CH03 : Structures algébriques usuelles

Table des matières

I Groupes

1) Groupes et sous-groupes

Définition 1 (Groupe)
Un **groupe** *est un ensemble G muni d'une loi de composition interne $* : G \times G \to G$ qui vérifie les propriétés suivantes :*

(i) associativité : $\forall (x,y,z) \in G^3,\ x*(y*z) = (x*y)*z$;

(ii) existence d'un élément neutre : $\exists e \in G,\ \forall x \in G,\ x*e = e*x = x$;

(iii) existence d'un symétrique pour tout élément : $\forall x \in G,\ \exists y \in G,\ x*y = y*x = e$.

Notation
Un groupe sera noté $(G,*)$, où G est l'ensemble et $*$ la loi de composition interne.

Définition 2 (Groupe commutatif)
On dit qu'un groupe $(G,*)$ est **commutatif** *lorsque la loi $*$ est (en plus du reste) commutative, c'est-à-dire $\forall (x,y) \in G^2,\ x*y = y*x$.*

Vocabulaire
Un groupe commutatif est aussi appelé **groupe abélien** (en référence au mathématicien norvégien Abel).

Propriété 3 (Propriétés immédiates d'une loi de groupe)
Soit $(G,*)$ un groupe.

(i) L'élément neutre e est unique.

(ii) Tout élément $x \in G$ possède un unique symétrique.

(iii) Tout élément est simplifiable à gauche : $\forall (x,y,z) \in G^3,\ x*y = x*z \implies y = z$.

(iv) Tout élément est simplifiable à droite : $\forall (x,y,z) \in G^3,\ y*x = z*x \implies y = z$.

Preuve (non traitée en classe)

(i) S'il existe deux éléments neutres e et e' dans G, alors on a $e = e*e'$ (car e' est neutre) et $e*e' = e'$ (car e est neutre), donc $e = e'$.

(ii) Soit $x \in G$. Si x' et x'' sont deux symétriques de x, alors $x' = x'*e = x'*(x*x'') = (x'*x)*x'' = x''$.

(iii) Immédiat en multipliant à gauche par le symétrique x' de x (et en utilisant l'associativité).

(iv) Idem à droite.

Notation

- Lorsque la loi du groupe G est notée $*$, $\times$ ou $\cdot$ ("notations multiplicatives"), le neutre sera noté e (ou e_G ou 1 ou 1_G) et le symétrique d'un élément $x \in G$ sera appelé "inverse" et noté x^{-1}. On notera également pour tout $n \in \mathbb{N}$:
$$x^n = x*x*\cdots*x \quad (n\ fois),$$
$$x^{-n} = (x*x*\cdots*x)^{-1} = x^{-1}*\cdots*x^{-1} \quad (n\ fois),$$
avec la convention $x^0 = e$.
- Lorsque la loi du groupe G est notée $+$ ("notation additive"), le neutre sera noté 0 (ou 0_G) et le symétrique d'un élément $x \in G$ sera appelé "opposé" et noté $-x$. On notera également pour tout $n \in \mathbb{N}$:
$$nx = x + x + \cdots + x \quad (n\ fois),$$
$$(-n)x = -(x + x + \cdots + x) = (-x) + (-x) + \cdots + (-x) \quad (n\ fois),$$
avec la convention $0x = 0_G$.
Attention, la notation additive n'est employée que pour des groupes commutatifs.

- Les résultats généraux sur les groupes seront énoncés en notation multiplicative, mais se transposent bien évidemment en notation additive.

Exemple
Exemples classiques de groupes :

- $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes commutatifs, mais $(\mathbb{N},+)$ n'est pas un groupe.
- $(\mathbb{R}^*,\times)$ est un groupe, ainsi que $(\mathbb{C}^*,\times)$.
- Pour tout ensemble X, l'ensemble $S(X)$ des bijections $X \to X$ est un groupe (non commutatif) pour la loi $\circ$ (composition). L'élément neutre est l'application identité $Id_X : X \to X$.
- En particulier, pour tout $n \in \mathbb{N}^*$, l'ensemble S_n des bijections $\{1,\cdots,n\} \to \{1,\cdots,n\}$ est un groupe pour la loi $\circ$, appelé **groupe symétrique d'ordre n** (ou **groupe des permutations d'ordre n**). S_n est fini, de cardinal $n!$.
- Pour $n \in \mathbb{N}^*$, $(GL_n(\mathbb{R}),\times)$ (matrices inversibles) est un groupe non commutatif. L'élément neutre est la matrice identité I_n.

Rappel (Produit fini d'ensembles)
Si $n \in \mathbb{N}^*$ et $E_1,\cdots,E_n$ sont des ensembles, alors le **produit cartésien** $E_1 \times \cdots \times E_n$ est l'ensemble des listes (appelées aussi n-uplets) $(x_1,\cdots,x_n)$, avec $x_1 \in E_1,\cdots,x_n \in E_n$, et on a

$$(x_1,\cdots,x_n) = (y_1,\cdots,y_n) \iff \forall i \in \{1,\cdots,n\},\ x_i = y_i.$$

Propriété 4 (Produit fini de groupes)
Soit $n \in \mathbb{N}^*$ et $(G_1,*_1),\cdots,(G_n,*_n)$ des groupes. Alors, l'ensemble $G_1 \times \cdots \times G_n$ muni de la loi de composition interne :

$$(x_1,\cdots,x_n) * (y_1,\cdots,y_n) = (x_1 *_1 y_1,\cdots,x_n *_n y_n)$$

est un groupe. L'élément neutre est $(e_1,\cdots,e_n)$ (où e_i est le neutre de G_i pour tout i), et pour tout $(x_1,\cdots,x_n) \in G_1 \times \cdots \times G_n$, on a

$$(x_1,\cdots,x_n)^{-1} = (x_1^{-1},\cdots,x_n^{-1}),$$

où x_i^{-1} désigne le symétrique de x_i dans G_i pour tout i).
Ce groupe $(G_1 \times \cdots \times G_n,*)$ est appelé **groupe produit** *des groupes $(G_1,*_1),\cdots,(G_n,*_n)$.*

Preuve laissée en exercice
Vérifications immédiates (bien qu'un peu fastidieuses).

