



Chapitre 5 : Compléments de théorie des ensembles et algèbre générale

I Théorie des ensembles

A) Relation binaire, application

Soient E, F deux ensembles, G une partie de $E \times F$.

Soit \mathcal{R} définie par :

$$\forall (x, y) \in E \times F, x\mathcal{R}y \iff (x, y) \in G \quad (5.1)$$

On dit que \mathcal{R} est une relation binaire de source E , de but F et de graphe G .

Une relation binaire \mathcal{R} est une application si $\forall x \in E, \exists! y \in F, x\mathcal{R}y$.

On note alors $y = \mathcal{R}(x)$.

B) Partitions, relation d'équivalence, quotient

- On appelle partition d'un ensemble E toute partie Π de $\mathcal{P}(E)$ telle que :
 - Les éléments de Π sont non vides ($\Pi \subset \mathcal{P}(E) \setminus \{\emptyset\}$)
 - Les éléments de Π sont deux à deux disjoints ($\forall A, B \in \Pi, A \neq B \implies A \cap B = \emptyset$)
 - Les éléments de Π recouvrent E ($\prod_{A \in \Pi} A = E$)

Remarque :

\emptyset admet une unique partition, à savoir $\Pi = \emptyset$ (et pas $\Pi = \{\emptyset\}$!)

- Surjection canonique et partition par fibres :

Proposition :

- Soit Π une partition de E . La relation binaire \mathcal{R} définie sur $E \times \Pi$ par $\forall (x, A) \in E \times \Pi, x\mathcal{R}A \iff x \in A$ est une application surjective $E \rightarrow \Pi$.
- Inversement, si $\varphi: E \rightarrow F$ est surjective, alors $\Pi = \{\varphi^{-1}\{y\}, y \in F\}$ est une partition de E . (les $\varphi^{-1}\{y\}$ sont appelées les fibres de φ)

Définition :

Dans le point (1), l'application $E \rightarrow \Pi$ s'appelle la surjection
 $x \mapsto A$ unique élément de Π tel que $x \in A$
canonique de E sur Π .

- Relation d'équivalence...(symétrique, réflexive, transitive)

Définition (Classe d'équivalence d'une relation d'équivalence) :

- Soit \mathcal{R} une relation d'équivalence sur E . On appelle classe d'équivalence de $x \in E$ la partie $Cl_{\mathcal{R}}(x) = \{y \in E, x\mathcal{R}y\}$.

Théorème :

L'ensemble des classes d'équivalences de \mathcal{R} est une partition de E , notée E/\mathcal{R} , et l'application

$$\begin{aligned} E &\longrightarrow E/\mathcal{R} && \text{est la surjection canonique associée.} \\ x &\longmapsto Cl_{\mathcal{R}}(x) \end{aligned}$$

- Cas des ensembles finis :

Théorème :

Soit E un ensemble fini.

1. Soit $f: E \rightarrow F$ une application. Alors les fibres de f sont finies, et $\#E = \sum_{y \in F} \#f^{-1}\{y\}$.
2. Si Π est une partition de E , alors $\#E = \sum_{A \in \Pi} \#A$.

Cas particulier :

Si tous les cardinaux des éléments de Π sont égaux à m , alors $\#E = m \times \#\Pi$.

Démonstrations

Premier théorème L'ensemble des classes d'équivalences forment une partition :

1. $\forall x \in E, Cl_{\mathcal{R}}(x) \neq \emptyset$ (en effet, $x \in Cl_{\mathcal{R}}(x)$ car $x\mathcal{R}x$)
2. Soient $x, y \in E$. Alors soit $Cl_{\mathcal{R}}(y) = Cl_{\mathcal{R}}(x)$, soit $Cl_{\mathcal{R}}(y) \cap Cl_{\mathcal{R}}(x) = \emptyset$.
En effet, supposons que $Cl_{\mathcal{R}}(y) \cap Cl_{\mathcal{R}}(x) \neq \emptyset$.
Soit alors $z \in Cl_{\mathcal{R}}(y) \cap Cl_{\mathcal{R}}(x)$.
Pour $t \in Cl_{\mathcal{R}}(x)$, on a $t\mathcal{R}x$, et $x\mathcal{R}z$ et $z\mathcal{R}y$, donc par transitivité $t\mathcal{R}y$.
Donc $Cl_{\mathcal{R}}(x) \subset Cl_{\mathcal{R}}(y)$. De même, $Cl_{\mathcal{R}}(y) \subset Cl_{\mathcal{R}}(x)$, d'où l'égalité
3. Les classes recouvrent E : $\forall x \in E, x \in Cl_{\mathcal{R}}(x)$

Deuxième théorème

1. Par récurrence sur le nombre de fibres non vides.
2. Soit f la surjection canonique ; alors $f^{-1}\{A\} = A$, puis on applique le point précédent.

II Théorie des groupes

A) Catégorie des groupes

1) Généralités

Définitions Groupes, morphismes de groupes, iso/automorphismes, sous-groupes...

Exemple :

Automorphisme intérieur (conjugaison)

Soit $(G, *)$ un groupe, et $a \in G$.

Alors $\sigma_a: G \rightarrow G$ est un automorphisme.

$$g \mapsto a * g * a^{-1}$$

De plus, l'application $(G, *) \rightarrow (\text{Aut}G, \circ)$ est un morphisme de groupes :

$$a \mapsto \sigma_a$$

Soit $a, b \in G$. Pour tout $g \in G$, on a :

$$(\sigma_a \circ \sigma_b)(g) = \sigma_a(b * g * b^{-1}) = \underbrace{a * b * g * b^{-1} * a^{-1}}_{(a*b)^{-1}} = \sigma_{a*b}(g).$$

Donc $\sigma_a \circ \sigma_b = \sigma_{a*b}$.

Propriétés

- Image directe ou réciproque d'un sous-groupe par un morphisme
- Noyau ou image d'un morphisme
- Un morphisme de groupe est injectif si, et seulement si, $\ker \varphi = \{1_G\}$.

2) Groupes produits

Théorème :

Soient (G_k, \mathcal{T}_k) ($k = 1, 2$) deux groupes de neutres e_k .

Alors la loi $*$ définie sur $G_1 \times G_2$ par : $\forall (x_1, x_2, y_1, y_2) \in (G_1 \times G_2)^2, (x_1, x_2) * (y_1, y_2) = (x_1 \mathcal{T}_1 y_1, x_2 \mathcal{T}_2 y_2)$ est une loi de groupe, de neutre (e_1, e_2) pour laquelle le symétrique de (x, y) est (x^{-1}, y^{-1}) .

Définition :

C'est la structure produit sur $G_1 \times G_2$. On peut la généraliser à un produit infini.

3) Sous-groupes distingués (hors programme)

Définition :

Soit (G, \mathcal{T}) un groupe. Une partie H de G est appelée sous-groupe distingué si c'est un sous-groupe stable par toutes les conjugaisons de G , c'est-à-dire :

1. H est un sous-groupe de (G, \mathcal{T})
2. $\forall a \in G, \forall h \in H, a \mathcal{T} h \mathcal{T} a^{-1} \in H$

Théorème :

Le noyau d'un morphisme de groupe est un sous-groupe distingué de la source.

Démonstration :

Soit $\varphi: (G_1, \mathcal{T}_1) \rightarrow (G_2, \mathcal{T}_2)$ un morphisme.

Posons $H = \ker \varphi$.

Déjà, H est un sous-groupe de (G_1, \mathcal{T}_1) .

Soient $a \in G_1, h \in H$.

On a : $\varphi(a\mathcal{T}_1h\mathcal{T}_1a^{-1}) = \varphi(a)\mathcal{T}_2\varphi(h)\mathcal{T}_2\varphi(a)^{-1} = \varphi(a)\mathcal{T}_2\varphi(a)^{-1} = 1_{G_2}$.

Donc $a\mathcal{T}_1h\mathcal{T}_1a^{-1} \in H$, et H est donc bien un sous-groupe distingué de G_1 .

Plus généralement, l'image réciproque d'un sous-groupe distingué par un morphisme est un sous-groupe distingué. (Quasiment la même démonstration)

Attention : C'est faux pour les images directes.

Exemple :

Si G est un groupe commutatif, tout sous-groupe de G est distingué

Si (G, \mathcal{T}) est un groupe quelconque, alors $\{1_G\}$ et G sont distingués.

Définition :

Un groupe dont les seuls sous-groupes distingués sont $\{1_G\}$ et G s'appelle un groupe simple.

B) Exemples de groupes

$(\mathbb{Z}, +)$ est un groupe.

Théorème :

- Une partie H de \mathbb{Z} est un sous-groupe de \mathbb{Z} si, et seulement si, il existe $c \in \mathbb{N}$ tel que $H = c\mathbb{Z}$
- Soit H un sous-groupe de $(\mathbb{Z}^n, +)$. Alors il existe $r \leq n$ tel que H est isomorphe à \mathbb{Z}^r .

Démonstration (du deuxième point) :

Par récurrence sur n :

- Pour $n = 1$: les sous-groupes de \mathbb{Z} sont les $c\mathbb{Z}$, $c \in \mathbb{N}$.

Si $c = 0$, $c\mathbb{Z}$ est isomorphe à \mathbb{Z}^0 , sinon $c\mathbb{Z}$ est isomorphe à \mathbb{Z} , un isomorphisme étant
$$\begin{matrix} \mathbb{Z} & \longrightarrow & c\mathbb{Z} \\ n & \longmapsto & cn \end{matrix}$$

- Soit $n \in \mathbb{N}$, supposons que pour tout $k \leq n$, si H est un sous-groupe de $(\mathbb{Z}^k, +)$, alors il existe $r \leq k$ tel que H est isomorphe à \mathbb{Z}^r .

Soit alors H un sous-groupe de \mathbb{Z}^{n+1} .

On considère $\varphi: \begin{matrix} \mathbb{Z}^{n+1} & \longrightarrow & \mathbb{Z} \\ (x_1, x_2, \dots, x_{n+1}) & \longmapsto & x_{n+1} \end{matrix}$, morphisme surjectif de groupe. Alors $\varphi(H)$ est un sous-groupe de $(\mathbb{Z}, +)$; il existe donc $c \in \mathbb{N}$ tel que $\varphi(H) = c\mathbb{Z}$.

1. Si $c = 0$, $H \subset \ker \varphi = \mathbb{Z}^n \times \{0\}$.

Par hypothèse de récurrence, H est donc isomorphe à un certain \mathbb{Z}^r où $r \leq n$.

En effet : Soit $\Pi: \begin{matrix} \mathbb{Z}^{n+1} & \longrightarrow & \mathbb{Z}^n \\ (x_1, x_2, \dots, x_{n+1}) & \longmapsto & (x_1, x_2, \dots, x_n) \end{matrix}$. Alors $\Pi|_{\mathbb{Z}^n \times \{0\}}$ est un isomorphisme.

Donc $H \sim \Pi(H)$ (\sim : isomorphe à). Or, $\Pi(H)$ est un sous-groupe de \mathbb{Z}^n , donc est isomorphe à \mathbb{Z}^r pour un certain $r \leq n$. Donc H est isomorphe à \mathbb{Z}^r .

2. Si $c > 0$:

Soit $v \in H$ tel que $\varphi(v) = c$. Alors, pour $h \in H$, $\frac{\varphi(h)}{c} = \alpha \in \mathbb{Z}$.

Ainsi, $\varphi(h - \alpha v) = \varphi(h) - \varphi(\alpha v) = \alpha c - \varphi(\alpha v) = 0$.

Donc $h - \alpha v \in \ker \varphi \cap H$. Posons $H' = \ker \varphi \cap H$.

Alors $H' \sim \mathbb{Z}^r$ pour un certain $r \leq n$ (d'après le cas $c = 0$)

Considérons maintenant l'application $u: H' \times \mathbb{Z} \rightarrow H$. Alors u est un morphisme.
 $(h', n) \mapsto h' + nv$
 u est surjectif : soit $h \in H$. Il existe alors $\alpha \in \mathbb{Z}$ tel que $h - \alpha v \in H'$. Ainsi, si on pose $h' = h - \alpha v$, on a $h = u(h', \alpha)$. u est injectif : si $u(h', n) = 0$, alors $h' + nv = 0$, donc $\varphi(h' + nv) = \underbrace{\varphi(h')}_{=0} + nc = 0$, d'où $n = 0$, puis $h' = 0$. Donc u est un isomorphisme, et H est isomorphe à \mathbb{Z}^{r+1} ($r + 1 \leq n + 1$), ce qui achève la récurrence.

Groupe des éléments inversibles d'un anneau unitaire Soit $(A, +, *)$ un anneau, d'élément unité 1_A .

