bA \subset \mathcal{I}$. Montrons l'inclusion réciproque $\mathcal{I} \subset bA$. Soit $x \in \mathcal{I}$. Il existe q, $r \in A$ tels que $x = bq + r$ avec $r = 0$ où $\vartheta(r) < \vartheta(b)$. Étant donné que bq appartient à $\mathcal{I}$, $r = x - bq$ appartient à $\mathcal{I}$; l'hypothèse « $\vartheta(b)$ est le plus petit élément de $\vartheta(\mathcal{I} \setminus \{0\})$ » entraîne $r = 0$. Autrement dit $x = bq$ et x appartient à bA. Ainsi $\mathcal{I} = bA$ et l'idéal $\mathcal{I}$ est principal. □

Algorithme d'Euclide

Comme dans $\mathbb{Z}$ et $\Bbbk[X]$, cet algorithme permet de calculer un pgcd et de trouver une relation de Bezout.

Soit A un anneau euclidien. Soient a, b des éléments de A tels que $b \neq 0$. Faisons les divisions euclidiennes successives suivantes tant que n'apparaît pas un reste nul :

$$\begin{aligned} a &= bq + r_1 \\ b &= r_1 q_2 + r_2 \\ \vdots &= \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

Les $\vartheta(r_k)$, pour $r_k \neq 0$, forment une suite strictement décroissante d'entiers positifs ou nuls, donc l'un des restes, disons r_{n+1} est nécessairement nul et l'algorithme s'arrête. En raisonnant comme pour les polynômes nous montrons que

$$\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r_1) = \ldots = \operatorname{pgcd}(r_{n-1}, r_n) = r_n.$$

Le pgcd de a et b (qui est défini à un inversible près) est le dernier reste non nul dans l'algorithme d'Euclide.

Pour trouver une relation de Bezout $au + bv = \operatorname{pgcd}(a, b)$, nous procédons comme dans le cas des entiers.

3.4 Des anneaux pour l'arithmétique

Dans ce paragraphe on se donne un entier $d \in \mathbb{Z}$ différent de 0 et qui n'est pas le carré d'un entier ; en particulier $d \neq 1$. Posons

$$\gamma = \begin{cases} \sqrt{d} \text{ si } d > 0 \\ \mathbf{i}\sqrt{-d} \text{ si } d < 0 \end{cases}$$

Nous avons $\gamma^2 = d$, autrement dit γ est une racine (complexe) du polynôme $X^2 - d$. Posons $\mathbb{Z}[\gamma] = \{x + y\gamma \,|\, x, y \in \mathbb{Z}\}$.

Exemples 13. ◇ Pour $d = -1$, $\mathbb{Z}[\gamma] = \{x + y\mathbf{i} \,|\, x, y \in \mathbb{Z}\} = \mathbb{Z}[\mathbf{i}]$ est l'anneau des entiers de Gauss.
◇ Pour $d = 5$, $\mathbb{Z}[\gamma] = \mathbb{Z}[\sqrt{5}] = \{x + y\sqrt{5} \,|\, x, y \in \mathbb{Z}\}$ est inclus dans $\mathbb{R}$.

Proposition 3.9

◇ Si x, x', y, y' sont des entiers tels que $x + y\gamma = x' + y'\gamma$, alors $x = x'$ et $y = y'$.
◇ Si $d > 0$, alors $\mathbb{Z}[\gamma]$ est un sous-anneau de $\mathbb{R}$; si $d < 0$, alors $\mathbb{Z}[\gamma]$ est un sous-anneau de $\mathbb{C}$.
◇ $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[\gamma]$.

Démonstration. ◇ Soient x, x', y, y' des entiers tels que $x + y\gamma = x' + y'\gamma$.
Si $d < 0$, alors γ est imaginaire donc en séparant partie réelle et partie imaginaire, nous obtenons $x = x'$ et $y = y'$.
Supposons $d > 0$. Les entiers $u = x - x'$ et $v = y - y'$ vérifient $u - v\gamma = 0$. Nous devons montrer les égalités $u = v = 0$. Supposons $v \neq 0$; alors $u^2 = \gamma^2 v^2 = dv^2$. Puisque d n'est pas le carré d'un entier, l'un des facteurs premiers de d, disons p, apparaît dans la décomposition de d avec un exposant impair. L'exposant de p dans dv^2 est impair et l'exposant de p dans u^2 est pair : contradiction. Ainsi $v = 0$ et $u = 0$.
◇ L'ensemble $\mathbb{Z}[\gamma]$ est un sous-groupe additif de $\mathbb{C}$. Soient $a = x + y\gamma$ et $a' = x' + y'\gamma$ des éléments de $\mathbb{Z}[\gamma]$. Nous avons

