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 $R$ définie par :
$\forall (x, y) \in E \times F, xRy \iff (x, y) \in G$
On dit que $R$ est une relation binaire de source $E$, de but $F$ et de graphe $G$.
Une relation binaire $R$ est une application si $\forall x \in E, \exists y \in F, xRy$.
On note alors $y = R(x)$.

B) Partitions, relation d’équivalence, quotient

- On appelle partition d’un ensemble $E$ toute partie $\Pi$ de $P(E)$ telle que :
  - Les éléments de $\Pi$ sont non vides ($\Pi \subset P(E) \setminus \{\emptyset\}$)
  - Les éléments de $\Pi$ sont deux à deux disjoints ($\forall A, B \in \Pi, A \not= B \Rightarrow A \cap B = \emptyset$)
  - Les éléments de $\Pi$ recouvrent $E$ ($\bigcup_{\Pi} A = E$)

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

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

Définition :
Dans le point (1), l’application $E \to \Pi$
$x \mapsto A$ unique élément de $\Pi$ tel que $x \in A$
la surjection canonique de $E$ sur $\Pi$.

- Relation d’équivalence… (symétrique, réflexive, transitive)

- Classe d’équivalence d’une relation d’équivalence :
  Soit $R$ une relation d’équivalence sur $E$. On appelle classe d’équivalence de $x \in E$
la partie $\text{Cl}_R(x) = \{y \in E, xRy\}$.

Théorème :
L’ensemble des classes d’équivalences de $R$ est une partition de $E$, notée $E / R$, et
l’application $E \to E / R$ est la surjection canonique associée.
$x \mapsto \text{Cl}_R(x)$
• Cas des ensembles finis :

Théorème :
Soit $E$ un ensemble fini.

1. Soit $f : E \to F$ une application. Alors les fibres de $f$ sont finies, et
\[
\# E = \sum_{y \in F} \# f^{-1}\{y\}.
\]

2. Si $\Pi$ est une partition de $E$, alors $\# E = \sum_{A \in \Pi} \# A$.

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

Démonstrations :
- Premier théorème :
L’ensemble des classes d’équivalences forment une partition :

(i) $\forall x \in E, Cl_g(x) \neq \emptyset$ (en effet, $x \in Cl_g(x)$ car $xRx$)

(ii) Soient $x, y \in E$. Alors soit $Cl_g(y) = Cl_g(x)$, soit $Cl_g(y) \cap Cl_g(x) = \emptyset$.
En effet, supposons que $Cl_g(y) \cap Cl_g(x) \neq \emptyset$.
Soit alors $z \in Cl_g(y) \cap Cl_g(x)$.
Pour $t \in Cl_g(x)$, on a $tRx$, et $xRz$ et $zRy$, donc par transitivité $tRy$.
Donc $Cl_g(x) \subseteq Cl_g(y)$. De même, $Cl_g(y) \subseteq Cl_g(x)$, d’où l’égalité

(iii) Les classes recouvrent $E$: $\forall x \in E, x \in Cl_g(x)$
- 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 (1).

## 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 $\sigma_a : G \to G$ est un automorphisme,
\[ g \mapsto a * g * a^{-1} \]
De plus, l’application $(G, *) \to (\text{Aut} G, \circ)$ est un morphisme de groupes :
\[ a \mapsto \sigma_a \]
Soit $a, b \in G$. Pour tout $g \in G$, on a :
\[(\sigma_a \circ \sigma_b)(g) = \sigma_a(b * g * b^{-1}) = a * b * g * b^{-1} * a^{-1} = \sigma_{a * b}(g) .\]
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 \((G_k,T_k) \ (k=1,2)\) deux groupes de neutres \(e_k\).
Alors la loi * définie sur \(G_1 \times G_2\) par :
\[
\forall (x_1,x_2,y_1,y_2) \in (G_1 \times G_2)^2, (x_1,x_2)*(y_1,y_2) = (x_1T_1y_1,x_2T_2y_2)
\]
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 \((G,T)\) 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 \((G,T)\)
2. \(\forall a \in G, \forall h \in H, aThTa^{-1} \in H\)

Théorème :
Le noyau d’un morphisme de groupe est un sous-groupe distingué de la source.

Démonstration :
Soit \(\varphi : (G_1,T_1) \to (G_2,T_2)\) un morphisme.
Posons \(H = \ker \varphi\).
Déjà, \(H\) est un sous-groupe de \((G_1,T_1)\).
Soient \(a \in G_1, \ h \in H\).
On a : \(\varphi(aT_1hT_1a^{-1}) = \varphi(a)T_2\varphi(h)T_2\varphi(a)^{-1} = \varphi(a)T_2T(a)^{-1} = 1_G\).
Donc \(aT_1hT_1a^{-1} \in H\), 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 \(\bar{G}\) est un groupe commutatif, tout sous-groupe de \(G\) est distingué
Si \((G,T)\) 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 \( (\mathbb{Z}',+) \). Alors il existe \( r \leq n \) tel que \( H \) est isomorphe à \( \mathbb{Z}' \).

**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 \( \mathbb{Z}' \), sinon \( c.\mathbb{Z} \) est isomorphe à \( \mathbb{Z} \), un isomorphisme étant \( \mathbb{Z} \to c.\mathbb{Z} \).
- 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 \( \mathbb{Z}' \).

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

On considère \( \varphi : \mathbb{Z}^{n+1} \to \mathbb{Z}^n \) morphisme surjectif de groupe. Alors \( \varphi(H) \)

\( (x_1,x_2,\ldots,x_{n+1}) \to x_{n+1} \)

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 \( \mathbb{Z}' \) où \( r \leq n \).

En effet :

Soit \( \Pi : \mathbb{Z}^{n+1} \to \mathbb{Z}^n \) Alors \( \Pi (x_1,x_2,\ldots,x_{n+1}) \) est un isomorphisme.

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

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

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

Alors \( H' \sim \mathbb{Z}' \) pour un certain \( r \leq n \) (d’après (1))

Considérons maintenant l’application \( u : H \times \mathbb{Z} \to H \). Alors \( u \) est un morphisme. \( u \) est surjectif : soit \( h \in H \). Il existe alors \( \alpha \in \mathbb{Z} \) tel que \( h - \alpha.v \in H' \). Ainsi, si on pose \( h' = h - \alpha.v \), \( h = u(h',\alpha) \). \( u \) est injectif : si \( u(h',n) = 0 \), alors \( h'+nv = 0 \), donc \( \varphi(h'+nv) = \varphi(h')+nc = 0 \), 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 \((A,+,\ast)\) un anneau, d’élément unité \(1_A\).
On note \(A^\ast = \{a \in A, \exists b \in A, a \ast b = b \ast a = 1_A\}\)
Proposition :
\((A^\ast,\ast)\) est un groupe.