On note $A^* = \{a \in A, \exists b \in A, a * b = b * a = 1_A\}$

Proposition :

$(A^*, *)$ est un groupe.

On note $\mathcal{M}_n(\mathbb{Z}) = \left\{ M = (m_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \in \mathcal{M}_n(\mathbb{R}), \forall (i, j) \in \llbracket 1, n \rrbracket^2, m_{i,j} \in \mathbb{Z} \right\}$

Alors $\mathcal{M}_n(\mathbb{Z})$ est un sous anneau de $(\mathcal{M}_n(\mathbb{R}), +, \times)$...

On peut alors noter $\mathcal{M}_n(\mathbb{Z})^* = \{M \in \mathcal{M}_n(\mathbb{Z}), \exists M' \in \mathcal{M}_n(\mathbb{Z}), MM' = M'M = I_n\}$

Soit $M \in \mathcal{M}_n(\mathbb{Z})$. On a alors l'équivalence : $M \in \mathcal{M}_n(\mathbb{Z})^* \iff \det M = \pm 1$

En effet : • Si $M \in \mathcal{M}_n(\mathbb{Z})^*$, Alors $(\det M)(\det M^{-1}) = \det I_n = 1$.

Le déterminant d'une matrice à coefficients dans \mathbb{Z} est dans \mathbb{Z} . Donc $\det M$ est inversible dans \mathbb{Z} .

Donc $\det M = \pm 1$.

• Si maintenant $\det M = \varepsilon$ avec $\varepsilon = \pm 1$:

On a $M^{-1} = \frac{{}^t \text{com}(M)}{\varepsilon}$.

Les coefficients de $\text{com}(M)$ sont entiers, donc ${}^t \text{com}(M) \in \mathcal{M}_n(\mathbb{Z})$.

Donc $M \in \mathcal{M}_n(\mathbb{Z})^*$

Groupes symétriques et alternés

Définition :

• \mathfrak{S}_n est l'ensemble des permutations de $\{1, \dots, n\}$. Ainsi, $\#\mathfrak{S}_n = n!$.

• Signature de $\sigma \in \mathfrak{S}_n$: $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$

Théorème :

• $\forall \sigma \in \mathfrak{S}_n, \varepsilon(\sigma) \in \{\pm 1\}$

Si σ est une transposition, alors $\varepsilon(\sigma) = -1$

• ε est un morphisme de groupe : $\varepsilon: (\mathfrak{S}_n, \circ) \rightarrow (\{\pm 1\}, \times)$

Définition :

$A_n = \ker \varepsilon$: groupe alterné.

A_n est donc un sous-groupe distingué de (\mathfrak{S}_n, \circ) , et $\#A_n = \frac{n!}{2}$ pour $n \geq 2$.

En effet : Posons $B_n = \{\sigma \in \mathfrak{S}_n, \varepsilon(\sigma) = -1\}$

On a ainsi $\mathfrak{S}_n = A_n \cup B_n$ et $A_n \cap B_n = \emptyset$

Posons $\tau = (1, 2)$.

Alors $A_n \xrightarrow{\sigma \mapsto \sigma \circ \tau} B_n$ est bijective (car involutive).

Donc $\#A_n = \#B_n$, d'où $\#A_n = \frac{n!}{2}$.

C) Puissance dans un groupe et applications

1) Cas des entiers naturels

Soit $(G, *)$ un groupe (il suffirait en fait que $*$ soit associative et admette un neutre)

Soit $g \in G$. On pose $\begin{cases} g^0 = e_G \\ \forall n \in \mathbb{N}, g^{n+1} = g^n * g \end{cases}$

Proposition :

Pour tous $n, m \in \mathbb{N}$, on a $g^{n+m} = g^n * g^m$.

Cas particulier (où $*$ = +) :

On note plutôt $e_G = 0$, et pour $g \in G$: $\begin{cases} 0.g = e_G = 0 \\ \forall n \in \mathbb{N}, (n+1).g = n.g + g \end{cases}$

2) Extension à \mathbb{Z}

Notation multiplicative On suppose ici que $(G, *)$. Pour $n \in \mathbb{Z} \setminus \mathbb{N}$, on pose $g^n = (g^{-1})^{-n}$.

Notation additive ...

Théorème :

Soit $(G, *)$ un groupe, et $g \in G$.

Alors $\sigma_g : (\mathbb{Z}, +) \xrightarrow{n \mapsto g^n} (G, *)$ est un morphisme de groupes.

3) Sous-groupe engendré par une partie

Théorème :

Soit $(G, *)$ un groupe, et A une partie de G .

- L'intersection des sous-groupes de G contenant A est un sous-groupe de G , noté $\text{gr}(A)$.
- $\text{gr}(A)$ est le plus petit sous-groupe de G contenant A .
- On a

$$\begin{aligned} \text{gr}(A) &= \left\{ a_1^{N_1} * a_2^{N_2} * \dots * a_p^{N_p}, N_i \in \mathbb{Z}, (a_1, \dots, a_p) \in A^p \right\} \quad (= H_1) \\ &= \left\{ a_1^{\varepsilon_1} * a_2^{\varepsilon_2} * \dots * a_p^{\varepsilon_p}, \varepsilon_i = \pm 1, (a_1, \dots, a_p) \in A^p \right\} \quad (= H_2) \end{aligned} \quad (5.2)$$

Démonstration :

Pour les deux premiers points : ok

Montrons que $\text{gr}(A) = H_1 = H_2$.

Déjà, $H_1 \subset H_2$, et $H_2 \subset \text{gr}(A)$.

Montrons maintenant que $\text{gr}(A) \subset H_1$. On va montrer que H_1 est un sous-groupe de G contenant A .

Déjà, $A \subset H_1$. De plus, H_1 est un sous-groupe de G : il est stable par produit et inverse, et contient e_G .

Définition :

- Si $\text{gr}(A) = G$, on dit que A est génératrice de G .
- Si $A = \{a\}$, $\text{gr}(A)$ s'appelle le groupe monogène engendré par a .
- Un groupe monogène fini s'appelle un groupe cyclique.

Proposition :

Soit $(G, *)$ un groupe, et $g \in G$.

Le groupe $\text{gr}(g)$ est l'image du morphisme $\sigma_g : \mathbb{Z} \longrightarrow G$.
 $n \longmapsto g^n$

4) Exemples

- $(\mathbb{Z}, +)$ est monogène, car $\mathbb{Z} = \text{gr}(\{1\})$ (notation additive)
- Soit $(a, b) \in \mathbb{N}^2$. Alors $\text{gr}(\{a, b\}) = (a \wedge b) \cdot \mathbb{Z}$
 En effet : $\text{gr}(\{a, b\}) = \{na + mb, (n, m) \in \mathbb{Z}^2\} = a\mathbb{Z} + b\mathbb{Z} = (a \wedge b) \cdot \mathbb{Z}$ (théorème de Bézout)
- (\mathcal{S}_n, \circ) est engendré par les transpositions.
- Rappel :

◇ Matrice de dilatation =
$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \end{pmatrix} = D_k(\lambda) \quad (C_k \rightarrow \lambda C_k)$$

Pour $A \in M_n(K)$,

$$D_k(\lambda) \times A = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \end{pmatrix} \times \begin{pmatrix} a_{1,1} & \cdots & \cdots & a_{1,n} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n,1} & & & a_{n,n} \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & \cdots & a_{1,n} \\ \vdots & \ddots & & \vdots \\ \lambda a_{k,1} & \cdots & \cdots & \lambda a_{k,n} \\ \vdots & & & \vdots \end{pmatrix} \tag{5.3}$$

◇ Matrice de transvection :

$$T_{i,j}(\lambda) = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \end{pmatrix} = I_n + \lambda E_{i,j} \tag{5.4}$$

$T_{i,j}(\lambda) \times A$: matrice obtenue en ajoutant à la i -ième ligne de A λ fois la j -ième ligne de A .

Théorème :

Soit \mathbb{K} un corps.

1. Toute matrice de déterminant 1 est produit de matrices $T_{i,j}(\lambda)$. Autrement dit, $\mathcal{SL}_n(\mathbb{K})$ est le sous-groupe de $\mathcal{M}_n(\mathbb{K})$ engendré par les $T_{i,j}(\lambda)$.
2. Toute matrice de déterminant non nul s'écrit $A' \times D_n(\lambda)$ où A' est une matrice de $\mathcal{SL}_n(\mathbb{K})$. En d'autres termes, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les $T_{i,j}(\lambda)$ et les $D_n(\mu)$.

Démonstration :

Voir méthode du pivot.

Pour $A \in \mathcal{GL}_n(\mathbb{K})$, il existe une suite d'opérations élémentaires du type « on ajoute à une ligne de

A une combinaison linéaire des autres » qui transforme A en $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & d \end{pmatrix}$ où $d = \det A$.

Comme ajouter à la ligne i λ fois la ligne j revient à remplacer A par $T_{i,j}(\lambda) \times A$, il existe donc une famille $(T_{i_k,j_k}(\lambda_k))_{k \in [1,m]}$ telle que :

$$T_{i_m,j_m}(\lambda_m) \times \cdots \times T_{i_1,j_1}(\lambda_1) \times A = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & d \end{pmatrix} = D_n(d) \quad (5.5)$$

Si $A \in \mathcal{SL}_n(\mathbb{K})$, on a $\det A = 1$, et donc :

$$A = [T_{i_m,j_m}(\lambda_m) \times \cdots \times T_{i_1,j_1}(\lambda_1)]^{-1} = T_{i_1,j_1}(-\lambda_1) \times \cdots \times T_{i_m,j_m}(-\lambda_m) \quad (5.6)$$

Donc A appartient au groupe engendré par les transvections.

De plus, $\forall i, j, \lambda, \det(T_{i,j}(\lambda)) = 1$.

Donc ce groupe est un sous-groupe de $\mathcal{SL}_n(\mathbb{K})$

Application :

Montrer que $\mathcal{SL}_n(\mathbb{R})$ est connexe par arcs.

Soit $A \in \mathcal{SL}_n(\mathbb{R})$.

On va trouver $\varphi: [0; 1] \rightarrow \mathcal{SL}_n(\mathbb{R})$ continue telle que $\varphi(0) = I_n$ et $\varphi(1) = A$.

Comme $A \in \mathcal{SL}_n(\mathbb{R})$, A s'écrit sous la forme $T_{i_1,j_1}(\lambda_1) \times \cdots \times T_{i_m,j_m}(\lambda_m)$.

On pose alors $\varphi(t) = T_{i_1,j_1}(t\lambda_1) \times \cdots \times T_{i_m,j_m}(t\lambda_m)$.

On a, pour tout $t \in [0; 1]$, $\det(\varphi(t)) = 1$, $\varphi(0) = I_n$ et $\varphi(1) = A$.

De plus, φ est continue car $\varphi(t)$ est une matrice dont les coefficients dépendent polynomialement de t .

(ou : l'application $\mathcal{M}_n(\mathbb{R})^2 \rightarrow \mathcal{M}_n(\mathbb{R})$ est continue car bilinéaire en dimension finie)
 $(A, B) \mapsto AB$

Donc $\mathcal{SL}_n(\mathbb{R})$ est connexe par arcs.

Remarque :

$\mathcal{GL}_n(\mathbb{R})$ n'est pas connexe par arcs car sinon $\det(\mathcal{GL}_n(\mathbb{R})) = \mathbb{R}^*$ serait connexe par arcs.

III Théorie des anneaux commutatifs

A) Catégorie des anneaux

1) Définition

Définitions Anneaux (toujours unitaires, parfois commutatifs), morphismes d'anneaux, sous-anneaux...

Attention : Pour un morphisme d'anneaux, on a $\varphi(1) = 1$.

Un sous-anneau contient 1 (exemple : $2\mathbb{Z}$ n'est pas un sous-anneau de \mathbb{Z})

2) Idéal d'un anneau commutatif

Définition :

Soit $(A, +, \times)$ un anneau commutatif.

Soit I une partie de A .

On dit que I est un idéal de A si :

- $(I, +)$ est un sous-groupe de $(A, +)$
- $\forall a \in A, \forall i \in I, ai \in I$ (on a alors aussi $ia = ai \in I$)

Remarque :

Si A n'est pas commutatif, on a toujours les notions d'idéal à gauche/droite/bilatère : $\forall a \in A, \forall i \in I, ai \in I/ia \in I/ia \in I$ et $ai \in I$

Exemple :

Idéal principal engendré par $a \in A : aA = \{ax, x \in A\}$.