$$aa' = (xx' + \gamma^2 yy') + (xy' + x'y)\gamma = (xx' + dyy') + (xy' + x'y)\gamma$$

et comme $xx' + dyy'$ et $xy' + x'y$ sont des entiers, aa' appartient à $\mathbb{Z}[\gamma]$. Puisque $1 = 1 + 0\gamma$ appartient à $\mathbb{Z}[\gamma]$, $\mathbb{Z}[\gamma]$ est un sous-anneau de $\mathbb{C}$.

□

3.4.1 Conjugaison et norme

Présentons maintenant des outils essentiels pour calculer dans les anneaux $\mathbb{Z}[\gamma]$.

Définitions 3.1

Soit $z = a + b\gamma$ un élément de $\mathbb{Z}[\gamma]$.
◇ Le *conjugué* de z est l'élément $\overline{z} = a - b\gamma$.
◇ La *norme* de z est l'entier $N(z) = z\overline{z} = (a + b\gamma)(a - b\gamma) = a^2 - b^2 d$.
Nous définissons ainsi une application $N \colon \mathbb{Z}[\gamma] \to \mathbb{Z}$.

Remarques 2. ◇ Nous avons l'équivalence : $N(z) = 0 \iff z = 0$.
◇ Pour tout entier $m \in \mathbb{Z}$, nous avons $N(m) = m^2$.
◇ Supposons $d < 0$. Alors γ est immaginaire donc $a - b\gamma$ est le conjugué du nombre complexe $a + b\gamma$; dans ce cas la conjugaison dans $\mathbb{Z}[\gamma]$ est simplement la conjugaison des nombres complexes.
• Pour tout $z \in \mathbb{Z}[\gamma]$, $N(z) = |z|^2$ est le carré du module de z.

- Nous avons $N(x) \in \mathbb{N}$ pour tout $z \in \mathbb{Z}[\gamma]$.

◇ Si $d > 0$, alors il y a des éléments de norme négative ; par exemple, dans $\mathbb{Z}[\sqrt{5}]$, nous avons $N(\sqrt{5}) = -5$.

◇ Attention à ne pas confondre cette notion de norme avec celle employée pour définir les espaces vectoriels normés.

Proposition 3.10: Propriétés de la conjugaison et de la norme

◇ La conjugaison $z \mapsto \overline{z}$ est un morphisme d'anneaux $\mathbb{Z}[\gamma] \to \mathbb{Z}[\gamma]$ et pour tout $z \in \mathbb{Z}[\gamma]$ nous avons $\overline{\overline{z}} = z$.

◇ La norme est une application $N \colon \mathbb{Z}[\gamma] \to \mathbb{Z}$ telle que

$$\text{pour tous } z,\, z' \in \mathbb{Z}[\gamma],\ N(zz') = N(z)N(z').$$

Démonstration. ◇ Soient z et z' dans $\mathbb{Z}[\gamma]$. Nous avons $\overline{z+z'} = \overline{z}+\overline{z'}$. Si $z = a+b\gamma$ et $z' = a'+b'\gamma$, alors

$$\overline{z}\overline{z'} = (a-b\gamma)(a'-b'\gamma) = (aa'+bb'd) - (ab'+a'b) = \overline{zz'}.$$

Puisque $\overline{1} = 1$, l'application $z \mapsto \overline{z}$ est un morphisme d'anneaux de $\mathbb{Z}[\gamma]$ dans lui-même.

◇ Pour tous z, $z' \in \mathbb{Z}[\gamma]$ nous avons

$$N(zz') = (zz')\overline{(zz')} = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = N(z)N(z').$$

□

Proposition 3.11

Soit $z \in \mathbb{Z}[\gamma]$.

◇ z est inversible dans $\mathbb{Z}[\gamma]$ si et seulement si $N(z) = \pm 1$.

◇ Si $|N(z)|$ est un nombre premier, alors z est irréductible dans $\mathbb{Z}[\gamma]$.