Exemple
Sur l'ensemble $\mathbb{R}^2$, on définit la loi $+$ par :

$$\forall (x,y),(x',y') \in \mathbb{R}^2 \times \mathbb{R}^2, \qquad (x,y)+(x',y') = (x+x',y+y').$$

$(\mathbb{R}^2,+)$ est ainsi un groupe commutatif, de neutre $(0,0)$.

Définition 5 (Sous-groupe)
Soit $(G,*)$ un groupe de neutre e. On dit qu'une partie $H \subset G$ est un **sous-groupe** *de G lorsque :*

(i) $e \in H$;

(ii) H *est stable par* $*$: $\forall (x,y) \in H^2,\ x*y \in H$;

(iii) H *est stable par passage au symétrique :* $\forall x \in H,\ x^{-1} \in H$.

Remarque
Cela revient à dire que la restriction $*_H : H \times H \to H$ (appelée **loi induite** *sur H) est bien définie et que $(H,*_H)$ est un groupe.*

Exemple

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$, qui est lui-même un sous-groupe de $(\mathbb{C}, +)$.
- $(\{-1, 1\}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
- Pour $n \in \mathbb{N}^*$, on note $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$ (ensemble des racines n^e de l'unité). Alors, $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Propriété 6 (Caractérisation d'un sous-groupe)
Soit $(G, *)$ un groupe et $H \subset G$. Alors, H est un sous-groupe de G si et seulement si :

(a) $H \neq \emptyset$;

(b) $\forall (x, y) \in H^2,\ x^{-1} * y \in H$.

Preuve (non traitée en classe)
Montrons que ((*i*) *et* (*ii*) *et* (*iii*) $\iff$ (*a*) *et* (*b*)).

$\boxed{\Rightarrow}$ Si H est un sous-groupe de G, alors il est non vide (d'après (i)), d'où (a).
De plus, si $(x, y) \in H^2$, on a $x^{-1} \in H$ (par (iii)), mais aussi $y \in H$, donc par (ii), $x^{-1} * y \in H$, ce qui montre (b).

$\boxed{\Leftarrow}$ Si (a) et (b) sont vérifiées, alors d'après (a), il existe un élément $x_0 \in H$, donc par (b), $x_0^{-1} * x_0 = e \in H$, ce qui montre (i). Ensuite la propriété (b) utilisée avec $x \in H$ et $y = e$ (qui est bien dans H) entraîne $x^{-1} \in H$, donc (iii). Enfin, étant donné $(x, y) \in H^2$, on réutilise (b) avec x^{-1} (qui est bien dans H) et y, ce qui donne $(x^{-1})^{-1} * y \in H$, c'est-à-dire $x * y \in H$, donc (ii).

Remarque
En pratique, la vérification $H \neq \emptyset$ se fait en montrant que $e \in H$...

Propriété 7 (Intersection de sous-groupes)
Soit I un ensemble d'indices quelconque et $(H_i)_{i \in I}$ une famille de sous-groupes d'un même groupe $(G, *)$. Alors, $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Preuve (non traitée en classe)
On utilise la caractérisation d'un sous-groupe.
Le neutre e est dans chaque H_i (puisque ce sont des sous-groupes), donc $e \in \bigcap_{i \in I} H_i$.
Ensuite, pour tout $(x, y) \in \left(\bigcap_{i \in I} H_i\right)^2$, les éléments x et y sont dans tous les H_i, donc $\forall i \in I,\ x^{-1} * y \in H_i$ (par les propriétés de stabilité des H_i), c'est-à-dire $x^{-1} * y \in \bigcap_{i \in I} H_i$.

ATTENTION !
La réunion d'une famille de sous-groupes n'est pas un sous-groupe en général !
Par exemple, $\mathbb{U}_2 = \{-1, 1\}$ et $\mathbb{U}_3 = \{1, j, j^2\}$ sont deux sous-groupes de $\mathbb{C}^*$ (pour la loi $\times$), mais la réunion $\mathbb{U}_2 \cup \mathbb{U}_3 = \{-1, 1, j, j^2\}$ n'en est pas un car il n'est pas stable par produit (par exemple, $-1 \times j = -j \notin \mathbb{U}_2 \cup \mathbb{U}_3$).

Définition 8 (Sous-groupe engendré par une partie)
Soit $(G, *)$ un groupe et $A \subset G$ une partie (quelconque). On appelle **sous-groupe engendré par** *A l'intersection de tous les sous-groupes de G contenant A.*

Notation
On notera $\langle A \rangle$ le sous-groupe engendré par A :

$$\langle A \rangle = \bigcap_{\substack{H \text{ sg de } G \\ A \subset H}} H.$$

Remarque
Cette définition a du sens car l'intersection porte sur une famille non vide, étant donné qu'il existe toujours un sous-groupe de G contenant A : G lui-même !

Propriété 9 (Caractère minimal du sous-groupe engendré)
Soit $(G,*)$ un groupe et $A \subset G$ une partie (quelconque). Alors $\langle A \rangle$ est le plus petit sous-groupe de G (au sens de l'inclusion) contenant A.

Preuve (non traitée en classe)
En tant qu'intersection de sous-groupes de G contenant A, $\langle A \rangle$ est un sous-groupe de G contenant A.