Théorème :

Soit A une partie de \mathbb{Z} . Les conditions suivantes sont équivalentes :

- (1) A est un sous-groupe de $(\mathbb{Z}, +)$
- (2) A est un idéal de $(\mathbb{Z}, +, \times)$
- (3) $\exists n \in \mathbb{N}, A = n\mathbb{Z}$.

En particulier, tout idéal de \mathbb{Z} est principal.

Démonstration :

On a déjà vu que (1) \implies (3), (3) \implies (2) est vrai, c'est l'idéal principal de \mathbb{Z} engendré par n . et (2) \implies (1) aussi (par définition d'un idéal).

Remarque :

Il existe des idéaux non principaux.

Exemple :

$A = (\mathbb{Z}[X], +, \times)$ est un sous-anneau de $\mathbb{R}[X]$.

Mais $I = 3\mathbb{Z}[X] + X\mathbb{Z}[X]$ est un idéal non principal.

3) Divisibilité dans un anneau commutatif

Définition :

Soit $(A, +, \times)$ un anneau commutatif.

Soient $x, y \in A$.

On dit que x divise y (ou que y est un multiple de x) s'il existe $z \in A$ tel que $y = zx$.

Proposition :

Soient $(A, +, \times)$ un anneau commutatif, et $x, y \in A$.

Les conditions suivantes sont équivalentes :

1. x divise y .
2. y est un multiple de x
3. $y \in xA$
4. $yA \subset xA$

Exemple :

Les diviseurs de 1 sont les éléments inversibles de A .

Diviseurs (non nuls) de 0 :

On dit que x divise 0 lorsque $x \neq 0$ et $\exists y \in A \setminus \{0\}, xy = 0$.

Un anneau sans diviseur de 0 est dit intègre.

Exemples

- $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre ($\dot{2} \times \dot{2} = \dot{0}$)
- $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, a, b \in \mathbb{R} \right\}$ est commutatif unitaire, mais non intègre :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \tag{5.7}$$

4) Éléments remarquables d'un anneau

1. les éléments inversibles forment un sous-groupe pour \times ...
2. Outil important : soit $(A, +, *)$ un anneau.

Pour étudier $a \in A$, on a intérêt à étudier les applications :

$$\begin{array}{ccc} \delta_a : A & \longrightarrow & A & \text{et} & \gamma_a : A & \longrightarrow & A \\ x & \longmapsto & a * x & & x & \longmapsto & x * a \end{array} .$$

Proposition :

δ_a et γ_a sont des endomorphismes du groupe $(A, +)$ (mais pas d'anneaux)

Exemple (on suppose A commutatif) :

δ_a n'est pas injectif $\iff a$ est un diviseur de 0.

δ_a est bijective $\iff a$ est inversible.

Définition :

3. Un élément a non nul non inversible de A est dit irréductible (indécomposable) si $\forall b, c \in A, a = bc \implies b \in A^*$ ou $c \in A^*$
 Un élément a est dit premier lorsque $\forall b, c \in A, a|bc \implies a|b$ ou $a|c$.

Exemple :

- Dans \mathbb{Z} , un nombre est premier si et seulement si il est irréductible.
- Soit $A = \{a + ib\sqrt{6}, a, b \in \mathbb{Z}\}$

Alors : A est un anneau, 2 est irréductible non premier.

En effet : Déjà, A est un sous-anneau de $(\mathbb{C}, +, \times)$

$$A^* = \{-1; 1\} :$$

1 et -1 sont inversible donc déjà $\{-1; 1\} \subset A^*$.

Soit $z \in A^*$.

Il existe alors $z' \in A$ tel que $zz' = 1$, disons $z = a + ib\sqrt{6}, z' = a' + ib'\sqrt{6}$

Alors $(a^2 + 6b^2)(a'^2 + 6b'^2) = 1$ (par passage au module)

Donc $a^2 + 6b^2 = \pm 1$ (et $a'^2 + 6b'^2 = \pm 1$)

Donc $a^2 + 6b^2 = 1$. Donc $a = \pm 1$ et $b = 0$.

Donc $z = \pm 1$. Donc $A^* = \{-1; 1\}$.

Maintenant :

Soient $z, z' \in A$, supposons que $zz' = 2$.

Alors $(|z||z'|)^2 = 4$, soit $(a^2 + 6b^2)(a'^2 + 6b'^2) = 4$

◊ 1^{er} cas : $a^2 + 6b^2 = a'^2 + 6b'^2 = 2$: impossible

◊ 2^{ème} cas : $a^2 + 6b^2 = 1$; z est inversible.

◊ 3^{ème} cas : $a'^2 + 6b'^2 = 1$; z' est inversible.

Mais 2 n'est pas premier :

On a $2 \times 3 = -(i\sqrt{6})^2$. Donc $2|(i\sqrt{6})^2$.

Si 2 était premier, on aurait $2|i\sqrt{6}$ ce qui est faux :

Sinon, il existe $z = a + ib\sqrt{6}$ tel que $2z = i\sqrt{6}$, alors $2a + 2ib\sqrt{6} = i\sqrt{6}$, donc $a = 0$ et $b = \frac{1}{2}$, donc $z = \frac{i\sqrt{6}}{2} \notin A$.

B) Exemples d'anneaux et de corps

$(\mathbb{Z}, +, \times), \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux (et même des corps pour les trois derniers)

\mathbb{N} n'est pas un anneau (ni un corps)

Soit E un ensemble, on munit $\mathcal{P}(E)$ de Δ et \cap ($A\Delta B = A \cup B \setminus A \cap B$: différence symétrique).

Alors $\mathcal{P}(E)$ est un anneau (même une algèbre, appelée algèbre de Boole)

(montrer que $\chi_{A\Delta B} = \chi_A + \chi_B, \chi_{A \cap B} = \chi_A \times \chi_B$ où $\chi_A : E \longrightarrow \mathbb{Z}/2\mathbb{Z}$)

$$x \longmapsto \begin{cases} \bar{1} & \text{si } x \in A \\ \bar{0} & \text{sinon} \end{cases}$$

$\mathbb{Q}[i] = \{a + ib, a, b \in \mathbb{Q}\}$ est un sous-corps de \mathbb{C} .

$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est un anneau, l'anneau des entiers de Gauss.

Extension On dit que $x \in \mathbb{C}$ est algébrique lorsqu'il existe $P \in \mathbb{Q}[X] \setminus \{0\}$ tel que $P(x) = 0$.

Exemple :

$i, \sqrt{2}$ sont algébriques, π et e ne le sont pas (ils sont transcendants)

Proposition (hors programme) :

Soit $a \in \mathbb{C}$, algébrique.

On pose $\mathbb{Q}[a] = \left\{ \sum_{j=0}^n \alpha_j a^j, n \in \mathbb{N}, \alpha_j \in \mathbb{Q} \right\} = \{R(a), R \in \mathbb{Q}[X]\}$.

Alors :

1. $\mathbb{Q}[a]$ est un sous-corps de \mathbb{C} .
2. $\mathbb{Q}[a]$ est une \mathbb{Q} -algèbre de dimension finie.

Démonstration :

Comme a est algébrique, il existe $P_0 \in \mathbb{Q}[X] \setminus \{0\}$ tel que $P_0(a) = 0$, disons $P_0 = X^d + c_{d-1}X^{d-1} + \dots + c_0$

$\mathbb{Q}[a]$ est une sous-algèbre de la \mathbb{Q} -algèbre $(\mathbb{C}, +, \times, \cdot)$.

$(\cdot : \text{restriction du produit à } \mathbb{Q} \times \mathbb{C})$.

$\mathbb{Q}[a]$ est de dimension finie : elle est engendrée par $(1, a, \dots, a^{d-1})$ où $d = \deg P_0$:

Soit $z = R(a) \in \mathbb{Q}[a]$

La division euclidienne de R par P_0 donne $R = P_0Q + S$ où $\deg S < d$.

Donc $z = S(a) = \sum_{i=0}^{d-1} x_i a^i$, donc est combinaison linéaire de $(1, a, \dots, a^{d-1})$.

Montrons que $\mathbb{Q}[a]$ est un sous-corps de \mathbb{C} . Pour cela, montrons que tout élément x_0 non nul de $\mathbb{Q}[a]$ est inversible dans $\mathbb{Q}[a]$: Soit $x_0 \in \mathbb{Q}[a]$.

Posons $\varphi: \mathbb{Q}[a] \rightarrow \mathbb{Q}[a]$.
 $y \mapsto x_0 y$

Alors $\varphi \in \mathcal{L}_{\mathbb{Q}}(\mathbb{Q}[a])$.

$$\ker \varphi = \{y \in \mathbb{Q}[a], x_0 y = 0\} = \{0\} \tag{5.8}$$

Donc φ est injective, donc bijective (car $\mathbb{Q}[a]$ est de dimension finie)

Donc φ est un automorphisme, donc surjectif.

Comme $1 \in \mathbb{Q}[a]$, x_0 est inversible.

Construction d'anneaux et de corps On parle ici d'anneaux commutatifs

- Anneau produit :

Si A_1, A_2 sont deux anneaux, $A_1 \times A_2$ n'est jamais intègre : $(0, 1) \times (1, 0) = (0, 0)$

- Soit A un anneau.

$A[X]$: ensemble des polynômes à une indéterminée à coefficients dans A .

Attention : Si A n'est pas intègre, on n'a pas en général $\deg(PQ) = \deg(P) + \deg(Q)$.

On peut itérer : $A[X]$ étant un anneau, $(A[X])[Y]$ sera noté plutôt $A[X, Y]$.

- Soit \mathbb{K} un corps.

On définit le corps $\mathbb{K}(X)$ des fractions rationnelles en l'indéterminée X .

De même que précédemment, $(\mathbb{K}(X))(Y)$ sera noté plutôt $\mathbb{K}(X, Y)$.

C) Congruences modulo n dans \mathbb{Z} , anneau quotient $\mathbb{Z}/n\mathbb{Z}$

Définition :

Pour $a, b \in \mathbb{Z}$, $a \equiv b \pmod n \iff n|b - a$.

Théorème :

La relation de congruence est une relation d'équivalence compatible avec $+$ et \times (de \mathbb{Z})

Démonstration :

Compatibilité de $+$

$$\forall (x, x', y, y') \in \mathbb{Z}^4, \left. \begin{array}{l} x \equiv x' \pmod n \\ y \equiv y' \pmod n \end{array} \right\} \implies x + y \equiv x' + y' \pmod n \quad (5.9)$$

Compatibilité de \times Soit $(x, x', y, y') \in \mathbb{Z}^4$ tel que $x \equiv x' \pmod n$, $y \equiv y' \pmod n$

Il existe alors $k \in \mathbb{Z}$ tel que $x - x' = kn$, et $l \in \mathbb{Z}$ tel que $y - y' = ln$.

Alors $xy - x'y' = \dots = n(ky' + lx' + nkl)$, donc $xy \equiv x'y' \pmod n$.

Plus généralement Soit A un anneau, I un idéal de A .

On définit \mathcal{R} sur A par : $x\mathcal{R}y \iff x - y \in I$.

Alors \mathcal{R} est une relation d'équivalence, compatible avec $+$ et \times (de A)

Notation :

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences modulo n . On note \bar{x} la classe de x . ($\bar{x} = x + n\mathbb{Z}$)

Exemple :

Avec $n = 4$:

$$\mathbb{Z}/4\mathbb{Z} = \{\bar{0} = 4\mathbb{Z}, \bar{1} = 1 + 4\mathbb{Z}, \bar{2} = 2 + 2\mathbb{Z}, \bar{3} = 3 + 3\mathbb{Z}\} \subset \mathcal{P}(\mathbb{Z}).$$

On définit deux relations binaires entre $\mathbb{Z}/n\mathbb{Z}^2$ et $\mathbb{Z}/n\mathbb{Z}$:

$$\mathcal{R}_+ : \forall (a, b, c) \in \mathbb{Z}/n\mathbb{Z}^3, (a, b)\mathcal{R}_+c \iff \exists x \in a, \exists y \in b, c = \overline{x + y} \quad (5.10)$$

$$\mathcal{R}_\times : \forall (a, b, c) \in \mathbb{Z}/n\mathbb{Z}^3, (a, b)\mathcal{R}_\times c \iff \exists x \in a, \exists y \in b, c = \overline{x \times y} \quad (5.11)$$

Théorème :

Soit $n \geq 2$.

1. \mathcal{R}_+ et \mathcal{R}_\times sont des applications de $\mathbb{Z}/n\mathbb{Z}^2$ dans $\mathbb{Z}/n\mathbb{Z}$.

On les note $a_+ : (a, b) \mapsto a +_n b$, $a_\times : (a, b) \mapsto a \times_n b$.