Démonstration. ◇ Si $N(z) = z\overline{z} = 1$, alors $\overline{z}$ est l'inverse de z. Si $N(z) = z\overline{z} = -1$, akors $-\overline{z}$ est l'inverse de z.

Réciproquement, supposons que z soit inversible dans $\mathbb{Z}[\gamma]$. Il existe $z' \in \mathbb{Z}[\gamma]$ tel que $zz' = 1$ d'où $1 = N(1) = N(zz') = N(z)N(z')$. Les entiers positifs $|N(z)|$ et $|N(z')|$ ont pour produit 1, par suite $N(z) = N(z') = \pm 1$.

◇ Supposons que $|N(z)|$ soit un nombre premier. Alors $N(z) \neq \pm 1$ donc z n'est pas inversible d'après ce qui précède. Supposons que z s'écrive uv avec u, $v \in \mathbb{Z}[\gamma]$. Alors le nombre premier $N(z)$ se factorise en $|N(z)| = |N(u)|\,|N(v)|$; il en résulte que l'un des entiers positifs $|N(u)|$ ou $|N(v)|$ est égal à 1. Si par exemple $|N(u)| = 1$, alors u est inversible.

□

Les inversibles de $\mathbb{Z}[\gamma]$

◇ Les inversibles de $\mathbb{Z}[\mathbf{i}]$ sont les $a+b\mathbf{i}$ tels que a, $b \in \mathbb{Z}$ et $a^2+b^2 = 1$; ainsi $(\mathbb{Z}[\mathbf{i}])^* = \{1, -1, \mathbf{i}, -\mathbf{i}\}$.

- ◇ Soit δ un entier au moins égal à 2 qui n'est pas le carré d'un entier. Les inversibles de $\mathbb{Z}[\mathbf{i}\sqrt{\delta}]$ sont les $a+b\mathbf{i}\sqrt{\delta}$ tels que a, $b\in\mathbb{Z}$ et $a^2+\delta b^2=1$. Cela exige $b=0$, d'où $\left(\mathbb{Z}[\mathbf{i}\sqrt{\delta}]\right)^*=\{1,-1\}$.
- ◇ Supposons $d>0$. Les inversibles de $\mathbb{Z}[\sqrt{\delta}]$ sont les $x+y\sqrt{\delta}$ où x, $y\in\mathbb{Z}$ vérifient l'une des égalités suivantes

$$x^2-dy^2=1, \qquad\qquad x^2-dy^2=-1.$$

  On peut montrer qu'il y a une infinité de solutions.

Exemple 21. Dans $\mathbb{Z}[\mathbf{i}]$ nous avons $N(5+2\mathbf{i})=N(5-2\mathbf{i})=29$ qui est un nombre premier ; par suite $5+2\mathbf{i}$ et $5-2\mathbf{i}$ sont deux irréductibles dont le produit est 29.

Exemple 22. Montrons que 2 est irréductible dans l'anneau $A=\mathbb{Z}[\mathbf{i}\sqrt{3}]$. Tout d'abord, 2 n'est ni nul, ni inversible. Supposons que 2 s'écrive uv avec u, $v\in A$. Alors $N(u)N(v)=N(uv)=N(2)=4$. La norme étant une fonction $A\to\mathbb{N}$ nous en déduisons que

- ◇ ou bien l'un des entiers $N(u)$ ou $N(v)$ vaut 1,
- ◇ ou bien $N(u)=N(v)=2$.

Mais pour tout élément $z=x+y\mathbf{i}\sqrt{3}$ de A nous avons $N(z)=x^2+3y^2$ donc $N(z)=2$ implique $y=0$ et $x^2=2$ ce qui est impossible. Par suite l'un des éléments u ou v est de norme 1, donc est inversible. Ainsi 2 est irréductible dans A.

3.4.2 Quelques cas particuliers

Proposition 3.12

Les anneaux $\mathbb{Z}[\mathbf{i}\sqrt{2}]$, $\mathbb{Z}[\mathbf{i}]$, $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[\sqrt{3}]$ sont euclidiens, en utilisant $z\mapsto|N(z)|$ comme fonction ϑ. En particulier, ces anneaux sont principaux.