On note \(M_n(\mathbb{Z}) = \{M = (m_{i,j})_{i,j=1}^n \in M_n(\mathbb{R}), \forall (i,j) \in [1,n]^2, m_{i,j} \in \mathbb{Z}\}\)
Alors \(M_n(\mathbb{Z})\) est un sous anneau de \((M_n(\mathbb{R}),+,\times)\)
On peut alors noter \(M_n(\mathbb{Z})^\ast = \{M \in M_n(\mathbb{Z}), \exists M' \in M_n(\mathbb{Z}), MM' = M'M = I_n\}\)
Soit \(M \in M_n(\mathbb{Z})\). On a alors l’équivalence : \(M \in M_n(\mathbb{Z})^\ast \iff \det M = \pm 1\)
En effet :
• Si \(M \in M_n(\mathbb{Z})^\ast\), 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 \(M^{-1} = \frac{\\text{com}(M)}{\varepsilon}\).
Les coefficients de \(\text{com}(M)\) sont entiers, donc \(\frac{\\text{com}(M)}{\varepsilon} \in M_n(\mathbb{Z})\).
Donc \(M \in M_n(\mathbb{Z})^\ast\)

Groupes symétriques et alternés :
Définition :
- \(\mathcal{S}_n\) est l’ensemble des permutations de \(\{1,...,n\}\). Ainsi, \(#\mathcal{S}_n = n!\).
- Signature de \(\sigma \in \mathcal{S}_n : \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}\)
Théorème :
• \(\forall \sigma \in \mathcal{S}_n, \varepsilon(\sigma) \in \{\pm 1\}\)
• Si \(\sigma\) est une transposition, alors \(\varepsilon(\sigma) = -1\)
• \(\varepsilon\) est un morphisme de groupe : \(\varepsilon : (\mathcal{S}_n,\circ) \rightarrow (\{\pm 1\},\times)\)

Définition :
\(A_n = \ker \varepsilon : \) groupe alterné.
\(A_n\) est donc un sous-groupe distingué de \((\mathcal{S}_n,\circ)\), et \(#A_n = \frac{n!}{2}\) pour \(n \geq 2\).
En effet :
Posons \(B_n = \{\sigma \in \mathcal{S}_n, \varepsilon(\sigma) = -1\}\)
On a ainsi \(\mathcal{S}_n = A_n \cup B_n\) et \(A_n \cap B_n = \emptyset\)
Posons \(\tau = (1;2)\).
Alors \(A_n \rightarrow B_n\) 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 \((G,\ast)\) un groupe (il suffirait en fait que \(*\) soit associative et admette un neutre)

Soit \(g \in G\). On pose \[g^0 = e_G \]
\[\forall n \in \mathbb{N}, \ g^{n+1} = g^n * g\]

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 \(g \in G\) :
[\[
\begin{align*}
0.g &= e_G = 0 \\
\forall n \in \mathbb{N}, (n+1).g &= n.g + g
\end{align*}
\]

2) Extension à \(\mathbb{Z}\).

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

- Notation additive…

Théorème :

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

Alors \(\sigma_g : (\mathbb{Z},+) \to (G,\ast)\) est un morphisme de groupes.

\(n \mapsto g^n\)

3) Sous-groupe engendré par une partie

Théorème :

Soit \((G,\ast)\) 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 \(A\).
- \(\text{gr}(A) = \left\{ a_1^{e_1} * a_2^{e_2} * ... * a_p^{e_p}, e_i = \pm 1, (a_1, ..., a_p) \in A^p \right\}(H_1)\)
  \[= \left\{ a_1^{N_1} * a_2^{N_2} * ... * a_p^{N_p}, N_j \in \mathbb{Z}, (a_1, ..., a_p) \in A^p \right\}(H_2)\]

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 \(e_G\).
Définitions :
- 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 \( \sigma_g : \mathbb{Z} \rightarrow G \) :
\[
m \mapsto g^n
\]

4) Exemples

- \((\mathbb{Z},+)\) est monogène, car \( \mathbb{Z} = \text{gr}([1]) \) (notation additive)
- Soit \((a,b) \in \mathbb{N}^2 \). Alors \( \text{gr}([a,b]) = (a \wedge b)\mathbb{Z} \)
  En effet :
  \[
  \text{gr}([a,b]) = \{n.a + n.b; (n,m) \in \mathbb{Z}^2\} = a.\mathbb{Z} + b.\mathbb{Z} = (a \wedge b)\mathbb{Z} \quad \text{(th de Bézout)}
\]
- \((\mathbb{Z}_n,\circ)\) est engendré par les transpositions.
- Rappel :

Matrice de dilatation :
\[
D_\lambda(A) = \begin{pmatrix}
1 & & & \\
& \ddots & & \\
& & \ddots & \\
& & & \lambda
\end{pmatrix} = D_\lambda(A) \quad (C_k \rightarrow \lambda C_k)
\]

Pour \( A \in M_n(\mathbb{R}) \),
\[
D_\lambda(A) \times A = \begin{pmatrix}
1 & & & \\
& \ddots & & \\
& & \ddots & \\
& & & \lambda
\end{pmatrix} \begin{pmatrix}
a_{1,1} & \cdots & \cdots & a_{1,n} \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
a_{n,1} & \cdots & \cdots & a_{n,n}
\end{pmatrix} = \begin{pmatrix}
a_{1,1} & \cdots & \cdots & a_{1,n} \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
\lambda a_{k,1} & \cdots & \cdots & \lambda a_{k,n}
\end{pmatrix}
\]

Matrice de transvection :
\[
T_{i,j}(\lambda) = \begin{pmatrix}
1 & & \lambda \\
& \ddots & \\
& & \ddots \\
& & & 1
\end{pmatrix} = I_n + \lambda E_{i,j}
\]
\[
T_{i,j}(\lambda) \times A : \text{matrice obtenue en ajoutant à la } i\text{-ième ligne de } A \text{ } \lambda \text{ fois la } j\text{-ième ligne de } A.
\]

Théorème :
Soit \( \mathbb{K} \) un corps.
(1) Toute matrice de déterminant 1 est produit de matrices \( T_{i,j}(\lambda) \).
   Autrement dit, \( SL_n(\mathbb{K}) \) est le sous-groupe de \( M_n(\mathbb{K}) \) 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 \( SL_n(\mathbb{R}) \). En d’autres termes, \( GL_n(\mathbb{R}) \) est engendré par les \( T_{i,j}(\lambda) \) et les \( D_n(\mu) \).

Démonstration :
Voir méthode du pivot.

Pour \( A \in GL_n(\mathbb{R}) \), 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
\[
\begin{pmatrix}
1 & \cdots & 1
\end{pmatrix}
\]
\[
\begin{pmatrix}
d
\end{pmatrix}
\]
 où \( d = \det A \).

Comme ajouter à la ligne \( i \lambda \) fois la ligne \( j \) revient à remplacer \( A \) par
\( T_{i,j}(\lambda) \times A \), il existe donc une famille \( (T_{i,j}(\lambda))_{\lambda \in [\mathbb{R}]} \) telle que :
\[
T_{i,j}(\lambda_m) \times \ldots \times T_{i,j}(\lambda_1) \times A = \begin{pmatrix} 1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
d & & d \end{pmatrix} = D_n(d)
\]

Si \( A \in SL_n(\mathbb{R}) \), on a \( \det A = 1 \), et donc :
\[
A = [T_{i,j}(\lambda_m) \times \ldots \times T_{i,j}(\lambda_1)]^{-1} = T_{i,j}(\lambda_m) \times \ldots \times T_{i,j}(\lambda_1)
\]
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 \( SL_n(\mathbb{R}) \)

Application :
Montrer que \( SL_n(\mathbb{R}) \) est connexe par arcs.

Soit \( A \in SL_n(\mathbb{R}) \).
On va trouver \( \phi : [0;1] \to SL_n(\mathbb{R}) \) continue telle que \( \phi(0) = I_n \) et \( \phi(1) = A \).

Comme \( A \in SL_n(\mathbb{R}) \), \( A \) s’écrit sous la forme \( T_{i,j}(\lambda) \times \ldots \times T_{i,j}(\lambda_m) \).