Si H_0 est un sous-groupe quelconque de G tel que $A \subset H_0$, alors $\langle A \rangle = \left(\bigcap_{\substack{H \text{ sg de } G \\ A \subset H}} H \right) \subset H_0$,

puisque H_0 est l'un des ensembles sur lesquels porte l'intersection.

Notation
Si $a_1, \cdots, a_n$ sont des éléments de G, alors on notera

$$\langle a_1, \cdots, a_n \rangle = \langle \{a_1, \cdots, a_n\} \rangle.$$

Ainsi, pour tout $a \in G$ et $b \in G$:
$\langle a \rangle$ désigne le plus petit sous-groupe de G contenant a,
$\langle a, b \rangle$ désigne le plus petit sous-groupe de G contenant a et b, etc.

Propriété 10 (Description du sous-groupe engendré par un élément)
Soit $(G,*)$ un groupe et $a \in G$. Alors

$$\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}.$$

Preuve
Déjà, il est clair que $\{a^k,\ k \in \mathbb{Z}\} \subset \langle a \rangle$: puisque $\langle a \rangle$ est un sous-groupe de G contenant a, il contient $e = a^0$, a^{-1} et donc par une récurrence évidente toutes les puissances itérées de a et a^{-1}.
Ensuite, l'ensemble $\{a^k,\ k \in \mathbb{Z}\}$ est un sous-groupe de G, puisque $e = a^0 \in H$ et $\forall (k,k') \in \mathbb{Z}^2$, $(a^k)^{-1} * a^{k'} = a^{k'-k}$. Vu que $\langle a \rangle$ et $\{a^k,\ k \in \mathbb{Z}\}$ sont deux sous-groupes de G contenant a, on a $\langle a \rangle \subset \{a^k,\ k \in \mathbb{Z}\}$ d'après le caractère minimal du sous-groupe engendré.

Remarque
Pour tout $a \in G$, le sous-groupe $\langle a \rangle$ est commutatif, même si le groupe G ne l'est pas.

Théorème 11 (Sous-groupes de $(\mathbb{Z},+)$)
Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$, avec $n \in \mathbb{N}$.

Remarque
Les sous-groupes de $(\mathbb{Z},+)$ sont donc les sous-groupes engendrés $\langle n \rangle$, $n \in \mathbb{N}$.

Preuve
Soit H un sous-groupe de $(\mathbb{Z},+)$.

- Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
- Sinon, H contient au moins un élément non nul et son opposé (par stabilité), donc H contient au moins un élément strictement positif. Notons $n = \min(H \cap \mathbb{N}^*)$ (existe car $H \cap \mathbb{N}^*$ est non vide dans $\mathbb{N}$). Etant donné $x \in H$, on peut écrire, par division euclidienne :

  $$x = nq + r, \qquad (q,r) \in \mathbb{N} \times \{0, \cdots, n-1\}.$$

  Vu que n et x sont dans H, on a $r = x - nq \in H \cap \{0, \cdots, n-1\}$, donc nécessairement $r = 0$ (puisque $r > 0$ entrainerait $r \geq n$). D'où $x = nq$, ce qui montre $H \subset \langle n \rangle$ avec $n \in \mathbb{N}^*$.

Enfin, H étant un sous-groupe de $(\mathbb{Z},+)$ contenant n, on a automatiquement $\langle n\rangle \subset H$, donc $H = \langle n\rangle$.

Ceci montre que tout sous-groupe de $(\mathbb{Z},+)$ est de la forme $H = n\mathbb{Z}$.
Réciproquement, pour tout $n \in \mathbb{N}$, $n\mathbb{Z} = \langle n\rangle$ est bien un sous-groupe de $(\mathbb{Z},+)$, d'où le résultat.

2) Morphismes de groupes

Définition 12 (Morphisme de groupes)
Soit $(G,*)$ et $(G',\top)$ deux groupes. Un **morphisme de groupes** *de G dans G' est une application $\varphi : G \to G'$ telle que $\forall (x,y) \in G^2,\ \varphi(x*y) = \varphi(x)\top\varphi(y)$.*

Propriété 13 (Propriétés immédiates des morphismes de groupes)
Soit $\varphi : (G,*) \to (G',\top)$ un morphisme de groupes. Alors

(i) $\varphi(e_G) = e_{G'}$;

(ii) $\forall x \in G,\ \varphi(x^{-1}) = \varphi(x)^{-1}$.

Preuve (non traitée en classe)

(i) $\varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G)\top\varphi(e_G)$, donc en multipliant à gauche par $\varphi(e_G)^{-1}$, on obtient $e_{G'} = \varphi(e_G)$.

(ii) Pour tout $x \in G$, on a $\varphi(x^{-1})\top\varphi(x) = \varphi(x^{-1} * x) = \varphi(e_G) = e_{G'}$, et de même façon : $\varphi(x)\top\varphi(x^{-1}) = e_{G'}$, donc $\varphi(x^{-1})$ est bien l'inverse de $\varphi(x)$ dans G'.

Propriété 14 (Composée de deux morphismes de groupes)
La composée de deux morphismes de groupes en est un.

Preuve (non traitée en classe)
Soit $\varphi : (G,*) \to (G',\top)$ et $\psi : (G',\top) \to (G'',\perp)$ deux morphismes de groupes. On a $\forall (x,y) \in G^2$:

$$(\psi\circ\varphi)(x*y) = \psi(\varphi(x*y)) = \psi(\varphi(x)\top\varphi(y)) = \psi(\varphi(x))\perp\psi(\varphi(y)) = (\psi\circ\varphi)(x)\perp(\psi\circ\varphi)(y),$$

donc $\psi\circ\varphi : (G,*) \to (G'',\perp)$ est un morphisme de groupes.