Démonstration. Soit A l'un des anneaux de l'énoncé. Autrement dit $A=\mathbb{Z}[\gamma]$ où $\gamma^2=d$ est l'un des entiers -2, -1, 2 ou 3. Soient a, $b\in A$ avec $b\neq0$. Puisque A est un sous-anneau de $\mathbb{R}$ ou de $\mathbb{C}$, formons le nombre réel ou complexe $\frac{a}{b}=\frac{a\overline{b}}{N(b)}$. Il s'écrit $\frac{a}{b}=x+y\gamma$ avec x, $y\in\mathbb{Q}$. Soit n l'entier le plus proche de x et soit m l'entier le plus proche de y. Nous avons les inégalités $|x-n|\leq\frac{1}{2}$, $|y-m|\leq\frac{1}{2}$ et l'égalité

$$\frac{a}{b}=x+y\gamma=(n+m\gamma)+(x-n+(y-m)\gamma)$$

- ◇ Si $d\neq3$, alors $|d|\leq2$ et

$$|(x-n)^2-d(y-m)^2|\leq\frac{1}{4}+|d|\frac{1}{4}\leq\frac{1}{4}+\frac{1}{2}<1.$$

- ◇ Si $d=3$, alors $-\frac{3}{4}\leq(x-n)^2-d(y-m)^2\leq\frac{1}{4}$ donc

$$|(x-n)^2-d(y-m)^2|<1.$$

Posons $q=n+m\gamma$ et $r=a-bq=b(x-n+(y-m)\gamma)$. Nous avons $q\in A$, d'où $r\in A$. Définissons le conjugué et la norme d'un nombre $z=u+v\gamma$ où u, $v\in\mathbb{Q}$, en posant $\overline{z}=u-v\gamma$ et $N(z)=z\overline{z}=u^2-dv^2$. Alors l'égalité $N(zz')=N(z)N(z')$ est encore vraie. Par suite

$$|N(r)|=|N(b)||(x-n)^2-d(y-m)^2|<|N(b)|$$

car $N(b) \neq 0$. En prenant $\vartheta(z) = |N(z)|$ pour tout $z \in A$, nous définissons donc une division euclidienne dans A. □

Un exemple de division euclidienne

Dans l'anneau $\mathbb{Z}[\mathbf{i}]$ effectuons la division euclidienne de $a = 11 + 3\mathbf{i}$ par $b = 3 + 4\mathbf{i}$. Nous avons

$$\frac{a}{b} = \frac{11+3\mathbf{i}}{3+4\mathbf{i}} = \frac{(11+3\mathbf{i})(3+4\mathbf{i})}{3^2+4^2} = \frac{45}{25} - \frac{35}{25}\mathbf{i} = \frac{18}{10} - \frac{14}{10}\mathbf{i}$$

L'entier le plus proche de $\frac{18}{10}$ est 2 et l'entier le plus proche de $-\frac{14}{10}$ est -1 donc nous prenons comme quotient $q = 2 - \mathbf{i}$. Il vient

$$r = a - bq = (11+3\mathbf{i}) - (3+4\mathbf{i})(2-\mathbf{i}) = 1 - 2\mathbf{i}$$

et nous obtenons la division euclidienne :

$$a = b(2-\mathbf{i}) + (1-2\mathbf{i}) \text{ où } N(1-2\mathbf{i}) = 5 < N(b) = 25.$$

Nous avons aussi : $a = b(1-\mathbf{i}) + 4 + 2\mathbf{i}$ et $N(4+2\mathbf{i}) = 20 < N(b)$: c'est une autre division euclidienne de a par b.

Exemple 23. Montrons que l'anneau $A = \mathbb{Z}[\mathbf{i}\sqrt{3}]$ n'est pas principal (donc pas euclidien). Les éléments $1+\mathbf{i}\sqrt{3}$ et $1-\mathbf{i}\sqrt{3}$ appartiennent à A et nous avons $4 = (1+\mathbf{i}\sqrt{3})(1-\mathbf{i}\sqrt{3})$ donc 2 divise $(1+\mathbf{i}\sqrt{3})(1-\mathbf{i}\sqrt{3})$. De plus, 2 est irréductible dans A. Pour qu'un élément $a + b\mathbf{i}\sqrt{3} \in A$ soit multiple de 2 il faut et il suffit que a et b soient pairs. Donc 2 ne divise ni $(1+\mathbf{i}\sqrt{3})$, ni $(1-\mathbf{i}\sqrt{3})$. Le Corollaire 3.1 assure alors que l'anneau A n'est pas principal.