On pose alors \( \phi(t) = T_{i,j}(t\lambda) \times \ldots \times T_{i,j}(t\lambda_m) \).

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

De plus, \( \phi \) est continue car \( \phi(t) \) est une matrice dont les coefficients dépendent polynomiallement de \( t \).

(ou : l’application \( M_n(\mathbb{R})^2 \to M_n(\mathbb{R}) \) est continue car bilinéaire en \( (A,B) \mapsto AB \)

dimension finie)

Donc \( SL_n(\mathbb{R}) \) est connexe par arcs.

Remarque :
\( GL_n(\mathbb{R}) \) n’est pas connexe par arcs car sinon \( \det(GL_n(\mathbb{R})) = \mathbb{R}^* \) 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 : $\forall a \in A, \forall i \in I, ai \in I / ia \in I$ 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 $(\mathbb{Z},+)$
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) $\Rightarrow$ (3) , (3) $\Rightarrow$ (2) est vrai, c’est l’idéal principal de $\mathbb{Z}$
engendré par $n$. et (2) $\Rightarrow$ (1) aussi (par définition d’un idéal).

Remarque :
Il existe des idéaux non principaux.

Exemple :
$A = (\mathbb{Z}[X],+,$ 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) \(yA \subseteq xA\)

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 (\(2 \times 2 = 0\))
- \(A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, a, b \in \mathbb{R}\) est commutatif unitaire, mais non intègre :
\[
\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.
\]

4) Eléments remarquables d’un anneau

(1) les éléments inversibles forment un sous-groupe pour \(\times\)…
(2) Outil important : soit \((A,+,\ast)\) un anneau.
Pour étudier \(a \in A\), on a intérêt à étudier les applications :
\(
\delta_a : A \to A \quad \text{et} \quad \gamma_a : A \to A
\)
\(x \mapsto ax\quad \text{et} \quad x \mapsto x^\ast a
\)

Proposition :
\(\delta_a\) et \(\gamma_a\) sont des endomorphismes du groupe \((A,+)\) (mais pas d’anneaux)
Exemple (on suppose \(A\) commutatif) :
\(\delta_a\) n’est pas injectif \(\iff\) \(a\) est un diviseur de 0.
\(\delta_a\) est bijective \(\iff\) \(a\) est inversible.
(3) Définition :
Un élément $a$ non nul non inversible de $A$ est dit irréductible (indécomposable) si $\forall b, c \in A, a = bc \Rightarrow b \in A^*$ ou $c \in A^*$
Un élément $a$ est dit premier lorsque $\forall b, c \in A, a | bc \Rightarrow a | b$ 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 $(\mathbb{C}, +, \times) \ldots$
$A^* = \{-1 ; 1\}$
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 $\left(\frac{1}{2}z \pm z' \frac{1}{2}\right)^2 = 4 \cdot (a^2 + 6b^2)(a'^2 + 6b'^2) = 4$
- $1^\text{er}$ cas : $a^2 + 6b^2 = a'^2 + 6b'^2 = 2$ : impossible
- $2^\text{ème}$ cas : $a^2 + 6b^2 = 1 ; z$ est inversible.
- $3^\text{ème}$ 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 $2|\sqrt{6}$ 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 $z = \frac{\sqrt{6}}{2} \notin A$.

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 $P(E)$ de $\Delta$ et $\cap$ ($A \Delta B = A \cup B \setminus A \cap B$ : différence symétrique).
Alors $P(E)$ 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 $\chi_A : E \rightarrow \mathbb{Z} / 2\mathbb{Z}$)
\[
\chi \mapsto \begin{cases} 
1 & \text{si } x \in A \\
0 & \text{sinon}
\end{cases}
\]
\( \mathbb{Q}[i] = \{a + ib, a, b \in \mathbb{Q}\} \) 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, \( \pi \) et \( e \) ne le sont pas (ils sont transcendants)

**Proposition (hors programme) :**
Soit \( a \in \mathbb{C} \), algébrique.

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

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
\( P_0 = x^d + c_{d-1}x^{d-1} + \ldots + c_0 \)
\( \mathbb{Q}[a] \) est une sous-algèbre de la \( \mathbb{Q} \)-algèbre \( (\mathbb{C}, +, \cdot) \).
(\( \cdot \) : restriction du produit à \( \mathbb{Q} \times \mathbb{C} \)).
\( \mathbb{Q}[a] \) est de dimension finie : elle est engendrée par \((1, a, \ldots a^{d-1})\) 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 \((1, a, \ldots a^{d-1})\).

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 \( \varphi \in L_\mathbb{Q}(\mathbb{Q}[a]) \).
\( \ker \varphi = \{ y \in \mathbb{Q}[a], x_0 y = 0 \} = \{ 0 \} \)
Donc \( \varphi \) est injective, donc bijective (car \( \mathbb{Q}[a] \) est de dimension finie)
Donc \( \varphi \) 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 \( \deg(PQ) = \deg(P) + \deg(Q) \).
• Soit \( K \) un corps.
On définit le corps \( K(X) \) des fractions rationnelles en l’indéterminée \( X \).
De même que précédemment, \( (K(X))(Y) \) sera noté plutôt \( K(X,Y) \).

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

Définition :
Pour \( a, b \in \mathbb{Z} \), \( a \equiv b \ [n] \iff n | b - a \).

Théorème :
La relation de congruence est une relation d’équivalence compatible avec + et \( \times \) (de \( \mathbb{Z} \)).

Compatibilité de + :
\[
\forall (x, x', y, y') \in \mathbb{Z}^4, \quad x \equiv x' \ [n], \quad y \equiv y' \ [n] \implies x + y \equiv x' + y' \ [n]
\]

Compatibilité de \( \times \):
Soit \( (x, x', y, y') \in \mathbb{Z}^4 \) tel que \( x \equiv x' \ [n] \), \( y \equiv y' \ [n] \)
Il existe alors \( k \in \mathbb{Z} \) tel que \( x - x' = kn \), et \( l \in \mathbb{Z} \) tel que \( y - y' = ln \).
Alors \( xy - x'y' = \ldots = n(ky + lx + nkl) \), donc \( xy \equiv x'y' \ [n] \).

Plus généralement :
Soit \( A \) un anneau, \( I \) un idéal de \( A \).
On définit \( R \) sur \( A \) par : \( xRy \iff x - y \in I \).
Alors \( R \) 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 \( n = 4 \):
\[
\mathbb{Z}/4\mathbb{Z} = \{0 = 4\mathbb{Z}, 1 = 1 + 4\mathbb{Z}, 2 = 2 + 2\mathbb{Z}, 3 = 3 + 3\mathbb{Z}\} \subset P(\mathbb{Z})
\]
On définit deux relations binaires entre \( \mathbb{Z}/n\mathbb{Z}^2 \) et \( \mathbb{Z}/n\mathbb{Z}^3 \) :
\[
R_+: \forall (a, b, c) \in \mathbb{Z}/n\mathbb{Z}^3, (a, b)R_+ c \iff \exists x \in a, \exists y \in b, c = x + y
\]
\[
R_\times : \forall (a, b, c) \in \mathbb{Z}/n\mathbb{Z}^3, (a, b)R_\times c \iff \exists x \in a, \exists y \in b, c = x \times y
\]

Théorème :
Soit \( n \geq 2 \).