Propriété 15 (Image directe/réciproque d'un sous-groupe par un morphisme)
Soit $\varphi : (G,*) \to (G',\top)$ un morphisme de groupes. Alors

(i) Pour tout sous-groupe H de G, l'image directe $\varphi(H) = \{\varphi(x),\ x \in H\}$ est un sous-groupe de G'.

(ii) Pour tout sous-groupe H' de G', l'image réciproque $\varphi^{-1}(H') = \{x \in G,\ \varphi(x) \in H'\}$ est un sous-groupe de G.

Preuve

(i) Soit H un sous-groupe de G. On a :
- $e_{G'} = \varphi(e_G)$ avec $e_G \in H$ donc $e_{G'} \in \varphi(H)$.
- si $(a,b) \in \varphi(H)^2$, alors il existe $(x,y) \in H^2$ tels que $a = \varphi(x)$ et $b = \varphi(y)$. Donc
$$a^{-1}\top b = \varphi(x)^{-1}\top\varphi(y) = \varphi(x^{-1})\top\varphi(y) = \varphi(x^{-1} * y),$$
avec $x^{-1} * y \in H$ (par stabilité de H), ce qui montre que $a^{-1}\top b \in \varphi(H)$.

Donc $\varphi(H)$ est bien un sous-groupe de G'.

(ii) Soit H' un sous-groupe de G'. On a :
- $e_G \in \varphi^{-1}(H')$ car $\varphi(e_G) = e_{G'} \in H'$.
- si $(x,y) \in \varphi^{-1}(H')^2$, alors $(\varphi(x),\varphi(y)) \in H'^2$, donc
$$\varphi(x^{-1} * y) = \varphi(x)^{-1}\top\varphi(y) \in H'$$
(par stabilité de H'), ce qui montre que $x^{-1} * y \in \varphi^{-1}(H')$.

Donc $\varphi^{-1}(H')$ est bien un sous-groupe de G.

Définition 16 (Image et noyau d'un morphisme de groupes)
Soit $\varphi : (G, *) \to (G', \top)$ un morphisme de groupes.

(i) On appelle **image** *de φ l'ensemble $Im(\varphi) = \varphi(G)$. C'est un sous-groupe de G'.*

(ii) On appelle **noyau** *de φ l'ensemble $Ker(\varphi) = \varphi^{-1}(\{e_{G'}\})$. C'est un sous-groupe de G.*

Remarque
$Im(\varphi)$ est l'ensemble des éléments de G' qui possèdent au moins un antécédent dans G par φ.
$Ker(\varphi)$ est l'ensemble des antécédents de $e_{G'}$ par φ : $Ker(\varphi) = \{x \in G,\ \varphi(x) = e_{G'}\}$.

Propriété 17 (Caractérisation de l'injectivité/la surjectivité d'un morphisme de groupes)
Soit $\varphi : (G, *) \to (G', \top)$ un morphisme de groupes.

(i) φ est surjectif ssi $Im(\varphi) = G'$;

(ii) φ est injectif ssi $Ker(\varphi) = \{e_G\}$.

Preuve

(i) C'est direct d'après la définition de la surjectivité d'une application : φ est surjective signifie que tout $a \in G'$ possède au moins un antécédent par φ, c'est-à-dire que tout $a \in G'$ est dans $Im(\varphi)$, ou encore que $G' = Im(\varphi)$, puisque l'inclusion $Im(\varphi) \subset G'$ est toujours vraie.

(ii) $\boxed{\Rightarrow}$ Si φ est injectif, alors vu qu'on a déjà $\varphi(e_G) = e_{G'}$, l'élément e_G est le seul antécédent de $e_{G'}$ par φ. Donc $Ker(\varphi) = \{e_G\}$.

$\boxed{\Leftarrow}$ Supposons $Ker(\varphi) = \{e_G\}$ et montrons que φ est injectif. Pour tout $(x, y) \in G^2$:

$$\varphi(x) = \varphi(y) \iff \varphi(x)^{-1} \top \varphi(y) = e_{G'} \iff \varphi(x^{-1} * y) = e_{G'} \iff x^{-1} * y \in Ker(\varphi).$$

L'hypothèse $Ker(\varphi) = \{e_G\}$ entraîne donc

$$\varphi(x) = \varphi(y) \iff x^{-1} * y = e_G \iff x = y,$$

ce qui montre l'injectivité de φ.

Définition 18 (Isomorphisme de groupes)
Un **isomorphisme** *de groupes de $(G, *)$ dans $(G', \top)$ est un morphisme de groupes bijectif de $(G, *)$ dans $(G', \top)$.*

Propriété 19 (Réciproque d'un isomorphisme de groupes)
Si $\varphi : (G, *) \to (G', \top)$ est un isomorphisme de groupes, alors l'application réciproque $\varphi^{-1} : (G', \top) \to (G, *)$ est aussi un isomorphisme de groupes.

Preuve (non traitée en classe)
Puisque $\varphi : G \to G'$ est bijective, l'application réciproque $\varphi^{-1} : G' \to G$ est bien définie (et bijective).
Reste à montrer que φ^{-1} est un morphisme de groupes.
Pour $(a, b) \in G'^2$, on a, en notant $x = \varphi^{-1}(a)$ et $y = \varphi^{-1}(b)$:

$$\varphi^{-1}(a \top b) = \varphi^{-1}(\varphi(x) \top \varphi(y)) = \varphi^{-1}(\varphi(x * y)) = x * y = \varphi^{-1}(a) \top \varphi^{-1}(b),$$

d'où le résultat.

Exemple

- L'exponentielle complexe $\exp : \left\{ \begin{array}{ccc} (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & e^z \end{array} \right.$ est un morphisme de groupes.