2. $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ est un anneau

3. Soit $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique de \mathbb{Z} sur $\mathbb{Z}/n\mathbb{Z}$.

$$x \longmapsto \bar{x}$$

Alors π_n est un morphisme surjectif d'anneaux de $(\mathbb{Z}, +, \times)$ dans $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ et de noyau $n\mathbb{Z}$.

4. $\pi_n|_{\llbracket 0, n-1 \rrbracket}$ est bijective, et ainsi $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n .

Démonstration :

1. Pour \mathcal{R}_+ , on doit vérifier que tout couple de la source est en relation avec un unique c du but.

Soit $(a, b) \in \mathbb{Z}/n\mathbb{Z}^2$.

Existence Comme $a, b \in \mathbb{Z}/n\mathbb{Z}$, il existe $x, y \in \mathbb{Z}$ tels que $\bar{x} = a, \bar{y} = b$.

Alors, par définition de $\mathcal{R}_+, (a, b)\mathcal{R}_+ \overline{x+y}$

Unicité Supposons que $(a, b)\mathcal{R}_+ c$ et $(a, b)\mathcal{R}_+ c'$.

Il existe alors $(x, y) \in \mathbb{Z}^2$ tel que $a = \bar{x}, b = \bar{y}$ et $c = \overline{x+y}$.

De même, il existe $(x', y') \in \mathbb{Z}^2$ tel que $a = \bar{x}', b = \bar{y}'$ et $c' = \overline{x'+y'}$.

On a $x \equiv x' \pmod n, y \equiv y' \pmod n$. Donc $x + y \equiv x' + y' \pmod n$, c'est-à-dire $c = c'$.

2. Éléments de réponse :

Neutre pour $+_n : \bar{0}$.

Pour $a \in \mathbb{Z}/n\mathbb{Z}$, il existe $x \in \mathbb{Z}$ tel que $\bar{x} = a$, et on a $a +_n \bar{0} = \overline{x+0} = \bar{x} = a$.

Neutre pour $\times_n : \bar{1}$.

3. π_n est un morphisme d'anneaux par définition de $+_n$ et \times_n :

$$\pi_n(x + y) = \overline{x + y} = \bar{x} +_n \bar{y} = \pi_n(x) +_n \pi_n(y) \quad (5.12)$$

4. Faire une division euclidienne.

Exemple :

Quels sont les deux derniers chiffres de $N = 3^{2005}$?

On note a_1, a_0 ces deux derniers chiffres. Ainsi, $N \equiv 10a_1 + a_0 \pmod{100}$.

Remarque :

$$x \equiv y \pmod{100} \iff 4 \times 25 | x - y \iff 4 | x - y \text{ et } 25 | x - y \iff x \equiv y \pmod{4} \text{ et } x \equiv y \pmod{25} \quad (5.13)$$

(Car $4 \wedge 25 = 1$)

On cherche donc $Cl_4(N)$ et $Cl_{25}(N)$.

• modulo 4 :

$$\bar{N} = \bar{3}^{2005} = \bar{-1}. \text{ Donc } N \equiv -1 \pmod{4}.$$

• modulo 25 :

$$\bar{N} = \bar{3}^{2005} \quad (5.14)$$

$$\bar{3}^0 = \bar{1} \quad \bar{3}^1 = \bar{3} \quad \bar{3}^2 = \bar{9} \quad \bar{3}^3 = \bar{2} \quad \bar{3}^4 = \bar{6} \quad \bar{3}^5 = \bar{18} = \bar{-7} \quad (5.15)$$

$$\bar{3}^6 = \bar{-21} = \bar{4} \quad \bar{3}^7 = \bar{12} \quad \bar{3}^8 = \bar{11} \quad \bar{3}^9 = \bar{8} \quad \bar{3}^{10} = \bar{-1} \quad \bar{3}^{20} = (\bar{3}^{10})^2 = \bar{1} \quad (5.16)$$

Division euclidienne de 2005 par 20 :

$$2005 = 20 \times 100 + 5.$$

$$\text{Donc } \bar{3}^{2005} = \bar{3}^5 = \bar{-7}.$$

$$\text{Donc } N \equiv -7 \pmod{25}$$

• modulo 100 :

Avec une méthode simple :

$$18 \equiv -7 \pmod{25} \text{ mais } 18 \not\equiv -1 \pmod{4}$$

$18 + 25 \equiv 43 \equiv 18 \pmod{25}$ et $43 \equiv -1 \pmod{4}$. Donc 4 et 3 sont les deux chiffres cherchés.

D) Propriétés de structure de $\mathbb{Z}/n\mathbb{Z}$

Théorème :

Soit $n \geq 2$. Alors :

1. $(\mathbb{Z}/n\mathbb{Z}, +_n)$ est un groupe cyclique
2. Soit $x \in \mathbb{Z}$. Les conditions suivantes sont équivalentes :
 - $x \wedge n = 1$ dans \mathbb{Z} .
 - \bar{x} est un élément inversible de $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$
 - $\{\bar{x}\}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +_n)$.

Démonstration :

1. $\bar{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$.
2. On a :

$$\begin{aligned}
 x \wedge n = 1 &\iff \exists(u, v) \in \mathbb{Z}, ux + vn = 1 \\
 &\iff \exists(u, v) \in \mathbb{Z}, ux \equiv 1 \pmod{n} \\
 &\iff \bar{x} \in \mathbb{Z}/n\mathbb{Z}^*
 \end{aligned}
 \tag{5.17}$$

D'où déjà l'équivalence entre les deux premiers tirets.

Supposons que \bar{x} est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$.

Il existe alors $y \in \mathbb{Z}$ tel que $\bar{x} \times_n \bar{y} = \bar{1}$. On peut supposer que $y \in \mathbb{N}$.

Ainsi, $\bar{y}\bar{x} = \bar{1}$, donc $y \cdot \bar{x} = \bar{1}$.

Donc $\bar{1} \in \text{gr}(\{\bar{x}\})$.

Donc $\mathbb{Z}/n\mathbb{Z} = \text{gr}(\{\bar{x}\})$ (car $\bar{1}$ est générateur de $\mathbb{Z}/n\mathbb{Z}$)

Si maintenant $\{\bar{x}\}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +_n)$, alors il existe $y \in \mathbb{N}$ tel que $\bar{1} = y \cdot \bar{x}$, et donc $\bar{1} = \bar{y} \times_n \bar{x}$.

Donc \bar{x} est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

D'où les trois équivalences.

Corollaire :

Soit $n \geq 2$. Les conditions suivantes sont équivalentes :

- (1) n est premier
- (2) $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ est un corps.
- (3) $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ est un anneau intègre.

Démonstration :

(1) \implies (2) Soit $y \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{\bar{0}\}$.

Il existe alors $p \notin n\mathbb{Z}$ tel que $y = \bar{p}$.

Or, n est premier, et ne divise pas p . Donc $p \wedge n = 1$.

Donc $y = \bar{p}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

(2) \implies (3) ok

(3) \implies (1) montrons la contraposée :

Supposons non(1). Alors $n = a \times b$ où $a, b \geq 2$

Donc $\bar{0} = \bar{a} \times \bar{b}$, et $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ car $n|a$ et $n|b$.

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

En général, on note plutôt $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ que $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$.

Notation :

Si p est premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, noté \mathbb{F}_p : corps de Galois de cardinal p .

Pour $n \in \mathbb{N}$, on pose $\varphi(n) = \#((\mathbb{Z}/n\mathbb{Z})^*)$.

φ s'appelle la fonction indicatrice d'Euler.

Alors :

- $\forall n \geq 2, \varphi(n) = \# \{k \in [1, n], k \wedge n = 1\}$
- $\varphi(n)$ est aussi le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.
- $\forall n \geq 2, \varphi(n) \leq n - 1$, et il y a égalité si et seulement si n est premier.

Pour prolonger φ , on pose $\varphi(1) = 1$.

E) Passage au quotient modulo n .

Problème Soit $(G, *)$ un groupe, et $\sigma : (\mathbb{Z}, +) \rightarrow (G, *)$ un morphisme de groupe.

Existe-t-il φ morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(G, *)$ tel que $\sigma = \varphi \circ \pi_n$ (« σ peut-il se factoriser par π_n ? ») :

$$\begin{array}{ccc}
 (\mathbb{Z}, +) & \xrightarrow{\sigma} & (G, *) \\
 & \searrow \pi_n & \nearrow \varphi \\
 & (\mathbb{Z}/n\mathbb{Z}, +) &
 \end{array}
 \tag{5.18}$$

Théorème (pour les groupes) :

Soit $(G, *)$ un groupe. Alors σ se factorise par π_n si, et seulement si, $\sigma(n) = e_G$, c'est-à-dire si et seulement si $n\mathbb{Z} \subset \ker \sigma$.

Démonstration :

- Condition nécessaire :

Si $\sigma = \varphi \circ \pi_n$, alors $\sigma(n) = \varphi \circ \pi_n(n) = \varphi(\bar{0}) = e_G$ (car φ est un morphisme)

- Condition suffisante :

Supposons que $n\mathbb{Z} \subset \ker \sigma$.

On considère la relation binaire \mathcal{R} de source $\mathbb{Z}/n\mathbb{Z}$ et de but G définie par :

$$\forall (a, g) \in \mathbb{Z}/n\mathbb{Z} \times G, a\mathcal{R}g \iff \exists p \in \mathbb{Z}, a = \bar{p} \text{ et } g = \sigma(p)
 \tag{5.19}$$

Montrons que \mathcal{R} est une application :

Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$, a s'écrit \bar{p} , et a a au moins une image, à savoir $g = \sigma(p)$.

Unicité : si $a\mathcal{R}y$ et $a\mathcal{R}y'$, alors il existe $p, p' \in \mathbb{Z}$ tels que $a = \bar{p}$ et $a = \bar{p}'$, et $y = \sigma(p)$ et $y' = \sigma(p')$.

Alors il existe $k \in \mathbb{Z}$ tel que $p' = p + kn$.

Donc $y' = \sigma(p + kn) = \sigma(p) = y$.

Donc \mathcal{R} est une application. De plus, c'est un morphisme de groupes (...)

Ainsi, σ se factorise par π_n , et $\sigma = \mathcal{R} \circ \pi_n$.

Problème Soit $(A, +, \times)$ un anneau, $\sigma: (\mathbb{Z}, +, \times) \rightarrow (A, +, \times)$.

Existe-t-il $\varphi: (\mathbb{Z}/n\mathbb{Z}, +, \times) \rightarrow (A, +, \times)$ morphisme d'anneau tel que $\sigma = \varphi \circ \pi_n$?

Théorème (pour les anneaux) :

σ se factorise par π_n si et seulement si $\sigma(n) = 0_A$, c'est-à-dire si et seulement si $n\mathbb{Z} \subset \ker \sigma$.

Démonstration :

- Condition nécessaire : ok
- Condition suffisante :

On peut déjà définir $\varphi: (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (A, +)$ morphisme de groupes tel que $\sigma = \varphi \circ \pi_n$.

Il reste à vérifier que $\forall (a, b) \in \mathbb{Z}/n\mathbb{Z}^2, \varphi(ab) = \varphi(a) \times \varphi(b)$ et $\varphi(\bar{1}) = 1_A$.

Déjà, $\varphi(\bar{1}) = \sigma(1) = 1_A$.

Soit $(a, b) \in \mathbb{Z}/n\mathbb{Z}^2$, disons $a = \bar{p}, b = \bar{q}$.

Alors $\varphi(ab) = \varphi(\overline{pq}) = \sigma(pq) = \sigma(p)\sigma(q) = \varphi(\bar{p})\varphi(\bar{q}) = \varphi(a)\varphi(b)$.

Généralisation (hors programme)

Groupe quotient Soit $(G, *)$ un groupe, H un sous-groupe de G .

On définit dans G deux relations binaires \mathcal{R}_H et ${}_H\mathcal{R}$ par :

$$\forall (x, y) \in G^2, x\mathcal{R}_H y \iff x * y^{-1} \in H \quad (5.20)$$

$$\forall (x, y) \in G^2, x{}_H\mathcal{R} y \iff y^{-1} * x \in H \quad (5.21)$$

Alors \mathcal{R}_H et ${}_H\mathcal{R}$ sont des relations d'équivalence (...)