1. \( R_+ \) et \( R_\times \) sont des applications de \( \mathbb{Z}/n\mathbb{Z}^3 \) dans \( \mathbb{Z}/n\mathbb{Z}^3 \).
On les note \( a_+: (a, b) \mapsto a +_n b \), \( a_\times : (a, b) \mapsto a \times_\times b \).

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

3. Soit \( \pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \) la surjection canonique de \( \mathbb{Z} \) sur \( \mathbb{Z}/n\mathbb{Z} \).
\( \chi \mapsto \bar{\chi} \)
Alors \( \pi_+ \) est un morphisme surjectif d’anneaux de \( (\mathbb{Z}, +, \times) \) dans \( (\mathbb{Z}/n\mathbb{Z}, +_n, \times_\times) \) et de noyau \( n\mathbb{Z} \).
(4) $\pi_{n/\mathbb{Z}}$ est bijective, et ainsi $\mathbb{Z}/n\mathbb{Z}$ est de cardinal $n$.

**Démonstration** :

(1) : Pour $R_\pi$, 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 $\overline{x} = a$, $\overline{y} = b$.

Alors, par définition de $R_\pi$, $(a, b)R_\pi x + y$

**Unicité** :

Supposons que $(a, b)R_\pi c$ et $(a, b)R_\pi c'$.

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

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

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

(2) : éléments de réponse :

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

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

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

(3) : $\pi_n$ est un morphisme d’anneaux par définition de $+_n$ et $\times_n$ :

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

(4) : faire une division euclidienne.

**Exemple** :

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

On note $a_1, a_6$ ces deux derniers chiffres. Ainsi, $N \equiv 10a_1 + a_6 [100]$.

Remarque :

$x \equiv y [100] \iff 4 \times 25 \mid x - y \iff 4 \mid x - y$ et $25 \mid x - y \iff x \equiv y [4]$ et $x \equiv y [25]$ (Car $4 \times 25 = 1$)

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

- modulo 4 :
  $\overline{N} = \overline{3^{2005}} = \overline{-1}$. Donc $N \equiv -1 [4]$.

- modulo 25 :
  $\overline{N} = \overline{3^{2005}}$

  $\overline{3^0} = \overline{1}$  $\overline{3^1} = \overline{3}$  $\overline{3^2} = \overline{9}$  $\overline{3^3} = \overline{2}$  $\overline{3^4} = \overline{6}$  $\overline{3^5} = \overline{18} = \overline{-7}$

  Division euclidienne de 2005 par 20 :

  2005 = 20×100 + 5.

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

  Donc $N \equiv -7 [25]$.

- modulo 100 :
  Avec une méthode simple :

  18 $\equiv -7 [25]$ mais 18 $\not\equiv -1 [4]$


  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) $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$ 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 $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$.  
- $\{\bar{x}\}$ engendre $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$.

Démonstration :
(1) : $\bar{T}$ engendre $\mathbb{Z}/n\mathbb{Z}$.
(2) :
$x \wedge n = 1 \iff \exists (u,v) \in \mathbb{Z}, ux + vn = 1$

$\iff \exists (u,v) \in \mathbb{Z}, ux = 1 [n]$

$\iff \bar{x} \in \mathbb{Z}/n\mathbb{Z}^*$

D'où déjà l'équivalence entre les deux premiers tirets.
Supposons que $\bar{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$.
Il existe alors $y \in \mathbb{Z}$ tel que $\bar{x} \times_n \bar{y} = \bar{T}$. On peut supposer que $y \in \mathbb{N}$.

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

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

Donc $\mathbb{Z}/n\mathbb{Z} = \text{gr}(\{\bar{x}\})$ (car $\bar{T}$ est générateur de $\mathbb{Z}/n\mathbb{Z}$).
Si maintenant $\{\bar{x}\}$ engendre $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$, alors il existe $y \in \mathbb{N}$ tel que $\bar{T} = y \cdot \bar{x}$, et donc $\bar{T} = \bar{y} \times_n \bar{x}$. 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) $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$ est un corps.
(3) $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$ est un anneau intègre.

Démonstration :
(1) $\Rightarrow$ (2) :
Soit $y \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$.
Il existe alors $p \not\in n\mathbb{Z}$ 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) $\Rightarrow$ (3) : ok
(3) $\Rightarrow$ (1) : montrons la contraposée :
Supposons non(1). Alors $n = a \times b$ ou $a, b \geq 2$

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

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

En général, on note plutôt $(\mathbb{Z}/n\mathbb{Z},_n^+_n)$ que $(\mathbb{Z}/n\mathbb{Z},_n^+_n \times_n)$.
Notation : Si \( p \) est premier, \((\mathbb{Z}/p\mathbb{Z},+)\) est un corps, noté \( \mathbb{F}_p \) : corps de Galois de cardinal \( p \).

Pour \( n \in \mathbb{N} \), on pose \( \varphi(n) = \#((\mathbb{Z}/n\mathbb{Z})^*) \).
\( \varphi \) 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 \( \varphi \), on pose \( \varphi(1) = 1 \).

E) Passage au quotient modulo \( n \).

Problème :
Soit \((G,\cdot)\) un groupe, et \( \sigma : (\mathbb{Z},+) \rightarrow (G,\cdot) \) un morphisme de groupe.
Existe-t-il \( \varphi \) morphisme de \((\mathbb{Z}/n\mathbb{Z},+)\) dans \((G,\cdot)\) tel que \( \sigma = \varphi \circ \pi_n \) (« \( \sigma \) peut-il se factoriser par \( \pi_n \) ? ») :

\[
\begin{array}{ccc}
(\mathbb{Z},+) & \xrightarrow{\sigma} & (G,\cdot) \\
\downarrow \pi_n & & \uparrow \varphi \\
(\mathbb{Z}/n\mathbb{Z},+) & & \\
\end{array}
\]

Théorème (pour les groupes) :
Soit \((G,\cdot)\) un groupe. Alors \( \sigma \) se factorise par \( \pi_n \) 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 \( \sigma(n) = \varphi \circ \pi_n(n) = \varphi(0) = e_G \) (car \( \varphi \) est un morphisme)
Condition suffisante :
Supposons que \( n\mathbb{Z} \subset \ker \sigma \).
On considère la relation binaire \( R \) de source \( \mathbb{Z}/n\mathbb{Z} \) et de but \( G \) définie par :
\( \forall (a,g) \in \mathbb{Z}/n\mathbb{Z} \times G, aRg \Leftrightarrow \exists p \in \mathbb{Z}, a = \bar{p} \text{ et } g = \sigma(p) \).
Montrons que \( R \) est une application :
Pourtout \( a \in \mathbb{Z}/n\mathbb{Z} \), \( a \) s’écrit \( \bar{p} \), et \( a \) a au moins une image, à savoir \( g = \sigma(p) \).
Unicité : si \( aRy \) et \( aRy' \), 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 \( \sigma(p + kn) = \sigma(p) = y \).
Donc \( R \) est une application. De plus, c’est un morphisme de groupes (…) Ainsi, \( \sigma \) se factorise par \( \pi_n \), et \( \sigma = R \circ \pi_n \).

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 \( \sigma = \varphi \circ \pi_n \) ?

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
Théorème (pour les anneaux) :
\( \sigma \) se factorise par \( \pi_n \) 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 \( \varphi : (\mathbb{Z}/n\mathbb{Z},+) \to (A,+) \) 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 \( \varphi(1) = 1_A \).

Déjà, \( \varphi(1) = \sigma(1) = 1_A \).