- La signature $\varepsilon : \left\{ \begin{array}{ccc} (S_n, \circ) & \longrightarrow & (\{-1,1\}, \times) \\ \sigma & \longmapsto & \varepsilon(\sigma) = \prod\limits_{1 \leq i < j \leq n} \frac{\sigma(j)-\sigma(i)}{j-i} \end{array} \right.$ est un morphisme de groupes.
- Pour $n \in \mathbb{N}^*$ fixé, le déterminant $\det : \left\{ \begin{array}{ccc} (GL_n(\mathbb{R}), \times) & \longrightarrow & (\mathbb{R}^*, \times) \\ A = (a_{i,j})_{1 \leq i,j \leq n} & \longmapsto & \det(A) = \sum\limits_{\sigma \in S_n} \varepsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \end{array} \right.$ est un morphisme de groupes.

Ces trois résultats proviennent du cours de MP2I.

3) Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Propriété 20 (Relation de congruence modulo n)
Soit $n \in \mathbb{N}^*$. La relation définie par

$$\forall (x,y) \in \mathbb{Z}^2 : \quad x \equiv y \ [n] \iff n | y - x$$

est une relation d'équivalence sur $\mathbb{Z}$, appelée la **relation de congruence modulo n**.

Preuve

- Cette relation est réflexive car pour tout $x \in \mathbb{Z}$, on a $x \equiv x \ [n]$, vu que n divise $x - x = 0$ $(0 = n * 0)$.
- Elle est symétrique car pour tout $(x,y) \in \mathbb{Z}^2$, si $x \equiv y \ [n]$, alors n divise $y - x$, donc aussi $x - y$, d'où $y \equiv x \ [n]$.
- Enfin, elle est transitive car pour tout $(x,y,z) \in \mathbb{Z}^3$, si $x \equiv y \ [n]$ et $y \equiv z \ [n]$, alors n divise $y - x$ et $z - y$, donc n divise leur somme $z - x$, c'est-à-dire $x \equiv z \ [n]$.

Notation
Soit $n \in \mathbb{N}^*$ fixé. Pour tout $x \in \mathbb{Z}$, on notera $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n :

$$\overline{x} = \{y \in \mathbb{Z}, \ x \equiv y \ [n]\} = \{x + kn, \ k \in \mathbb{Z}\} = x + n\mathbb{Z}.$$

Propriété 21 (Nombres de classes d'équivalence modulo n)
Soit $n \in \mathbb{N}^*$. Il y a exactement n classes d'équivalence distinctes pour la relation de congruence modulo n :

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}.$$

Preuve
Par division euclidienne, tout entier $x \in \mathbb{Z}$ s'écrit de manière unique $x = nq + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \cdots, n-1\}$, donc tout entier x appartient à une et une seule classe $\overline{r}$, avec $r \in \{0, \cdots, n-1\}$.

Remarque
Comme dans toute relation d'équivalence, les classes forment une partition de l'ensemble. On a donc :

$$\forall n \in \mathbb{N}^*, \qquad \mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \overline{n-1},$$

et les classes sont deux à deux disjointes.

Définition 22 (Ensemble $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Remarque
$\mathbb{Z}/n\mathbb{Z}$ est donc un ensemble fini de cardinal n. C'est un ensemble de parties de $\mathbb{Z}$.
Par exemple : $\overline{0} = n\mathbb{Z}$ est la partie formée des multiples de n.

Théorème 23 (Structure de groupe additif de $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. La loi de composition interne $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ donnée par

$$\forall (x,y) \in \mathbb{Z}^2, \qquad \overline{x} + \overline{y} = \overline{x+y}$$

est bien définie, et $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

Preuve

- La loi $+$ est bien définie car la classe $\overline{x}+\overline{y}$ ne dépend pas des représentants x, y choisis : en effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors on a $x \equiv x'\ [n]$ et $y \equiv y'\ [n]$, donc facilement $x + y \equiv x' + y'\ [n]$, ce qui montre que $\overline{x+y} = \overline{x'+y'}$.
- La loi est commutative puisque pour tout $(x,y) \in \mathbb{Z}^2$: $\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}$.
- La loi est associative car pour tout $(x,y,z) \in \mathbb{Z}^3$:

$$(\overline{x} + \overline{y}) + \overline{z} = \overline{x+y} + \overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} + \overline{y+z} = \overline{x} + (\overline{y} + \overline{z}).$$

- La loi possède un élément neutre : $\overline{0}$, car

$$\forall x \in \mathbb{Z}, \quad \overline{x} + \overline{0} = \overline{0} + \overline{x} = \overline{x+0} = \overline{x}.$$

- Tout élément $\overline{x}$ possède un symétrique ("opposé") : $-\overline{x} = \overline{-x}$, puisque

$$\forall x \in \mathbb{Z}, \quad \overline{x} + \overline{-x} = \overline{-x} + \overline{x} = \overline{x + (-x)} = \overline{0}.$$

4) Groupes monogènes et cycliques

Définition 24 (Groupe monogène, groupe cyclique)
Un groupe $(G, *)$ est dit **monogène** *lorsqu'il est engendré par un élément, c'est-à-dire lorsqu'il existe $a \in G$ tel que $G = \langle a \rangle$. Un tel élément a est alors appelé* **générateur de G**.
Un groupe $(G, *)$ est dit **cyclique** *s'il est monogène et fini.*

Exemple (Sous-groupes de $\mathbb{Z}$)
Tous les sous-groupes de $(\mathbb{Z}, +)$ sont monogènes (cf. théorème 11), et parmi eux, seul $\{0\}$ est cyclique.