Théorème :

Les propriétés suivantes sont équivalentes :

- (1) H est un sous-groupe distingué de G .
- (2) \mathcal{R}_H est compatible avec $*$.
- (3) ${}_H\mathcal{R}$ est compatible avec $*$.
- (4) $\mathcal{R}_H = {}_H\mathcal{R}$.
- (5) Il existe une lci \mathcal{T} sur G/\mathcal{R}_H telle que $(G, \times) \longrightarrow (G/\mathcal{R}_H, \mathcal{T})$ soit un morphisme.
 $g \longmapsto \mathcal{C}l_{\mathcal{R}_H}(g)$
- (6) Il existe une lci \mathcal{T} sur $G/{}_H\mathcal{R}$ telle que $(G, \times) \longrightarrow (G/{}_H\mathcal{R}, \mathcal{T})$ soit un morphisme.
 $g \longmapsto \mathcal{C}l_{{}_H\mathcal{R}}(g)$

Corollaire :

Une partie A de $(G, *)$ est un sous-groupe distingué si et seulement si il existe un morphisme de groupe $\varphi: (G, *) \rightarrow (G', *')$ de noyau A .

Démonstration (du théorème) :

- Déjà, (1) \implies (2) :
Soient $(x, y), (x', y') \in G^2$, supposons que $x\mathcal{R}_Hy$ et $x'\mathcal{R}_Hy'$.
Alors $xy^{-1} \in H$, et $x'y'^{-1} \in H$.
Comme $x'y'^{-1} \in H$ (et $x \in G$) et H est distingué, on a $x(x'y'^{-1})x^{-1} \in H$.
Comme de plus $xy^{-1} \in H$, on a $(x(x'y'^{-1})x^{-1})(xy^{-1}) \in H$,
c'est-à-dire par associativité $(xx')(y'^{-1}y^{-1}) = (xx')(yy')^{-1} \in H$
- De plus, on a aussi (2) \implies (5) (...)
- (5) \implies (1) : si $g \mapsto Cl(g)$ pour \mathcal{R}_H est un morphisme, son noyau qui est $\ker \varphi = Cl(e_G) = H$ est distingué.
- De même, (1) \implies (3) \implies (6) \implies (1).
- Enfin, (1) \implies (4).

Pour les anneaux (commutatifs) Soit I un idéal de $(A, +, \times)$.

On définit \mathcal{R} par : $\forall(x, y) \in A^2, x\mathcal{R}y \iff x - y \in I$

Théorème :

1. \mathcal{R} est une relation d'équivalence, compatible avec $+$ et \times .
2. On peut munir A/\mathcal{R} (qu'on note A/I) de deux lois $+_I$ et \times_I telles que $(A/I, +_I, \times_I)$ est un anneau et $\pi : A \rightarrow A/I$ (projection canonique) est un morphisme surjectif de noyau I .

Conséquence :

I est un idéal de A si, et seulement si c'est le noyau d'un morphisme d'anneau $A \rightarrow B$.

Pour les groupes Soit $(G, *)$ un groupe, et H un sous-groupe distingué.

Soit σ un morphisme de $(G, *)$ dans un groupe $(G', *')$.

Existe-t-il φ morphisme de groupe tel que $\sigma = \varphi \circ \pi$?

$$\begin{array}{ccc}
 (G, *) & \xrightarrow{\sigma} & (G', *') \\
 & \searrow \pi & \nearrow \varphi \\
 & (G/H, \mathcal{T}) &
 \end{array}
 \tag{5.22}$$

Oui si et seulement si $H \subset \ker \sigma$.

Énoncé analogue pour les anneaux

IV Application des anneaux $\mathbb{Z}/n\mathbb{Z}$

A) Au groupe monogène

Théorème :

Soit $(G, *)$ un groupe, et $g \in G$.

- (1) $\sigma_g : n \in (\mathbb{Z}, +) \mapsto g^n \in (G, *)$ est un morphisme de groupes d'image $\text{gr}(g)$, sous-groupe engendré par $\{g\}$.

- (2) Si σ_g est injectif, c'est un isomorphisme entre $(\mathbb{Z}, +)$ et $\text{gr}(g)$.
- (3) Si σ_g n'est pas injectif, alors :
- Il existe $n \geq 1$ tel que $\ker \sigma_g = n\mathbb{Z}$.
 - σ_g passe au quotient par $n\mathbb{Z}$, c'est-à-dire qu'il existe un morphisme $\bar{\sigma}_g: (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (G, *)$ tel que $\forall x \in \mathbb{Z}, \sigma_g(x) = \bar{\sigma}_g(\mathcal{C}_n(x))$
 - $\bar{\sigma}_g$ est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\text{gr}(g), *)$.

Démonstration :

- (2) si σ_g est injectif, c'est un isomorphisme entre sa source et son image $(\text{gr}(g), *)$
 - (3) si σ_g n'est pas injectif :
 - ◊ $\ker \sigma_g$ est un sous-groupe de $(\mathbb{Z}, +)$, non réduit à $\{0\}$, donc de la forme $n\mathbb{Z}$.
 - ◊ D'après le théorème de passage au quotient par $n\mathbb{Z}$, comme $n\mathbb{Z} \subset \ker \sigma_g$, σ_g passe au quotient par $n\mathbb{Z}$.
 - ◊ On sait que $\bar{\sigma}_g$ est un morphisme surjectif.
- Étude de $\ker \bar{\sigma}_g$: soit $a \in \mathbb{Z}/n\mathbb{Z}$, supposons que $\bar{\sigma}_g(a) = e_G$.
 Soit $x \in \mathbb{Z}$ tel que $\mathcal{C}_n(x) = a$. On a alors $\bar{\sigma}_g(a) = \sigma_g(x) = e_G$.
 Donc $x \in n\mathbb{Z}$, soit $a = \bar{0}$. Donc $\bar{\sigma}_g$ est injectif.

Corollaire (classification des groupes monogènes) :

1. Tout groupe monogène non fini est isomorphe à $(\mathbb{Z}, +)$.
2. Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration :

1. On applique le théorème précédent avec $G = \text{gr}(g)$ et σ_g est injectif.
2. Soit $G = \text{gr}(g)$ cyclique tel que $\#G = n$.
 Alors $\sigma_g: m \in (\mathbb{Z}, +) \mapsto g^m \in (G, *)$ n'est pas injectif car \mathbb{Z} est infini.
 Donc $\ker \sigma_g = m\mathbb{Z}$, pour $m \geq 1$. Donc σ_g passe au quotient en un isomorphisme $\bar{\sigma}_g: (\mathbb{Z}/m\mathbb{Z}, +) \rightarrow (G, *)$. Comme $\bar{\sigma}_g$ est une bijection, $m = n$.

Exemple :

Le groupe des racines n -ièmes de l'unité (μ_n, \times)

$$\mu_n = \{z \in \mathbb{C}, z^n = 1\}.$$

μ_n est un sous-groupe de (\mathbb{C}^*, \times) , noyau du morphisme $z \mapsto z^n$, et $\#\mu_n = n$.

Proposition :

(μ_n, \times) est un groupe cyclique, et $\omega_k = e^{\frac{2ik\pi}{n}}$ engendre μ_n si et seulement si $k \wedge n = 1$, c'est-à-dire si et seulement si $\forall p \in \{1, \dots, n-1\}, \omega_k^p \neq 1$.

Définition :

Un tel ω_k est une racine primitive n -ième de l'unité.

Démonstration :

Soit $\omega = e^{\frac{2i\pi}{n}}$. On a $\text{gr}(\omega) = \mu_n$ car $\forall k \in \llbracket 0, n-1 \rrbracket, \omega_k = \omega^k$.

Donc μ_n est cyclique.

Soit $\sigma: (\mathbb{Z}, +) \longrightarrow (\mu_n, \times)$ morphisme surjectif.
 $k \longmapsto \omega^k$

Alors μ_n passe au quotient par $\bar{\sigma}: (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (\mu_n, \times)$, isomorphisme.

Or, $\forall k \in \llbracket 0, n-1 \rrbracket, \omega^k = \sigma(k) = \bar{\sigma}(\text{Cl}_n(k))$.

Donc ω_k engendre μ_n si et seulement si $\text{Cl}_n(k)$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$, c'est-à-dire si et seulement si $k \wedge n = 1$.

Montrons maintenant que $k \wedge n = 1 \iff \forall p \in \{1, \dots, n-1\}, \omega_k^p \neq 1$

Supposons que $k \wedge n = 1$. Soit $p \in \mathbb{Z}$ tel que $\omega_k^p = 1$, c'est-à-dire $e^{\frac{2ipk\pi}{n}} = 1$.

Alors $n|pk$, donc d'après le théorème de Gauss $n|p$.

Supposons que $k \wedge n = d \geq 2$.

Soit k' tel que $k'd = k$, n' tel que $n'd = n$ ($n' \in \llbracket 1, n-1 \rrbracket$).

Alors $\omega_k^{n'} = e^{\frac{2ikn'\pi}{n}} = e^{2ik'\pi} = 1$.

B) Ordre d'un élément (hors programme)

Définition :

Soit $(G, *)$ un groupe, $g \in G$ et $\sigma_g: n \mapsto g^n$.

1. Si σ_g est injectif, on dit que g est d'ordre infini.
2. Sinon, $\ker \sigma_g = n\mathbb{Z}$ pour un certain $n \in \mathbb{N}^*$, et n s'appelle l'ordre de g .

Propriétés

1. L'ordre de g est $\# \text{gr}(g)$.
2. Si g est d'ordre infini, les puissances de g sont deux à deux distinctes.
3. Si g est d'ordre n , alors $\forall (k, l) \in \mathbb{Z}^2, g^k = g^l \iff k \equiv l \pmod n$ et $\text{gr}(g)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration :

On a montré que $\text{gr}(g)$ est isomorphe soit à $(\mathbb{Z}, +)$, soit à $(\mathbb{Z}/n\mathbb{Z}, +)$.

C) Théorème de Lagrange (hors programme)

Théorème (Cas d'un groupe abélien fini) :

Soit $(G, *)$ un groupe abélien de cardinal n .

Alors $\forall g \in G, g^n = e_G$.

Démonstration :

$x \in G \mapsto g * x \in G$ est une bijection (car d'inverse $x \in G \mapsto g^{-1} * x \in G$)

Donc $\prod_{x \in G} x = \prod_{x \in G} g * x = g^n \prod_{x \in G} x$.

Donc par régularité $g^n = e_G$.

Théorème (Théorème de Lagrange) :

Soit $(G, *)$ un groupe fini, et $H \subset G$ un sous-groupe de G . Alors $\#H \mid \#G$.

Cas particulier :

Soit $g \in G$, $H = \text{gr}(g)$. On a $\text{ordre } g = \#H \mid \#G$.

Démonstration :

Considérons la relation binaire \mathcal{R} définie sur G^2 par :

$$\forall (x, y) \in G^2, x \mathcal{R} y \iff xy^{-1} \in H \tag{5.23}$$

Alors déjà \mathcal{R} est une relation d'équivalence.

Soit $x_0 \in G$, on cherche $\text{Cl}_{\mathcal{R}}(x_0)$.

Soit $y \in \text{Cl}_{\mathcal{R}}(x_0)$. Alors $y * x_0^{-1} \in H$. Soit $h \in H$ tel que $h = y * x_0^{-1}$.

Donc $y = h * x_0$.

Donc $\text{Cl}_{\mathcal{R}}(x_0) \subset \{x_0 * h, h \in H\}$, et l'autre inclusion est évidente.

Donc $\#\text{Cl}_{\mathcal{R}}(x_0) = \#H$ car $h \mapsto h * x_0$ est injective.

Si on note N le nombre de classes d'équivalences, on a $\#G = N \cdot \#H$.

D) Application aux anneaux $\mathbb{Z}/n\mathbb{Z}$ (hors programme)

- Soit $(n, m) \in \mathbb{N}^2$, $n \geq 1$, $m \geq 1$.

Alors $\pi_n: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ est un morphisme de groupes (resp. d'anneaux en adaptant).
 $x \mapsto \text{Cl}_n(x)$

$$\begin{array}{ccc} (\mathbb{Z}, +) & \xrightarrow{\pi_n} & (\mathbb{Z}/n\mathbb{Z}, +) \\ & \searrow \pi_m & \nearrow \varphi \\ & (\mathbb{Z}/m\mathbb{Z}, +) & \end{array} \tag{5.24}$$

Une condition nécessaire et suffisante pour qu'il existe un morphisme de groupes (resp. d'anneaux) $\varphi: (\mathbb{Z}/m\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ tel que π_n passe au quotient modulo m est que $m\mathbb{Z} \subset \ker \pi_n = n\mathbb{Z}$, c'est-à-dire $n \mid m$.

Autrement dit, $(\mathbb{Z}/m\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ est une application si et seulement si $n \mid m$, et dans ce cas c'est un morphisme de groupes (resp. d'anneaux).