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

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

Généralisation (hors programme) :
Groupe quotient :
Soit \( (G,*) \) un groupe, \( H \) un sous-groupe de \( G \).

On définit dans \( G \) deux relations binaires \( R_H \) et \( _H R \) par :
\( \forall (x,y) \in G^2, xR_H y \iff x \ast y^{-1} \in H \)
\( \forall (x,y) \in G^2, _H R y \iff y^{-1} \ast x \in H \)

Alors \( R_H \) et \( _H R \) sont des relations d'équivalence (…)

Théorème :
Les propriétés suivantes sont équivalentes :
(1) \( H \) est un sous-groupe distingué de \( G \).
(2) \( R_H \) est compatible avec \( * \).
(3) \( _H R \) est compatible avec \( * \).
(4) \( R_H = _H R \).
(5) Il existe une loi \( T \) sur \( G/R_H \) telle que \( (G,\times) \to (G/R_H, T) \) soit un morphisme.
\[ g \mapsto Cl_{R_H}^T(g) \]
(6) Il existe une loi \( T \) sur \( G/_H R \) telle que \( (G,\times) \to (G/_H R, T) \) soit un morphisme.
\[ g \mapsto Cl_{_H R}^T(g) \]

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

Démonstration (du théorème) :
Déjà, (1) \( \Rightarrow \) (2) :
Soient \( (x,y),(x',y') \in G^2 \), supposons que \( xR_H y \) et \( x'R_H y' \).
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) \( \Rightarrow \) (5) (…)

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
(5) \(\Rightarrow\) (1) : si \(g \mapsto Cl(g)\) pour \(R_H\) est un morphisme, son noyau qui est \(\ker \phi = Cl(e_g) = H\) est distingué.

De même, (1) \(\Rightarrow\) (3) \(\Rightarrow\) (6) \(\Rightarrow\) (1).

Enfin, (1) \(\Leftrightarrow\) (4).

Pour les anneaux (commutatifs) :
Soit \(I\) un idéal de \((A,+,\times)\).
On définit \(R\) par : \(\forall (x,y) \in A^2\), \(xRy \iff x - y \in I\)

Théorème :
(1) \(R\) est une relation d’équivalence, compatible avec + et \(\times\).
(2) On peut munir \(A/R\) (qu’on note \(A/I\)) de deux lois \(+_I\) et \(\times_I\) telles que 
\((A/I,+,\times_I)\) est un anneau et \(\pi : A \to A/I\) (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 
\(A \to B\).

Pour les groupes :
Soit \((G,\ast)\) un groupe, et \(H\) un sous-groupe distingué.
Soit \(\sigma\) un morphisme de \((G,\ast)\) dans un groupe \((G',\ast')\).

Existe-t-il \(\phi\) morphisme de groupe tel que \(\sigma = \phi \circ \pi\) ?

\[
\begin{array}{ccc}
(G,\ast) & \xrightarrow{\sigma} & (G',\ast') \\
\downarrow\pi & & \uparrow\phi \\
(G/H,T) & & \\
\end{array}
\]

Oui si et seulement si \(H \subset \ker \sigma\).

Enoncé analogue pour les anneaux

**IV Application des anneaux** \(\mathbb{Z}/n\mathbb{Z}\).

**A) Au groupe monogène**

Théorème :
Soit \((G,\ast)\) un groupe, et \(g \in G\).
(1) \(\sigma_g : n \in (\mathbb{Z},+) \mapsto g^n \in (G,\ast)\) est un morphisme de groupes d’image \(\text{gr}(g)\), 
sous-groupe engendré par \(\{g\}\).
(2) Si \(\sigma_g\) est injectif, c’est un isomorphisme entre \((\mathbb{Z},+)\) et \(\text{gr}(g)\).
(3) Si \(\sigma_g\) n’est pas injectif, alors :
- Il existe \(n \geq 1\) tel que \(\ker \sigma_g = n\mathbb{Z}\).
- \(\sigma_g\) passe au quotient par \(n\mathbb{Z}\), c’est-à-dire qu’il existe un morphisme 
\(\overline{\sigma}_g : (\mathbb{Z}/n\mathbb{Z},+) \to (G,\ast)\) tel que \(\forall x \in \mathbb{Z}, \sigma_g(x) = \overline{\sigma}_g(Cl_e(x))\)
- \(\overline{\sigma}_g\) est un isomorphisme de \((\mathbb{Z}/n\mathbb{Z},+)\) dans \((\text{gr}(g),\ast)\).
Démonstration :
(2) si \( \sigma \) est injectif, c’est un isomorphisme entre sa source et son image \((\text{gr}(g),\ast)\)
(3) si \( \sigma \) n’est pas injectif :
- ker\( \sigma \) 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 \(n\mathbb{Z} \subset \ker\sigma\), \(\sigma\)
passe au quotient par \(n\mathbb{Z}\).
- On sait que \(\overline{\sigma}\) est un morphisme surjectif.
Etude de ker\( \overline{\sigma} \) : soit \(a \in \mathbb{Z}/n\mathbb{Z}\), supposons que \(\overline{\sigma}(a) = e_G\).
Soit \(x \in \mathbb{Z}\) tel que \(Cl_x(a) = a\). On a alors \(\overline{\sigma}(a) = \overline{\sigma}(x) = e_G\).
Donc \(x \in n\mathbb{Z}\), soit \(a = \overline{0}\). Donc \(\overline{\sigma}\) 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 \(\sigma\) est injectif.
(2) Soit \(G = \text{gr}(g)\) cyclique tel que \(#G = n\).
Alors \(\sigma : m \in (\mathbb{Z},+) \mapsto g^m \in (G,\ast)\) n’est pas injectif car \(\mathbb{Z}\) est infini.
Donc ker\( \sigma = m\mathbb{Z} \), pour \(m \geq 1\). Donc \(\sigma\) passe au quotient en un isomorphisme
\(\overline{\sigma} : (\mathbb{Z}/m\mathbb{Z},+) \rightarrow (G,\ast)\). Comme \(\sigma\) est une bijection, \(m = n\).

Exemple :
Le groupe des racines \(n\)-ièmes de l’unité \((\mu_n,\times)\)
\(\mu_n = \{z \in \mathbb{C}, z^n = 1\}\).
\(\mu_n\) est un sous-groupe de \((\mathbb{C}^\ast,\times)\), noyau du morphisme \(z \mapsto z^n\), et \(#\mu_n = n\).
Proposition :
\((\mu_n,\times)\) est un groupe cyclique, et \(\omega_k = e^{2\pi i/k}\) engendre \(\mu_n\) si et seulement si \(k \wedge n = 1\), c’est-à-dire si et seulement si \(\forall p \in \{1,...,n-1\}, \omega_k^p \neq 1\).
Dénomination :
Un tel \(\omega_k\) est une racine primitive \(n\)-ième de l’unité.
Démonstration :
Soit \(\omega = e^{2\pi i/n}\). On a \(\text{gr}(\omega) = \mu_n\) car \(\forall k \in [0,n-1], \omega_k = \omega^k\).
Donc \(\mu_n\) est cyclique.
Soit \(\sigma : (\mathbb{Z},+) \rightarrow (\mu_n,\times)\), morphisme surjectif.
\(k \mapsto \omega_k\)
Alors \(\mu_n\) passe au quotient par \(\overline{\sigma} : (\mathbb{Z}/n\mathbb{Z},+) \rightarrow (\mu_n,\times)\), isomorphisme.
Or, \(\forall k \in [0,n-1], \omega^k = \sigma(k) = \sigma(Cl_x(k))\).
Donc \(\omega_k\) engendre \(\mu_n\) si et seulement si \(Cl_x(k)\) engendre \((\mathbb{Z}/n\mathbb{Z},+)\), c’est-à-dire si et seulement si \(k \wedge n = 1\).
Montrons maintenant que \( k \land n = 1 \Leftrightarrow \forall p \in \{1,\ldots,n-1\}, \omega_k^p \neq 1 \)

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

Alors \( n \mid pk \), donc d'après le théorème de Gauss \( n \mid p \).