Exemple (Groupe des racines n^e de l'unité)
Pour tout $n \in \mathbb{N}^*$, le groupe $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$ (multiplicatif) est cyclique car d'une part :

$$\mathbb{U}_n = \{e^{2ik\pi/n},\ k \in \mathbb{Z}\} = \{(e^{2i\pi/n})^k,\ k \in \mathbb{Z}\} = \langle e^{2i\pi/n} \rangle,$$

et d'autre part, il est fini de cardinal n, puisque

$$\mathbb{U}_n = \{e^{2ik\pi/n},\ 0 \leq k \leq n-1\},$$

et $0 \leq \frac{2\pi}{n} < \cdots < \frac{2(n-1)\pi}{n} < 2\pi$.

Théorème 25 (Cyclicité et générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$)
Pour tout $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et ses générateurs sont exactement les $\overline{k}$ où k est premier avec n.

Preuve
Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique car $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$ (puisque $\overline{k} = k\overline{1}$ pour tout $k \in \{0, \cdots, n-1\}$).
Ensuite : une classe $\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $\overline{1} \in \langle \overline{k} \rangle$. Or :

$$\overline{1} \in \langle \overline{k} \rangle \iff \exists p \in \mathbb{Z},\ p\overline{k} = \overline{1} \iff \exists p \in \mathbb{Z},\ \overline{pk} = \overline{1} \iff \exists p \in \mathbb{Z},\ pk \equiv 1\ [n]$$

$$\iff \exists (p,q) \in \mathbb{Z}^2,\ pk + qn = 1 \iff k \text{ est premier avec } n$$

(d'après le théorème de Bézout).

Théorème 26 (Classification des groupes monogènes)
Soit $(G,*)$ un groupe monogène.

(i) Si G est infini, alors $(G,*)$ est isomorphe à $(\mathbb{Z},+)$.

(ii) Si G est fini, alors $(G,*)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$, où $n = Card(G)$.

Remarque
Ainsi, tous les groupes monogènes sont connus à isomorphisme près.

Preuve
Notons $a \in G$ un générateur de $(G,*)$. On a alors $G = \{a^k,\ k \in \mathbb{Z}\}$, donc G est l'image de l'application

$$\varphi_a : \left\{ \begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (G,*) \\ k & \longmapsto & a^k \end{array} \right. ,$$

qui est un morphisme de groupes car

$$\forall (k,k') \in \mathbb{Z}^2, \quad \varphi_a(k+k') = a^{k+k'} = a^k * a^{k'} = \varphi_a(k) * \varphi_a(k').$$

Le noyau de φ_a est un sous-groupe de $(\mathbb{Z},+)$ (cf. prop. 15 et def. 16), donc d'après le théorème 11, il existe $n \in \mathbb{N}$ tel que $Ker(\varphi_a) = n\mathbb{Z}$.

(i) Si $n = 0$, alors $Ker(\varphi_a) = \{0\}$ et $Im(\varphi_a) = G$, donc $\varphi_a : (\mathbb{Z},+) \to (G,*)$ est un isomorphisme, ce qui prouve que $(G,*)$ est isomorphe à $(\mathbb{Z},+)$, et donc infini.

(ii) Si $n \geq 1$, alors le morphisme $\varphi_a : \mathbb{Z} \to G$ est constant sur les classes d'équivalences modulo n, puisque :

$$k \equiv k'\ [n] \iff k' - k \in n\mathbb{Z} = Ker(\varphi_a) \iff \varphi_a(k-k') = e \iff \varphi_a(k) * \varphi_a(k')^{-1} = e$$

$$\iff \varphi_a(k') = \varphi_a(k).$$

Cela permet de définir l'application :

$$\overline{\varphi_a} : \left\{ \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z},+) & \longrightarrow & (G,*) \\ \overline{k} & \longmapsto & a^k \end{array} \right.$$

(car la valeur de $\varphi_a(k)$ ne dépend pas du représentant choisi dans la classe $\overline{k}$. Ce procédé s'appelle *passage au quotient de l'application* φ_a).
Tout comme φ_a, l'application $\overline{\varphi_a}$ est un morphisme de groupes, et on a $Im(\overline{\varphi_a}) = Im(\varphi_a) = G$, donc $\overline{\varphi_a}$ est surjectif.
En outre, $\overline{\varphi_a}$ est également injectif car pour tout $k \in \mathbb{Z}$:

$$\overline{k} \in Ker(\overline{\varphi_a}) \iff \overline{\varphi_a}(\overline{k}) = e \iff \varphi_a(k) = e \iff k \in Ker(\varphi_a) = n\mathbb{Z} \iff \overline{k} = \overline{0}.$$

Donc $\overline{\varphi_a} : (\mathbb{Z}/n\mathbb{Z},+) \to (G,*)$ est un isomorphisme, ce qui montre que $(G,*)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$, et donc fini de cardinal n.

Remarque
Retenir l'isomorphisme de la preuve, il est important.

5) Ordre d'un élément dans un groupe

Définition 27 (Element d'ordre fini, ordre d'un élément)
Soit $(G,*)$ un groupe.

(i) On dit qu'un élément $x \in G$ est **d'ordre fini** *lorsqu'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$.*

(ii) Si $x \in G$ est d'ordre fini, on appelle **ordre de x** *le plus petit entier $k \in \mathbb{N}^*$ tel que $x^k = e$. On le notera $ord(x)$.*

Remarque

- *Si x est d'ordre fini, alors l'ensemble $\{k \in \mathbb{N}^*,\ x^k = e\}$ est une partie non vide de $\mathbb{N}$, donc elle possède un plus petit élément, ce qui permet de définir*

$$ord(x) = \min\{k \in \mathbb{N}^*,\ x^k = e\}.$$

- *L'élément neutre e est d'ordre fini, et c'est le seul élément de G d'ordre 1.*
- *Un élément est d'ordre fini ssi son inverse l'est, et dans ce cas, $ord(x) = ord(x^{-1})$. En effet :*

$$\forall k \in \mathbb{N}^*, \qquad (x^{-1})^k = e \iff (x^k)^{-1} = e \iff x^k = e.$$

- *Tout isomorphisme de groupes conserve l'ordre des éléments. En effet, si $\varphi : G \to G'$ est un isomorphisme, alors pour tout $x \in G$:*

$$\forall k \in \mathbb{Z}, \qquad (\varphi(x))^k = e_{G'} \iff \varphi(x^k) = e_{G'} \iff x^k = e_G,$$

donc $ord(x) = ord(\varphi(x))$ (en cas d'ordre fini).