Théorème (Théorème chinois) :

- Soient $n, m \geq 1$, et $\psi: (\mathbb{Z}/nm\mathbb{Z}, +, \times) \rightarrow (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times)$.
 $\text{Cl}_{nm}(x) \mapsto (\text{Cl}_n(x), \text{Cl}_m(x))$

Alors ψ est une application, c'est même un morphisme d'anneaux, et c'est un isomorphisme si et seulement si $n \wedge m = 1$.

Démonstration :

Le fait que ψ est un morphisme découle du point précédent car $n \mid nm$ et $m \mid nm$.

On a $\#\mathbb{Z}/nm\mathbb{Z} = nm = \#\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Il reste donc à montrer la (non) injectivité pour avoir la (non) bijectivité

On cherche $\ker \psi$:

Soit $a \in \mathbb{Z}/nm\mathbb{Z}$. Soit $x \in \llbracket 0, nm - 1 \rrbracket$ tel que $a = \text{Cl}_{nm}(x)$.

Alors $a \in \ker \psi$ si et seulement si $Cl_n(x) = \bar{0}$ et $Cl_m(x) = \bar{0}$, c'est-à-dire si et seulement si $n|x$ et $m|x$.

- ◇ Si $n \wedge m = 1$, alors $a \in \ker \psi \implies nm|x$, donc $a = \bar{0}$, donc ψ est injective.
- ◇ Si $n \wedge m \neq 1$, on pose $x = n \vee m$; alors $x \notin nm\mathbb{Z}$, donc $\psi(Cl_{nm}(x)) = (0, 0)$ et $Cl_{nm}(x) \neq \bar{0}$, donc ψ n'est pas injectif.

D'où le résultat.

Corollaire :

Soient G_1, G_2 deux groupes cycliques de cardinaux n_1, n_2 .

Alors $G_1 \times G_2$ est cyclique si et seulement si $n_1 \wedge n_2 = 1$

Théorème (Théorème chinois arithmétique – résolution de congruences multiples) :

Soient N_1, N_2 tels que $N_1 \wedge N_2 = 1$.

Soient a_1, a_2 tels que $a_1 N_1 + a_2 N_2 = 1$ (il en existe d'après le théorème de Bézout).

Soient enfin $b_1, b_2 \in \mathbb{Z}$.

Alors $x \in \mathbb{Z}$ vérifie $\begin{cases} x \equiv b_1 \pmod{N_1} \\ x \equiv b_2 \pmod{N_2} \end{cases}$ si et seulement si $x \equiv \underbrace{b_2 a_1 N_1 + b_1 a_2 N_2}_{x_0} \pmod{N_1 N_2}$.

En effet :

$$Cl_{N_1}(x_0) = Cl_{N_1}(b_1 a_2 N_2) = Cl_{N_1}(b_1) \times \underbrace{Cl_{N_1}(a_2 N_2)}_{= \bar{1} \text{ car } a_1 N_1 + a_2 N_2 = 1} = Cl_{N_1}(b_1) \quad (5.25)$$

De même, $Cl_{N_2}(x_0) = Cl_{N_2}(b_2)$

Donc x_0 est solution du système, et tout nombre $x = x_0 + \lambda N_1 N_2$ en est solution.

Réciproquement, si x est solution du système, alors $x - x_0$ est multiple de N_1 et N_2 (car $Cl_{N_1}(x_0) = Cl_{N_1}(b_1)$ et $Cl_{N_2}(x_0) = Cl_{N_2}(b_2)$), et donc $N_1 N_2 | x - x_0$ car $N_1 \wedge N_2 = 1$.

Exemple :

- ◇ Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $x^2 + ax + b = 0$.

On a :

$$x^2 + ax + b = \bar{0} \iff \left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} = \bar{0} \iff \left(x + \frac{a}{2}\right)^2 = -a^2 - b = \frac{a^2 + 4b}{4} \quad (5.26)$$

Ainsi :

- Si $a^2 - 4b = \Delta$ n'est pas un carré de $\mathbb{Z}/5\mathbb{Z}$, il n'y a pas de solution.
- Si $\Delta = 0$, $x = \frac{-a}{2} = -3a = 2a$
- Si Δ est un carré non nul, $\Delta = \delta^2$:

$$\begin{aligned} \left(x + \frac{a}{2}\right)^2 - \left(\frac{\delta}{2}\right)^2 = 0 &\iff \left(x + \frac{a - \delta}{2}\right) \left(x + \frac{a + \delta}{2}\right) = 0 \\ &\iff x = \frac{-a \pm \delta}{2} \end{aligned} \quad (5.27)$$

- ◇ Résoudre dans $\mathbb{Z}/143\mathbb{Z}$ l'équation $x^2 - 4x + 3 = \bar{0}$.

On a $143 = 13 \times 11$, donc $\mathbb{Z}/143\mathbb{Z}$ n'est pas un corps.

On cherche x sous la forme $x = Cl_{143}(n)$ où $n \in \mathbb{Z}$.

Alors x est solution si et seulement si $143|n^2 - 4n + 3$, c'est-à-dire si et seulement si $11|n^2 - 4n + 3$ et $13|n^2 - 4n + 3$.

On a $\bar{n}^2 - 4\bar{n} + \bar{3} = (\bar{n} - \bar{1})(\bar{n} - \bar{3})$ (dans n'importe quel $\mathbb{Z}/k\mathbb{Z}$)

Donc $11|n^2 - 4n + 3 \iff n \equiv 1 \pmod{11}$ ou $n \equiv 3 \pmod{11}$ (car $\mathbb{Z}/11\mathbb{Z}$ est un corps)

Et de même $13|n^2 - 4n + 3 \iff n \equiv 1 \pmod{13}$ ou $n \equiv 3 \pmod{13}$.

Donc x est solution si et seulement si $\begin{cases} n \equiv 1 \pmod{13} \text{ ou } n \equiv 3 \pmod{13} \\ \text{et} \\ n \equiv 1 \pmod{11} \text{ ou } n \equiv 3 \pmod{11} \end{cases}$

On a donc 4 solutions dans $\mathbb{Z}/143\mathbb{Z}$, à savoir $\bar{1}, \bar{3}, \bar{14}, \bar{133}$:

$$1 \equiv 1 \pmod{11} \text{ et } 1 \equiv 1 \pmod{13} \quad 3 \equiv 3 \pmod{11} \text{ et } 3 \equiv 3 \pmod{13}, \quad (5.28)$$

$$14 \equiv 3 \pmod{11} \text{ et } 14 \equiv 1 \pmod{13} \quad 133 \equiv 1 \pmod{11} \text{ et } 133 \equiv 3 \pmod{13} \quad (5.29)$$

Pour le dernier, méthode de Bézout :

On cherche n tel que $n \equiv 1 \pmod{11}$ et $n \equiv 3 \pmod{13}$:

$$13 = 11 \times 1 + 2 \quad (5.30)$$

$$11 = 2 \times 5 + 1 \quad (5.31)$$

Donc

$$1 = 11 - 2 \times 5 \quad (5.32)$$

$$1 = 11 - (13 - 11 \times 1) \times 5 = 6 \times 11 - 5 \times 13 \quad (5.33)$$

Ainsi, on peut prendre $n = \underbrace{3 \times 6 \times 11}_{\substack{\equiv 3 \pmod{13} \\ 11|_}}$ - $\underbrace{1 \times 5 \times 13}_{\substack{\equiv 1 \pmod{11} \\ 13|_}}$

Théorème (hors programme) :

- 1. $\varphi: n \in \mathbb{N}^* \mapsto \#(\mathbb{Z}/n\mathbb{Z}) \in \mathbb{N}^*$ est une fonction multiplicative, c'est-à-dire :

$$\forall n, m \in \mathbb{N}^*, n \wedge m = 1 \implies \varphi(n \times m) = \varphi(n) \times \varphi(m) \quad (5.34)$$

- 2. Si $n = p_1^{\alpha_1} \times \dots \times p_i^{\alpha_i}$, où les p_j sont des nombres premiers deux à deux distincts et $\alpha_j \geq 1$, alors $\varphi(n) = \prod_{j=1}^i \left(p_j^{\alpha_j} - p_j^{\alpha_j-1} \right) = n \prod_{j=1}^i \left(1 - \frac{1}{p_j} \right)$

Exemple :

$$\varphi(20) = \varphi(2^2 \times 5) = (2^2 - 2) \times (5 - 1) = 8.$$

Conséquence :

$$\forall n \in \mathbb{Z}, n \wedge 20 = 1 \implies n^8 \equiv 1 \pmod{20} \quad (5.35)$$

En effet, il suffit d'appliquer le théorème de Lagrange à $((\mathbb{Z}/20\mathbb{Z})^*, \times)$ de cardinal 8 : Pour $n \in \mathbb{Z}$, si $n \wedge 20 = 1$, l'ordre de $\bar{n} = Cl_{20}(n)$ divise 8, et donc $\bar{n}^8 = \bar{1}$, c'est-à-dire $n^8 \equiv 1 \pmod{20}$.

Démonstration (du théorème) :

1. $\varphi(nm) = \#(\mathbb{Z}/nm\mathbb{Z})^*$.

On dispose d'un isomorphisme d'anneaux :

$$\psi: (\mathbb{Z}/nm\mathbb{Z}, +, \times) \rightarrow (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times) \tag{5.36}$$

Ainsi, $x \in \mathbb{Z}/nm\mathbb{Z}$ est inversible si et seulement si $\psi(x)$ l'est. Or, $(\alpha, \beta) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est inversible si et seulement si $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$ et $\beta \in (\mathbb{Z}/m\mathbb{Z})^*$.

Ainsi, $\varphi(nm) = \#((\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*) = \varphi(n)\varphi(m)$

2. On a $n = \prod_{j=1}^r p_j^{\alpha_j}$.

Comme les $p_j^{\alpha_j}$ sont premiers entre eux deux à deux, on a :

$$\varphi(n) = \prod_{j=1}^r \varphi(p_j^{\alpha_j}) \tag{5.37}$$

On cherche ainsi $\varphi(p^\alpha)$ où p est premier et $\alpha \geq 1$.

$$\begin{aligned} \varphi(p^\alpha) &= \text{nombre de } k \in \llbracket 1, p^\alpha \rrbracket \text{ tels que } k \wedge p^\alpha = 1 \\ &= \text{nombre de } k \in \llbracket 1, p^\alpha \rrbracket \text{ tels que } p \nmid k. \\ &= p^\alpha - p^{\alpha-1} \end{aligned} \tag{5.38}$$

(car $\# \{k \in \llbracket 1, p^\alpha \rrbracket, p|k\} = \# \{ip, i \in \llbracket 1, p^{\alpha-1} \rrbracket\} = p^{\alpha-1}$)

V Caractéristique d'un corps, corps premier

Soit \mathbb{K} un corps commutatif, on pose $\tau: (\mathbb{Z}, +, \times) \rightarrow (\mathbb{K}, +, \times)$.

$$n \mapsto n \cdot 1_{\mathbb{K}}$$

Avec :

$$n \cdot 1_{\mathbb{K}} = \begin{cases} 0 & \text{si } n = 0 \\ 1_{\mathbb{K}} + \dots + 1_{\mathbb{K}} & \text{si } n > 0 \\ -((-n) \cdot 1_{\mathbb{K}}) & \text{si } n < 0 \end{cases} \tag{5.39}$$

(Remarque : τ est le $\sigma_{1_{\mathbb{K}}}$ du paragraphe précédent pour le groupe $(\mathbb{K}, +)$ avec $g = 1_{\mathbb{K}}$)

Théorème :

- τ est un morphisme d'anneaux (Pas de corps! \mathbb{Z} n'est pas un corps).
- Si τ n'est pas injectif, son noyau est de la forme $p\mathbb{Z}$ où p est premier, et il passe au quotient par l'idéal $p\mathbb{Z}$:

$$\begin{array}{ccc} (\mathbb{Z}, +, \times) & \xrightarrow{\tau} & (\mathbb{F}, +, \times) \\ & \searrow \pi_p & \nearrow \bar{\tau} \\ & (\mathbb{F}_p, +, \times) & \end{array} \tag{5.40}$$

où $\bar{\tau}$ est un morphisme de corps.

- Si τ est injectif, on peut le prolonger en un morphisme de corps :

$$\begin{aligned} \hat{\tau}: \quad \mathbb{Q} &\longrightarrow \mathbb{K} & \text{où } \frac{\tau(a)}{\tau(b)} &\text{ est indépendant du choix de } (a, b) \text{ tel que } r = \frac{a}{b}. \\ r = \frac{a}{b} &\longmapsto & \frac{\tau(a)}{\tau(b)} \end{aligned}$$

Définition :

Si τ est injectif, on dit que \mathbb{K} est de caractéristique 0.