Supposons que \( k \land n = d \geq 2 \).

Soit \( k' \) tel que \( k'd = k \), \( n' \) tel que \( n'd = n \) (\( n' \in \mathbb{N} \setminus \{1\} \)).

Alors \( \omega_k^p = e^{\frac{2\pi ip}{n}} = e^{2\pi ik'} = 1 \).

**B) Ordre d’un élément (hors programme)**

**Définition :**

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

1. Si \( \sigma_g \) 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 \( \forall (k,l) \in \mathbb{Z}^2, g^k \ast g^l = g^{k+l} \Leftrightarrow k \equiv l \pmod{n} \) 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)**

**Cas d’un groupe abélien fini :**

Soit \((G,\ast)\) un groupe abélien de cardinal \( n \).

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

**Démonstration :**

\( x \in G \mapsto g \ast x \in G \) est une bijection (car d’inverse \( x \in G \mapsto g^{-1} \ast x \in G \))

Donc \( \prod_{x \in G} x = \prod_{x \in G} g \ast x = g^n \prod_{x \in G} x \).

Donc par régularité \( g^n = e_G \).

**Théorème de Lagrange :**

Soit \((G,\ast)\) 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 ordre \( g = \# H \mid \# G \).

**Démonstration :**

Considérons la relation binaire \( R \) définie sur \( G^2 \) par :

\( \forall (x,y) \in G^2, xRy \Leftrightarrow xy^{-1} \in H \).
Alors déjà $R$ est une relation d’équivalence. 

Soit $x_0 \in G$, on cherche $Cl_R(x_0)$.

Soit $y \in Cl_R(x_0)$. Alors $y \cdot x_0^{-1} \in H$. Soit $h \in H$ tel que $h = y \cdot x_0^{-1}$.

Donc $y = h \cdot x_0$.

Donc $Cl_R(x_0) \subseteq \{ x_0 \cdot h, h \in H \}$, et l’autre inclusion est évidente.

Donc $\#Cl_R(x_0) = \#H$ car $h \mapsto h \cdot x_0$ 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 $\pi_n : (\mathbb{Z},+) \to (\mathbb{Z}/n\mathbb{Z},+)$ est un morphisme de groupes (resp. d’anneaux en $x \mapsto Cl_n(x)$

adaptant).

$\pi_n : (\mathbb{Z}/n\mathbb{Z},+) \to (\mathbb{Z}/m\mathbb{Z},+)$

$\uparrow \phi$

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

Autrement dit, $(\mathbb{Z}/m\mathbb{Z},+) \to (\mathbb{Z}/n\mathbb{Z},+)$ est une application si et seulement si $n|m$, $Cl_m(x) \to Cl_n(x)$

et dans ce cas c’est un morphisme de groupes (resp. d’anneaux).

- Théorème chinois :

Soient $n,m \geq 1$, et $\psi : (\mathbb{Z}/nm\mathbb{Z},+) \to (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},+)$.

$Cl_{nm}(x) \mapsto (Cl_n(x), Cl_m(x))$

Alors $\psi$ est une application, c’est même un morphisme d’anneaux, et c’est un isomorphisme si et seulement si $n \cdot m = 1$.

Démonstration :

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

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 $a = Cl_{nm}(x)$.

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

- Si $n \cdot m = 1$, alors $a \in \ker \psi \Rightarrow nm|x$, donc $a = 0$, donc $\psi$ est injective.

- Si $n \cdot m \neq 1$, on pose $x = n \cdot m$ ; alors $x \notin nm\mathbb{Z}$, donc $\psi(Cl_{nm}(x)) = (0,0)$ et $Cl_{nm}(x) \neq 0$, donc $\psi$ 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 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

\[
\begin{cases}
    x \equiv b_1 [N_1] \\
    x \equiv b_2 [N_2]
\end{cases}
\]

si et seulement si $x \equiv b_1 a_1 N_1 + b_2 a_2 N_2 = b_1 a_1 N_1 \wedge N_2$.

En effet :
\[
Cl_{N_1}(x) = Cl_{N_1}(b_1 a_1 N_1) \times Cl_{N_1}(b_1) = Cl_{N_1}(b_1)
\]

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 $N_1 \wedge N_2 = 1$.

Exemples :
Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l’équation $x^2 + ax + b = 0$.
On a :
\[
x^2 + ax + b = 0 \iff (x + \frac{a}{2})^2 + b - \frac{a^2}{4} = 0 \iff (x + \frac{a}{2})^2 = -a^2 - b = \frac{a^2 + 4b}{4}.
\]
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 $\Delta = 0$, $x = -\frac{a}{2} = -\frac{3a}{2} = 2a$
- Si $\Delta$ est un carré non nul, $\Delta = \delta^2$ :
\[
\left(x + \frac{a}{2}\right)^2 - \left(\delta  \frac{2}{2}\right)^2 = 0 \iff \left(x + \frac{a - \delta}{2}\right) \left(x + \frac{a + \delta}{2}\right) = 0
\]
\[
\iff x = -\frac{a \pm \delta}{2}
\]
Résoudre dans $\mathbb{Z}/143\mathbb{Z}$ l’équation $x^2 - 4x + 3 = 0$.
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 $n^2 - 4n + 3 = (n - 1)(n - 3)$ (dans n’importe quel $\mathbb{Z}/k\mathbb{Z}$).
Donc $11 \mid n^2 - 4n + 3 \iff n \equiv 1 [11]$ ou $n \equiv 3 [11]$, (car $\mathbb{Z}/11\mathbb{Z}$ est un corps)
Et de même $13 \mid n^2 - 4n + 3 \iff n \equiv 1 [13]$ ou $n \equiv 3 [13]$. 

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
Donc $x$ est solution si et seulement si \[ \begin{cases} n \equiv 1 \pmod{13} \text{ ou } n \equiv 3 \pmod{13} \\ n \equiv 1 \pmod{11} \text{ ou } n \equiv 3 \pmod{11} \end{cases} \]

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

Pour le dernier, méthode de Bézout :
On cherche $n$ tel que $n \equiv 1 [11]$ et $n \equiv 3 [13] :
13 = 11 \times 1 + 2
11 = 2 \times 5 + 1.
Donc $1 = 11 - (13 - 11 \times 1) \times 5
1 = 6 \times 11 - 5 \times 13

Ainsi, on peut prendre $n = \frac{3 \times 6 \times 11 - 1 \times 5 \times 13}{11 - 13}$.

- 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 :
     $\forall n, m \in \mathbb{N}^*, n \wedge m = 1 \Rightarrow \varphi(n \times m) = \varphi(n) \times \varphi(m)$.
  2. Si $n = p_1^{\alpha_1} \times \ldots \times p_r^{\alpha_r}$, où les $p_j$ sont des nombres premiers deux à deux distincts $\alpha_j \geq 1$, alors $\varphi(n) = \prod_{j=1}^r \left( p_j^{\alpha_j} - p_j^{\alpha_j-1} \right) = n \prod_{j=1}^r \left( 1 - \frac{1}{p_j} \right)$.