Propriété 28 (Propriétés de l'ordre d'un élément)
Soit $(G, *)$ un groupe et $x \in G$.

(i) x est d'ordre fini si et seulement si $\langle x \rangle$ est fini, et dans ce cas, on a $\langle x \rangle = \{e, x, \cdots, x^{ord(x)-1}\}$. En particulier, on a $ord(x) = Card(\langle x \rangle)$.

(ii) Si x est d'ordre fini, alors pour tout $k \in \mathbb{Z}$: $x^k = e \iff ord(x)$ divise k.

Preuve

(i) Si $\langle x \rangle = \{x^k,\ k \in \mathbb{Z}\}$ est fini, alors il existe deux entiers relatifs $k < k'$ tels que $x^k = x^{k'}$.
Donc $x^{k'-k} = e$ avec $k' - k \in \mathbb{N}^*$, et donc x est d'ordre fini.
Réciproquement, supposons x d'ordre fini et notons $m = ord(x) \in \mathbb{N}^*$. Tout entier $k \in \mathbb{Z}$ s'écrit de manière unique $k = mq + r$ avec $0 \leq r < m$, donc $x^k = (x^m)^q * x^r = e * x^r = x^r$, ce qui montre

$$\langle x \rangle = \{x^r,\ 0 \leq r < m\} = \{e, x, \cdots, x^{m-1}\},$$

et les $(x^r)_{0 \leq r < m}$ sont bien distincts, car si $0 \leq r < r' < m$:

$$x^r = x^{r'} \implies x^{r'-r} = e \implies r' - r \geq m,$$

ce qui est contradictoire. Donc on a bien $Card(\langle x \rangle) = m = ord(x)$.

(ii) Avec les mêmes notations que précédemment, on a pour tout $k \in \mathbb{Z}$:

$$x^k = e \iff x^r = e \iff r = 0,$$

car $0 \leq r < m = ord(x)$. Donc

$$x^k = e \iff m | k,$$

puisque r est le reste dans la division de k par m.

Corollaire 29 (Lien entre cyclicité et ordre des éléments)
Un groupe fini de cardinal n est cyclique si et seulement si il possède des éléments d'ordre n, et dans ce cas, les générateurs sont ces éléments d'ordre n.

Preuve
Un groupe G de cardinal n est cyclique si et seulement si il existe des éléments $a \in G$ tels que $\langle a \rangle = G$, ce qui équivaut à $Card(\langle a \rangle) = n$ (puisqu'on a toujours l'inclusion $\langle a \rangle \subset G$), ou encore $ord(a) = n$, d'après la proposition précédente.

Exemple
Déterminer les ordres de tous les éléments de $(\mathbb{Z}/6\mathbb{Z}, +)$.

- L'élément neutre $\overline{0}$ est d'ordre 1.

- Les éléments $\overline{1}$ et $\overline{5} = -\overline{1}$ sont d'ordre 6 (les générateurs sont les classes des entiers premiers avec 6).
- Les éléments $\overline{2}$ et $\overline{4} = -\overline{2}$ sont d'ordre 3 car : $\overline{2} + \overline{2} = \overline{4} \neq \overline{0}$ et $\overline{2} + \overline{2} + \overline{2} = \overline{0}$.
- L'élément $\overline{3}$ est d'ordre 2 car $\overline{3} + \overline{3} = \overline{0}$.

Exemple
Déterminer les ordres de tous les éléments du groupe symétrique $(\mathcal{S}_3, \circ)$. *Est-il cyclique ?*

- L'élément neutre Id est d'ordre 1.
- Les transpositions $\tau_{1,2}, \tau_{1,3}, \tau_{2,3}$ sont d'ordre 2 (toute transposition vérifie $\tau^2 = \tau \circ \tau = Id$).
- Les 3-cycles $c_1 = (1 \quad 2 \quad 3)$ et $c_2 = c_1^{-1} = (1 \quad 3 \quad 2)$ sont d'ordre 3 car $c_1^2 = c_2 \neq Id$ et $c_1^3 = c_1 c_2 = Id$.

Le groupe $(\mathcal{S}_3, \circ)$ n'est donc pas cyclique (pas d'élément d'ordre $6 = Card(S_3)$).
Autre argument : $(\mathcal{S}_3, \circ)$ est non commutatif, et tout groupe cyclique est commutatif.

Théorème 30 (Ordre des éléments d'un groupe fini)
Soit $(G, *)$ *un groupe fini de cardinal* $n \in \mathbb{N}^*$. *Alors* $\forall x \in G,\ x^n = e$.
En d'autres termes, tout $x \in G$ *est d'ordre fini, et* $ord(x)$ *divise* $Card(G)$.

Preuve (Cas où G est commutatif)
Fixons $x \in G$. L'application $y \mapsto y * x$ est une bijection de G dans G, d'inverse $z \mapsto z * x^{-1}$. On a donc

$$\prod_{y \in G} y = \prod_{y \in G} (y * x).$$

Mais par commutativité de G :

$$\prod_{y \in G} (y * x) = \left(\prod_{y \in G} y \right) * \left(\prod_{y \in G} x \right) = \left(\prod_{y \in G} y \right) * x^n,$$

ce qui entraîne $\prod_{y \in G} y = \left(\prod_{y \in G} y \right) * x^n$, et donc $x^n = e$.