Sinon, on dit que \mathbb{K} est de caractéristique finie p où p est tel que $\ker \tau = p\mathbb{Z}$.

Remarque :

Un morphisme de corps est toujours injectif :

Si $a \neq 0$, alors $a \times a^{-1} = 1_{\mathbb{K}}$, donc $\varphi(a) \times \varphi(a)^{-1} = 1_{\mathbb{K}'}$, d'où $\varphi(a) \neq 0$.

Définition :

Si \mathbb{K} est de caractéristique p , il contient un sous-corps isomorphe à \mathbb{F}_p (à savoir $\bar{\tau}(\mathbb{F}_p)$). Ce corps s'appelle sous-corps premier de \mathbb{K} : c'est le plus petit sous-corps de \mathbb{K} .

Si \mathbb{K} est de caractéristique 0 ; il contient un sous-corps isomorphe à \mathbb{Q} ($\hat{\tau}(\mathbb{Q})$). $\hat{\tau}(\mathbb{Q})$ est appelé le corps premier de \mathbb{K} , c'est aussi le plus petit sous-corps de \mathbb{K} .

Démonstration (du théorème) :

1. ...

2. montrons que p est premier (l'existence de p est évidente : $\ker \tau$ est un sous-groupe de \mathbb{Z}) :

Supposons que $p = a \times b$, avec $a, b \geq 2$.

Alors $0_{\mathbb{K}} = \tau(p) = \tau(a) \times \tau(b)$. Comme \mathbb{K} est un corps, il est intègre, donc $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$, ce qui est impossible.

Existence de $\bar{\tau}$: théorème de passage au quotient par l'idéal $p\mathbb{Z}$.

3. Si τ est injectif : on doit vérifier que si $\frac{a}{b} = \frac{a'}{b'}$, alors $\frac{\tau(a)}{\tau(b)} = \frac{\tau(a')}{\tau(b')}$, c'est-à-dire que $\tau(a)\tau(b') = \tau(a')\tau(b)$, ce qui est vrai car $ab' = a'b$ et τ est un morphisme d'anneaux.

On vérifie ensuite que $\hat{\tau}$ est un morphisme de corps...

(Et comme il est injectif, sa corestriction à $\hat{\tau}(\mathbb{Q})$ est bijective, ce qui justifie l'affirmation faite dans la deuxième définition)

Remarque :

Un corps \mathbb{K} de caractéristique 0 est une \mathbb{Q} -algèbre pour les lois suivantes :

Les lois $+$ et \times sont celles de \mathbb{K} en tant que corps.

Comme on peut identifier \mathbb{Q} à un sous-corps de \mathbb{K} par $\hat{\tau}$, on définit \cdot par la restriction de $\times : \mathbb{K}^2 \rightarrow \mathbb{K}$ à $\mathbb{Q} \times \mathbb{K}$ (en fait, pour $a \in \mathbb{Q}$, $b \in \mathbb{K}$, $a \cdot b = \hat{\tau}(a) \times b$)

Il suffit ensuite de vérifier les différentes lois...

Un corps \mathbb{K} de caractéristique p est une \mathbb{F}_p -algèbre (il suffit ici encore d'identifier \mathbb{F}_p à $\bar{\tau}(\mathbb{F}_p)$, sous-corps de \mathbb{K})

Théorème :

Tout corps fini a un cardinal de la forme p^n (primaire), où p est premier.

Démonstration :

- Tout corps de caractéristique 0 est infini car $\tau : \mathbb{Z} \rightarrow \mathbb{K}$ est injectif.

- Donc si \mathbb{K} est fini, sa caractéristique est un nombre premier p .

Ainsi, \mathbb{K} est un \mathbb{F}_p -ev de dimension finie (car \mathbb{K} est fini et engendre \mathbb{K} comme \mathbb{F}_p -ev)

On pose $n = \dim_{\mathbb{F}_p} \mathbb{K}$. Donc \mathbb{K} est isomorphe à \mathbb{F}_p^n comme \mathbb{F}_p -ev, donc $\#\mathbb{K} = p^n$.

Théorème (Théorème de Galois – admis et hors programme) :

Pour tout p premier et tout $n \in \mathbb{N}^*$, il existe un corps de cardinal p^n , unique à isomorphisme près.

Exemple :

Soit \mathbb{K} un corps de caractéristique p .

Alors $\forall x \in \mathbb{K}, px = 0$, et $\varphi: \mathbb{K} \rightarrow \mathbb{K}$ est un endomorphisme de corps.
 $x \mapsto x^p$

En effet : • Soit $x \in \mathbb{K}$.

Déjà, $p1_{\mathbb{K}} = 0_{\mathbb{K}}$ (définition de la caractéristique)

Donc $px = 1_{\mathbb{K}}x + 1_{\mathbb{K}}x + \dots + 1_{\mathbb{K}}x = (p1_{\mathbb{K}})x = 0$.

• Déjà : on a, pour tout $k \in \llbracket 1, p-1 \rrbracket$, $p|C_p^k$.

En effet, $C_p^k = \frac{p!}{k!(p-k)!} = \frac{p}{k} C_{p-1}^{k-1}$, donc $p|kC_p^k$, et comme $p \wedge k = 1$, on a bien $p|C_p^k$.

Maintenant :

Soient $x, y \in \mathbb{K}$.

Alors $\varphi(x \times y) = \varphi(x) \times \varphi(y)$ car \mathbb{K} est commutatif

$$\varphi(1_{\mathbb{K}}) = 1_{\mathbb{K}} \tag{5.41}$$

$$\varphi(x + y) = (x + y)^p = \sum_{k=0}^p C_p^k x^k y^{p-k} \tag{5.42}$$

Or, $\forall k \in \llbracket 1, p-1 \rrbracket$, $C_p^k x^k y^{p-k} = 0$ car p divise C_p^k .

Donc $\varphi(x + y) = x^p + y^p = \varphi(x) + \varphi(y)$.

VI Exemples de corps

- Sous corps de \mathbb{C} : $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Q}[i]$ sont des corps de caractéristique 0.
- Soit p premier. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est de caractéristique p .

Exemples de corps infinis de caractéristique p $\mathbb{F}_p(X)$ (fractions rationnelles à une indéterminée)

Théorème (Théorème de Fermat) :

$\forall x \in \mathbb{F}_p, x^p = x$, ou encore $\forall n \in \mathbb{Z}, n^p \equiv n \pmod{p}$

Démonstration :

- Si $p = 2$, alors $n^2 \equiv n \pmod{2}$ car n^2 et n ont la même parité.
- Si $p \geq 3$:

Montrons par récurrence que $\forall n \in \mathbb{N}, n^p \equiv n \pmod{p}$.

Pour $n = 0$: ok ($0 \equiv 0 \pmod{p}$)

Soit $n \in \mathbb{N}$, supposons que $n^p \equiv n \pmod{p}$.

Alors $(n + 1)^p = \sum_{k=0}^p C_p^k n^k = 1 + n^p \equiv n + 1 \pmod{p}$ (car $p|C_p^k, k \in \llbracket 1, p-1 \rrbracket$)

Pour $n \in \mathbb{Z}, n \equiv m \pmod{p}$ où $m \geq 0$, et on travaille avec m .

Autre démonstration (hors programme) Pour p premier, $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ est un groupe de cardinal $p - 1$.

D'après le théorème de Lagrange, $\forall a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}, a^{p-1} = \bar{1}$.

Donc $\forall a \in \mathbb{Z}/p\mathbb{Z}, a^p = a$.

Remarque :

Pour $N \geq 2$, on a (extension du théorème de Fermat) :

$$\forall n \in \mathbb{Z}, n \wedge N = 1 \implies n^{\varphi(N)} = \bar{1} \text{ (dans } \mathbb{Z}/N\mathbb{Z}\text{)}.$$

Théorème (Théorème de Wilson) :

$p \in \mathbb{N} \setminus \{0, 1\}$ est premier si et seulement si $(p - 1)! \equiv -1 \pmod{p}$.

Démonstration :

- Si p n'est pas premier, alors $p = a \times b$, où $a, b \geq 2$.

Si $a \neq b$, alors $a \times b | (p - 1)!$, donc $(p - 1)! \equiv 0 \pmod{p}$.

Si $a = b \geq 3$, alors $1 \leq a < 2a \leq p - 1$.

Donc $a^2 = p | (p - 1)!$

Si $p = 4$, $(p - 1)! \equiv 2 \pmod{4}$.

- Si p est premier ≥ 3 : on va montrer que $\prod_{a \in \mathbb{F}_p^*} a = \overline{-1}$.

Soit $A = \{x \in \mathbb{F}_p^*, x = \frac{1}{x}\}$. Alors $A = \{1, -1\}$. En effet :

Dans \mathbb{F}_p , $x = \frac{1}{x}$ équivaut à $(x - \bar{1})(x + \bar{1}) = \bar{0}$.

Ainsi, $\mathbb{F}_p^* \setminus A$ est de cardinal pair, et on peut regrouper ses éléments deux par deux : x avec $\frac{1}{x}$.

Donc $\prod_{a \in \mathbb{F}_p^* \setminus A} a = \bar{1}$, et comme $p \geq 3$, on a $-\bar{1} \neq \bar{1}$.

Donc $\prod_{a \in \mathbb{F}_p^*} a = \bar{1} \times (-\bar{1}) \times \bar{1} = -\bar{1}$.

Enfin, si $p = 2$, on a bien $1 \equiv -1 \pmod{2}$.

Remarque :

Pour $p \geq 3$, qu'obtient-on en regroupant x et $-\frac{1}{x}$?

$$A = \left\{x \in \mathbb{F}_p^*, x = \frac{-\bar{1}}{x}\right\} = \left\{x \in \mathbb{F}_p^*, x^2 + \bar{1} = \bar{0}\right\}.$$

1. Si l'équation $x^2 + \bar{1} = \bar{0}$ n'a pas de solution dans \mathbb{F}_p :

$$\prod_{a \in \mathbb{F}_p^*} a = \prod_{a \in S} a \times \frac{-\bar{1}}{a} \text{ où } \#S = \frac{p-1}{2}.$$

$$\text{Donc } -\bar{1} = (-\bar{1})^{\frac{p-1}{2}}$$

Ainsi, si $x^2 + \bar{1} = \bar{0}$ n'a pas de solution, on a $p \equiv 3 \pmod{4}$.

2. Si elle a des solutions, elle en a deux opposées x_0 et $-x_0$.

$$-\bar{1} = \prod_{a \in \mathbb{F}_p^*} a = \prod_{a \in S} \left(a \times \frac{-\bar{1}}{a}\right) \times \underbrace{x_0 \times (-x_0)}_{=\bar{1}} \tag{5.43}$$

S est une partie de $\mathbb{F}_p^* \setminus \{\pm x_0\}$ de cardinal $\frac{p-3}{2}$

Donc $-\bar{1} = (-\bar{1})^{\frac{p-3}{2}}$, d'où $p \equiv 1 \pmod{4}$.

VII Propriétés générales de $\mathbb{K}[X]$ et $\mathbb{K}(X)$ (où \mathbb{K} est un corps)

Soit \mathbb{K} un corps quelconque (commutatif). On étend sans difficulté au cas d'un corps quelconque les définitions et résultats suivants vus en première année :

- Opérations et structure de \mathbb{K} -algèbre commutative unitaire de $\mathbb{K}[X]$.
- Degré d'un polynôme, intégrité de $\mathbb{K}[X]$; polynômes unitaires (ou normalisés), degré d'un produit, d'une somme; sous- \mathbb{K} -espace $\mathbb{K}_n[X]$ des polynômes de degré au plus n .
- Fractions rationnelles, corps $\mathbb{K}(X)$.
- Multiples et diviseurs d'un polynôme, polynômes associés. Division euclidienne dans $\mathbb{K}[X]$, algorithme de la division euclidienne.
- Polynôme scindé sur \mathbb{K} ; relations entre les coefficients et les racines d'un polynôme scindé.

Attention :

Le théorème de D'Alembert n'est pas vrai en général. Un corps dans lequel tout polynôme non constant est scindé est dit algébriquement clos.