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

Conséquence :
$\forall n \in \mathbb{Z}, n \wedge 20 = 1 \Rightarrow n^8 \equiv 1 [20]$.

En effet, il suffit d’appliquer le théorème de Lagrange à $(\mathbb{Z}/20\mathbb{Z})^*$ 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 $n^8 \equiv 1 [20]$.

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

On dispose d’un isomorphisme d’anneaux :
$\psi : (\mathbb{Z}/nm\mathbb{Z}, +, \times) \rightarrow (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times)$.
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, $\varphi(nm) = \#(\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/m\mathbb{Z}^*) = \varphi(n) \varphi(m)$

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

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

---

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
\[ \varphi(p^a) = \text{nombre de } k \in \mathbb{Z}, p^a \text{ tels que } k \land p^a = 1 \]
\[ = \text{nombre de } k \in \mathbb{Z}, p^a \text{ tels que } p \nmid k. \]
\[ = p^a - p^{a-1}. \]
\( (\text{car } \# \{ k \in \mathbb{Z}, p^a \mid p \mid k \} = \# \{ p, i \in \mathbb{Z}, p^{a-1} \} = p^{a-1} ) \)

**V Caractéristique d’un corps, corps premier**

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

\[
\begin{align*}
n \mapsto n1_{\overline{K}} \\
n1_{\overline{K}} = \begin{cases} 
0 & \text{si } n = 0 \\
1_{\overline{K}} + \ldots + 1_{\overline{K}} & \text{si } n > 0 \\
-(n1_{\overline{K}}) & \text{si } n < 0 
\end{cases}
\end{align*}
\]

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

Théorème :

1. \( \tau \) est un morphisme d’anneaux (! Pas de corps : \( \mathbb{Z} \) n’est pas un corps).
2. Si \( \tau \) 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 \( p\mathbb{Z} \) :  
   \[
   (\mathbb{Z},+;\times) \xrightarrow{\pi_p} (\overline{\mathbb{Z}},+;\times) \xrightarrow{\tau} \overline{\mathbb{Z}} 
   \]
   \( \pi_p \downarrow \uparrow \tau \) où \( \tau \) est un morphisme de corps.

3. Si \( \tau \) est injectif, on peut le prolonger en un morphisme de corps :

\[
\tau : \mathbb{Q} \rightarrow \overline{K} \quad \text{où} \quad \frac{\tau(a)}{\tau(b)} \text{ est indépendant du choix de } (a,b) \text{ tel que } r = \frac{a}{b}.
\]

Définition :

Si \( \tau \) est injectif, on dit que \( \overline{K} \) est de caractéristique 0.

Sinon, on dit que \( \overline{K} \) 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 \( a \times a^{-1} = 1_{\overline{K}} \), donc \( \varphi(a) \times \varphi(a)^{-1} = 1_{\overline{K}} \), d’où \( \varphi(a) \neq 0 \).

Définition :

Si \( \overline{K} \) est de caractéristique \( p \), il contient un sous–corps isomorphe à \( \mathbb{F}_p \) (à savoir \( \tau(\mathbb{F}_p) \)).

Ce corps s’appelle sous–corps premier de \( \overline{K} \) : c’est le plus petit sous–corps de \( \overline{K} \).

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

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 $\tau$ 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 $\tau$ est un morphisme d’anneaux.

On vérifie ensuite que $\bar{\tau}$ est un morphisme de corps…

(Comme il est injectif, sa corestriction à $\bar{\tau}(\mathbb{Q})$ 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 $\bar{\tau}$, on définit : par la restriction de $\times : \mathbb{K}^2 \to \mathbb{K}$ à $\mathbb{Q} \times \mathbb{K}$ (en fait, pour $a \in \mathbb{Q}$, $b \in \mathbb{K}$, $a \cdot b = \bar{\tau}(a) \times b$)

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 $\tau : \mathbb{Z} \to \mathbb{K}$ 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 de Gallois, 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.

**Exemples** :
Soit $\mathbb{K}$ un corps de caractéristique $p$.
Alors $\forall x \in \mathbb{K}, p \cdot x = 0$, et $\varphi : \mathbb{K} \to \mathbb{K}$ est un endomorphisme de corps.

$x \mapsto x^p$

En effet :
- Soit $x \in \mathbb{K}$.
DÉJÀ, $p \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$ (définition de la caractéristique)

Donc $p \cdot x = 1_{\mathbb{K}} \cdot x + 1_{\mathbb{K}} \cdot x + \ldots + 1_{\mathbb{K}} \cdot x = (p \cdot 1_{\mathbb{K}}) \cdot x = 0$.

- DÉJÀ : on a, pour tout $k \in ]1, p - 1], p \mid \mathbb{C}_p^*$. 

---

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
Page 25 sur 32
En effet, \( C_p^k = \frac{p!}{k!(p-k)!} = \frac{p}{k} C_{p-1}^k \), donc \( p|C_p^k \), et comme \( p \land k = 1 \), 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  
\( \varphi(1_\mathbb{K}) = 1_\mathbb{K} \) .  
\( \varphi(x + y) = (x + y)^p = \sum_{k=0}^{p} C_p^k x^k y^{p-k} \). 
Or, \( \forall k \in [1, p-1], C_p^k x^{k} y^{p-k} = 0 \) 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 \( p \) :  
\( \mathbb{F}_p \langle X \rangle \) (fractions rationnelles à une indéterminée)

Théorème de Fermat :  
\( \forall x \in \mathbb{F}_p, x^p = x \), ou encore \( \forall n \in \mathbb{Z}, n^p \equiv n[p] \)

Démonstration :
- Si \( p = 2 \), alors \( n^2 \equiv n[2] \) car \( n^2 \) et \( n \) ont la même parité.
- Si \( p \geq 3 \) :
Montrons par récurrence que \( \forall n \in \mathbb{N}, n^p \equiv n[p] \).
Pour \( n = 0 \) : ok (\( 0 \equiv 0[p] \)).
Soit \( n \in \mathbb{N} \), supposons que \( n^p \equiv n[p] \).
Alors \( (n+1)^p = \sum_{k=0}^{p} C_p^k n^k = 1 + n^p \equiv n + 1[p] \) (car \( p|C_p^k, k \in [1, p-1] \)).

Pour \( n \in \mathbb{Z}, n \equiv m[p] \) 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, \( \forall a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}, a^{p-1} = 1 \).
Donc \( \forall a \in \mathbb{Z}/p\mathbb{Z}, a^{p-1} = a \).

Remarque :
- Pour \( N \geq 2 \), on a (extension du théorème de Fermat) :  
\( \forall n \in \mathbb{Z}, n \land N = 1 \Rightarrow n^{\varphi(N)} = 1 \) (dans \( \mathbb{Z}/N\mathbb{Z} \)).

Théorème de Wilson :  
\( p \in \mathbb{N} \setminus \{0,1\} \) est premier si et seulement si \( (p-1)! \equiv -1[p] \).
Démonstration :
- Si $p$ n’est pas premier, alors $p = ab$, où $a, b \geq 2$.
Si $a \neq b$, alors $a \times b \times (p-1)!$, 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 $\geq 3$ : on va montrer que $\prod_{a \in \mathbb{F}_p^*} a = -1$.