Pour factoriser les polynômes de $\mathbb{K}[X]$, il ne suffit pas, en général, de considérer les facteurs de degré 1 ou 2 : il faut introduire la notion de polynôme irréductible (voir VIII)

- Fonction polynomiale associée à un polynôme. Équations algébriques. Zéros (ou racines) d'un polynôme; reste de la division euclidienne d'un polynôme P par $X - a$; caractérisation des zéros de P par le fait que $X - a$ divise P . Ordre de multiplicité d'un zéro du polynôme non nul P : c'est le plus grand entier m tel que $(X - a)^m$ divise P .
- Algorithme de Horner pour le calcul des valeurs d'une fonction polynomiale. Fonction rationnelle associée à une fraction rationnelle. Zéros et pôles d'une fraction rationnelle; ordre de multiplicité.
- Polynôme dérivé. Linéarité de la dérivation, dérivée d'un produit. Dérivées successives, dérivée n -ième d'un produit (formule de Leibniz)

Attention : L'application $\varphi : P \in \mathbb{K}[X] \mapsto \tilde{P} \in \mathbb{K}^{\mathbb{K}}$ qui à un polynôme associe sa fonction polynomiale est injective si, et seulement si, \mathbb{K} est infini, et on a même le théorème :

Théorème :

1. φ est un morphisme d'algèbre.
 2. Si \mathbb{K} est infini, φ est injective non surjective.
 3. Si \mathbb{K} est fini, φ est surjective non injective, et $\ker \varphi = P_0 \mathbb{K}[X]$ avec $P_0 = \prod_{a \in \mathbb{K}} X - a = X^q - X$, où $q = \#\mathbb{K}$.
- Lorsque \mathbb{K} est infini, on peut ainsi identifier polynôme et fonction polynomiale associée.

Démonstration :

Déjà, c'est un morphisme d'algèbre...

Soit $P \in \ker \varphi$, et $a_1, a_2 \dots a_r$ des éléments deux à deux distincts de \mathbb{K} .

On a : $\forall i \in \llbracket 1, r \rrbracket, \tilde{P}(a_i) = 0$ (car $\tilde{P} = \tilde{0}$)

Comme les a_i sont distincts, on a $\prod_{i=1}^r (X - a_i) | P$. Donc $P = 0$ ou $\deg P \geq r$.

1. Si \mathbb{K} est infini, alors $P = 0$ (car si $P \neq 0$ de degré d , on prend $r = d + 1$ et on a une contradiction) φ n'est pas surjective car la fonction qui vaut $1_{\mathbb{K}}$ en $0_{\mathbb{K}}$ et $0_{\mathbb{K}}$ ailleurs n'est pas polynomiale (car $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$ est infini).

2. Si \mathbb{K} est fini, on prend $r = q = \#\mathbb{K}$, et on a, si $P \in \ker \varphi$, $\prod_{a \in \mathbb{K}} X - a \mid P$; inversement, si $\prod_{a \in \mathbb{K}} X - a \mid P$, alors $\forall a \in \mathbb{K}, \tilde{P}(a) = 0$.

Problème : pourquoi $P_0 = X^q - X = \prod_{a \in \mathbb{K}} X - a$?

Vérifions que $X^q - X \in \ker \varphi$ c'est-à-dire que $\forall a \in \mathbb{K}, a^q = a$, ce qui est vrai d'après le théorème de Lagrange appliqué à \mathbb{K}^* pour $a \neq 0$ et évident pour $a = 0$.

Donc $\prod_{a \in \mathbb{K}} X - a \mid X^q - X$. Or, ils sont tous deux unitaires, de degré q , donc égaux.

Surjectivité : toute fonction est polynomiale : interpolation de Lagrange :

Pour $f: \mathbb{K} \rightarrow \mathbb{K}$, on pose $P = \sum_{a \in \mathbb{K}} f(a) \prod_{b \in \mathbb{K} \setminus \{a\}} \frac{X-b}{a-b}$, et on a $\tilde{P} = f$.

Attention : La formule de Taylor et son application à la caractérisation de la multiplicité d'une racine ne sont vérifiées que si \mathbb{K} est de caractéristique 0.

Si \mathbb{K} est de caractéristique p non nulle, les entiers multiples de p ne sont pas inversibles dans \mathbb{K} , donc la formule de Taylor n'a pas de sens.

Remarque :

Si \mathbb{K} est de caractéristique 0, le noyau de la dérivation est constitué des polynômes constants, alors que si \mathbb{K} est de caractéristique p premier, il est constitué des polynômes en X^p , c'est-à-dire de la forme $\sum_{j=0}^n a_j X^{jp}$.

Formule de Taylor pour les polynômes Si \mathbb{K} est de caractéristique 0, pour tout $P \in \mathbb{K}[X]$ et tout $a \in \mathbb{K}$, on a :

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} (X - a)^k \quad (\text{somme finie}) \quad (5.44)$$

$$P(a + X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} X^k = \sum_{k=0}^{+\infty} a^k \frac{P^{(k)}(a)}{k!} \quad (5.45)$$

Si \mathbb{K} est de caractéristique 0, a est racine de multiplicité n si et seulement si :

$$P(a) = P'(a) = \dots = P^{(n-1)}(a) = 0 \quad (5.46)$$

Faux en caractéristique p Par exemple avec $\mathbb{K} = \mathbb{F}_p$, $P = X^p + 1$, $P' = pX^{p-1} = 0$.

VIII Étude arithmétique de $\mathbb{K}[X]$ (où \mathbb{K} est un corps)

Remarque (hors programme) :

L'existence d'une division euclidienne dans $\mathbb{K}[X]$ permet d'obtenir les mêmes propriétés arithmétiques que pour \mathbb{Z} . Ce qui suit serait plus généralement valable dans un anneau euclidien, c'est-à-dire un anneau (commutatif) intègre $(A, +, \times)$ muni d'une application $\varphi: A \setminus \{0\} \rightarrow \mathbb{N}$ telle que $\forall (a, b) \in A^2, b \neq 0 \implies$

$$\exists (q, r) \in A^2, a = bq + r \text{ et } \begin{cases} \varphi(r) = 0 \\ \text{ou } \varphi(r) < \varphi(q) \end{cases}$$

Une telle fonction φ s'appelle stathme euclidien; le degré et la valeur absolue sont des stathmes euclidiens respectivement sur $\mathbb{K}[X]$ et \mathbb{Z} .

Par exemple, les anneaux $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ sont des anneaux euclidiens, on peut donc y faire la même arithmétique que dans \mathbb{Z} .

Théorème :

Soit \mathbb{K} un corps. Tout idéal de $\mathbb{K}[X]$ est principal, c'est-à-dire de la forme $I = P_0\mathbb{K}[X]$.

Démonstration :

Soit I un idéal de $\mathbb{K}[X]$, différent de $\{0\}$. Il contient donc un élément non nul de $\mathbb{K}[X]$. Ainsi, $\{\deg P, P \in I\} \subset \mathbb{N}$ et est non vide. Soit donc P_0 de degré minimal dans I . Alors $I = P_0\mathbb{K}[X]$. En effet :

Déjà, $P_0\mathbb{K}[X] \subset I$ puisque I est un idéal de $\mathbb{K}[X]$.

Soit maintenant $P \in I$. La division euclidienne de P par P_0 donne :

$P = P_0Q + R$ où $\deg R < \deg P_0$. Or, $R = P - P_0Q$, et $P \in I, P_0Q \in I$ donc comme I est un groupe $R \in I$. Comme P_0 est le polynôme non nul de degré minimal dans I , on a donc nécessairement $R = 0$. Donc $P = P_0Q$. Donc $P \in P_0\mathbb{K}[X]$. D'où l'autre inclusion et l'égalité.

Théorème (Théorème de Bézout) :

Soient $A, B \in \mathbb{K}[X]$.

Alors A et B sont premiers entre eux $\iff \exists (U, V) \in \mathbb{K}[X]^2, AU + BV = 1$.

(Même démonstration que dans \mathbb{Z})

Pour n polynômes :

Soient $P_1, P_2, \dots, P_n \in \mathbb{K}[X] \setminus \{0\}$. Les propositions suivantes sont équivalentes :

- (1) P_1, P_2, \dots, P_n sont premiers entre eux deux à deux (c'est-à-dire les seuls diviseurs communs sont les polynômes constants)
- (2) Il existe $(U_i)_{i \in \llbracket 1, n \rrbracket}$ telle que $\sum_{i=1}^n P_i U_i = 1$.
- (3) L'idéal engendré par les P_i ($P_1\mathbb{K}[X] + \dots + P_n\mathbb{K}[X]$) est $\mathbb{K}[X]$.

Démonstration :

(2) \implies (1) ok

(3) \implies (2) $P_1\mathbb{K}[X] + \dots + P_n\mathbb{K}[X] = \mathbb{K}[X]$, alors comme $1 \in \mathbb{K}[X]$, il s'écrit sous la forme $\sum_{i=1}^n P_i U_i$.

(1) \implies (3) on pose $I = P_1\mathbb{K}[X] + \dots + P_n\mathbb{K}[X]$.

Alors I est un idéal de $\mathbb{K}[X]$, donc principal. Soit alors $D \in \mathbb{K}[X]$ tel que $I = D\mathbb{K}[X]$.

Alors $D \neq 0$ car $P_1 \in I$.

De plus, $\forall i \in \llbracket 1, n \rrbracket, P_i \in I$, donc P_i est multiple de D . Donc D est constant, et $I = \mathbb{K}[X]$.

Théorème (Théorème de Gauss) :

Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$. Si A divise BC et si A est premier avec B alors A divise C .

Théorème :

Dans l'anneau $\mathbb{K}[X]$ (comme dans \mathbb{Z}), les éléments premiers et les éléments irréductibles sont les mêmes.

Tout élément $A \in \mathbb{K}[X] \setminus \{0\}$ s'écrit, de manière unique à permutation près des P_i , sous la forme $A = \varepsilon P_1^{r_1} \dots P_s^{r_s}$ où $\varepsilon = \text{cte}$, où les P_i sont irréductibles (ou premiers) et unitaires et où les r_i sont des entiers naturels.

Théorème :

Soit $(P_i)_{i \in \llbracket 1, n \rrbracket}$ une famille d'éléments non tous nuls de $\mathbb{K}[X]$. Il existe un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que $\forall R \in \mathbb{K}[X], (\forall i, R|P_i \iff R|D)$.

Propriétés et définition D s'appelle PGCD des P_i . Il est caractérisé par le fait qu'il divise tous les P_i et qu'il existe des polynômes $(U_i)_{i \in \llbracket 1, n \rrbracket}$ tels que $D = \sum_{i=1}^n U_i P_i$. En fait, D est le générateur unitaire de l'idéal $P_1\mathbb{K}[X] + P_2\mathbb{K}[X] + \dots + P_n\mathbb{K}[X]$.

Il est aussi caractérisé par le fait qu'il divise tous les P_i et que tout autre diviseur commun à tous les P_i divise D ; D est le diviseur commun de tous les P_i de plus grand degré.

Théorème :

Soit $(P_i)_{i \in \llbracket 1, n \rrbracket}$ une famille d'éléments non nuls de $\mathbb{K}[X]$. L'ensemble des polynômes multiples de tous les P_i est l'intersection des idéaux $P_i\mathbb{K}[X]$, c'est aussi un idéal. Ainsi, il existe un unique polynôme $M \in \mathbb{K}[X]$ unitaire tel que :

$$\forall R \in \mathbb{K}[X], (\forall i, P_i|R \iff M|R) \tag{5.47}$$

Propriétés et définitions M s'appelle PPCM des P_i . Il est caractérisé par le fait qu'il est multiple de tous les P_i et que tout autre multiple de tous les P_i est multiple de M ; M est le polynôme unitaire de plus degré multiple de tous les P_i .

Théorème :

Le PGCD D et PPCM M des polynômes non nuls A et B sont liés par $AB = \lambda MD$ où λ est le produit des dominants de A et B .

Calcul avec la décomposition en irréductibles

Notation :

Pour tout R irréductible unitaire et tout polynôme A non nul, on note $V_R(A)$ l'exposant de R de la décomposition de A . $V_R(A)$ s'appelle valuation R -adique de A .

Exemple :

$R = X - x_0$; $V_R(A)$ est la multiplicité de la racine x_0 de A .

Théorème :

Soient A_1, \dots, A_n des polynômes non nuls; pour tout polynôme R irréductible unitaire, on pose $\alpha_R = \min_{i \in \llbracket 1, n \rrbracket} (V_R(A_i))$, $\beta_R = \max_{i \in \llbracket 1, n \rrbracket} (V_R(A_i))$.

Alors $\alpha_R = \beta_R = 0$ sauf pour un nombre fini de R .

De plus, $PGCD(A_i) = \prod_R R^{\alpha_R}$ et $PPCM(A_i) = \prod_R R^{\beta_R}$.

Démonstration :

La même que dans \mathbb{Z} .