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

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

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

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

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

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

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

(1) Si l’équation $x^2 + \overline{1} = \overline{0}$ n’a pas de solution dans $\mathbb{F}_p^*$ :

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

Donc $-\overline{1} = (-\overline{1})^\frac{p-1}{2}$.

Ainsi, si $x^2 + \overline{1} = \overline{0}$ 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 $-x_0$.

$-\overline{1} = \prod_{a \in \mathbb{F}_p^*} a = \prod_{a \in S} a \times \frac{-\overline{1}}{a} \times x_0 \times (-x_0) \times \frac{p-1}{2}$

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

Donc $-\overline{1} = (-1)^{\frac{p-1}{2}}$, d’où $p \equiv 1 \pmod{6}$.
VII Propriétés générales de $\overline{K}[X]$ et $\overline{K}(X)$ (où $K$ est un corps)

Soit $\overline{K}$ 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 $\overline{K}$-algèbre commutative unitaire de $\overline{K}[X]$.
- Degré d’un polynôme, intégrité de $\overline{K}[X]$ : polynômes unitaires (ou normalisés), degré d’un produit, d’une somme ; sous-$\overline{K}$-espace $\overline{K}_n[X]$ des polynômes de degré au plus $n$.
- Fractions rationnelles, corps $\overline{K}(X)$.
- Multiples et diviseurs d’un polynôme, polynômes associés. Division euclidienne dans $\overline{K}[X]$ ; algorithme de la division euclidienne.
- Polynôme scindé sur $\overline{K}$ ; 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 $\overline{K}[X]$, 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 $P$. Orde 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 $\varphi : P \in \overline{K}[X] \mapsto \overline{P} \in \overline{K}$ qui a un polynôme associe sa fonction polynomiale est injective si, et seulement si, $\overline{K}$ est infini, et on a même le théorème :

1. $\varphi$ est un morphisme d’algèbre.
2. Si $\overline{K}$ est fini, $\varphi$ est injective non surjective.
3. Si $\overline{K}$ est fini, $\varphi$ est surjective non injective, et $\ker \varphi = P_0 \overline{K}[X]$ avec $P_0 = \prod_{a \in \overline{K}} (X - a) = X^q - X$, où $q = \# \overline{K}$.

Lorsque $\overline{K}$ 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 $a_1, a_2, ..., a_r$ des éléments deux à deux distincts de $\overline{K}$.

On a : $\forall i \in [1, r], \overline{P}(a_i) = 0$ (car $\overline{P} = \overline{0}$)

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

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
Page 28 sur 32
(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)
\( \varphi \) n’est pas surjective car la fonction qui vaut \( 1_{\mathbb{K}} \) en \( 0_{\mathbb{K}} \) et 0 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 \( P \in \ker \varphi , \prod_{a \in \mathbb{K}} X - a \bigg| P \); inversement,
\[
\text{si } \prod_{a \in \mathbb{K}} X - a \bigg| P, \text{ alors } \forall a \in \mathbb{K}, \tilde{P}(a) = 0 .
\]

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 \( \prod_{a \in \mathbb{K}} X - a \bigg| X^q - X \). Or, ils sont tous deux unitaires, de degré \( q \), donc égaux.

Surjectivité : toute fonction est polynomiale : interpolation de Lagrange :

Pour \( f : \mathbb{K} \to \mathbb{K} \), 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 \( \sum_{j=0}^{n} a_j X^j \).

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 :
\[
P = \sum_{k=0}^{\infty} \frac{P^{(k)}(a)}{k!} (X - a)^k \quad \text{(somme finie)}
\]
\[
P(a + X) = \sum_{k=0}^{\infty} \frac{P^{(k)}(a)}{k!} X^k = \sum_{k=0}^{\infty} a^k \frac{P^{(k)}}{k!}.
\]
Si \( \mathbb{K} \) est de caractéristique 0, \( a \) est racine de multiplicité \( n \) si et seulement si :
\( P(a) = P'(a) = \ldots = P^{(n-1)}(a) = 0 \).
Faux en caractéristique \( p \) :
Par exemple avec \( \mathbb{K} = \mathbb{F}_p, P = X^p + 1, P' = pX^{p-1} = 0 \).
VIII Etude 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 $(A,+,\cdot)$ muni d’une application

$$
\varphi : A \setminus \{0\} \rightarrow \mathbb{N} \text{ telle que } \forall (a,b) \in A^2, b \neq 0 \Rightarrow \exists (q,r) \in A^2, a = bq + r \text{ et }
\begin{cases} 
\varphi(r) = 0 \\
\varphi(r) < \varphi(q)
\end{cases}
$$

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

Par exemple, les anneau $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ sont des anneau 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 :
  $$P = P_0Q + R \text{ où } \deg R < \deg P_0.$$  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 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 $P_1, P_2, \ldots, P_n \in \mathbb{K}[X] \setminus \{0\}$. Les propositions suivantes sont équivalentes :

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

**Démonstration :**

2. $\Rightarrow$ (1) : ok

3. $\Rightarrow$ (2) : $P_1\mathbb{K}[X] + \ldots + P_n\mathbb{K}[X] = \mathbb{K}[X]$, alors comme $1 \in \mathbb{K}[X]$, il s’écrit sous la forme $\sum_{i=1}^n P_iU_i$. 

Chapitre 5 : Compléments de théorie des ensembles et algèbre générale
Algèbre générale
(1) \implies (3) : on pose \( I = P_1\mathbb{K}[X] + ... + P_n\mathbb{K}[X] \).
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 \( P_i \in I \).
De plus, \( \forall i \in [1,n], P_i \in I \), donc \( P_i \) est multiple de \( D \). Donc \( D \) est constant, et \( I = \mathbb{K}[X] \).

**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 \( A = eP_1^{r_1} ... P_n^{r_n} \) où \( e = \text{cte} \), où les \( P_i \) sont irréductibles (ou premiers) et unitaires et où les \( r_i \) sont des entiers naturels.

**Théorème :**
Soit \( (P_i)_{i \in [1,n]} \) une famille d’éléments non tous nuls de \( \mathbb{K}[X] \). Il existe un unique polynôme unitaire \( D \in \mathbb{K}[X] \) tel que \( \forall R \in \mathbb{K}[X], (\forall i, R \text{ divise } P_i \iff R \text{ divise } D) \).

**Propriétés et définitions :**
\( D \) 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 \( (U_i)_{i \in [1,n]} \) tels que \( D = \sum_{i=1}^{n} U_i P_i \). En fait, \( D \) est le générateur unitaire de l’idéal \( P_1\mathbb{K}[X] + P_2\mathbb{K}[X] + ... + P_n\mathbb{K}[X] \).
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 \( (P_i)_{i \in [1,n]} \) 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 :
\( \forall R \in \mathbb{K}[X], (\forall i, P_i \text{ divise } R \iff M \text{ divise } R) \).

**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 \( \lambda \) 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 $A_1, \ldots, A_n$ des polynômes non nuls ; pour tout polynôme $R$ irréductible unitaire, on pose $\alpha_R = \min_{i\in[1,n]} (V_R(A_i))$, $\beta_R = \max_{i\in[1,n]} (V_R(A_i))$.

Alors $\alpha_R = \beta_R = 0$ sauf pour un nombre fini de $R$.
De plus, $PGCD(A) = \prod_R R^{\alpha_R}$ et $PPCM(A) = \prod_R R^{\beta_R}$.

**Démonstration :**
La même que dans $\mathbb{Z}$.