Preuve (Cas général)
On montre d'abord le *théorème de Lagrange* (tout sous-groupe d'un groupe fini est fini, et son cardinal divise le cardinal du groupe, résultat hors programme), et on en déduit ce résultat. Voir les exercices pour les détails.

ATTENTION !
Ce théorème ne dit pas que G contient des éléments d'ordre d pour tout diviseur d de n.

II Anneaux, corps

1) Anneaux et sous-anneaux

Définition 31 (Anneau)
Un **anneau** *est un ensemble A muni de deux lois de composition interne $+ : A \times A \to A$ (appelée "somme") et $\times : A \times A \to A$ (appelée "produit") qui vérifient les propriétés suivantes :*

(i) $(A, +)$ *est un groupe commutatif (i.e. la loi $+$ est associative, commutative, possède un élément neutre et tout élément $x \in A$ possède un symétrique noté $-x$) ;*

(ii) la loi $\times$ est associative ;

(iii) la loi $\times$ possède un élément neutre ;

(iv) la loi $\times$ est distributive sur la loi $+$, i.e.

$$\forall (x, y, z) \in A^3, \quad x \times (y + z) = x \times y + x \times z, \qquad (y + z) \times x = y \times x + z \times x.$$

Notation
Un anneau sera noté $(A, +, \times)$, le neutre de la loi $+$ (qui est unique) sera noté 0_A (ou 0) et le neutre de la loi $\times$ (également unique) sera noté 1_A (ou 1).
Souvent le "produit" de deux éléments sera noté simplement xy plutôt que $x \times y$.

ATTENTION !
Dans un anneau $(A, +, \times)$, la somme $+$ est toujours commutative, mais pas le produit $\times$.

Définition 32 (Anneau commutatif)
Un anneau $(A, +, \times)$ est dit **commutatif** *lorsque la loi $\times$ est commutative.*

Exemple

- $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathbb{R}[X], +, \times)$ est un anneau commutatif.
- $(\mathcal{M}_n(\mathbb{R}), +, \times)$ est un anneau (non commutatif).
- Pour tout espace vectoriel E, $(\mathcal{L}(E), +, \circ)$ est un anneau (non commutatif).
- Soit X un ensemble quelconque. L'ensemble des fonctions $X \to \mathbb{R}$, noté $\mathbb{R}^X$ (ou $\mathcal{F}(X, \mathbb{R})$) est un anneau commutatif.

Définition 33 (Elément inversible)
Soit $(A, +, \times)$ un anneau. Un élement $x \in A$ est dit **inversible** *lorsqu'il existe $y \in A$ tel que $xy = yx = 1_A$.*

Propriété 34 (Calculs dans un anneau)
Soit $(A, +, \times)$ un anneau.

(i) *Pour tout $x \in A$, $0_A \times x = x \times 0_A = 0_A$.*

(ii) *Pour tout $(x, y) \in A^2$, $(-x)y = -(xy) = x(-y)$.*

(iii) *Pour tout $n \in \mathbb{Z}$ et tout $(x, y) \in A^2$, $(nx)y = n(xy) = x(ny)$.*

(iv) *Si $x \in A$ est inversible, alors son inverse est unique. On le notera x^{-1}.*

(v) *Si $x \in A$ et $y \in A$ sont inversibles, alors xy est inversible et $(xy)^{-1} = y^{-1}x^{-1}$.*

(vi) *Si $(x, y) \in A^2$ sont tels que $\boldsymbol{xy = yx}$, alors pour tout $n \in \mathbb{N}$:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad \textit{(formule du binôme)}$$

(vii) *Si $(x, y) \in A^2$ sont tels que $\boldsymbol{xy = yx}$, alors pour tout $n \in \mathbb{N}$:*

$$x^n - y^n = (x-y)\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right) \qquad \textit{(identité de Bernoulli).}$$

En particulier

$$1_A - x^n = (1_A - x)(1_A + x + x^2 + \cdots + x^{n-1}).$$

Preuve (non traitée en classe)
Fixons x et y dans A.

(i) $0_A \times x = (0_A + 0_A) \times x = 0_A \times x + 0_A \times x$, d'où $0_A \times x = 0_A \times x - 0_A \times x = 0_A$, et de même pour $x \times 0_A$.

(ii) $(-x)y + xy = ((-x) + x)y = 0_A y = 0_A$, donc $(-x)y = -(xy)$. De même pour l'autre égalité.

(iii) La propriété $(nx)y = n(xy)$ est vraie pour $n = 0$ (d'après le point (i)), et elle est héréditaire car si $(nx)y = n(xy)$, alors $((n+1)x)y = (nx + x)y = (nx)y + xy = n(xy) + xy = (n+1)xy$, elle est donc vraie pour tout $n \in \mathbb{N}$. On l'étend à $\mathbb{Z}$ en utilisant le point (ii) : pour tout $n \in \mathbb{N}$,

$$((-n)x)y = (-(nx))y = -((nx)y) = -(n(xy)) = (-n)(xy).$$

On procède de même pour l'autre égalité.

(iv) Si y et y' sont deux inverses de x, alors $y' = y'1_A = y'(xy) = (y'x)y = 1_A y = y$.

(v) Si x et y sont inversibles, alors l'élément $u = y^{-1}x^{-1}$ vérifie (par associativité) $u(xy) = (y^{-1}x^{-1})(xy) = 1_A$ ainsi que $(xy)u = 1_A$, c'est donc l'inverse de xy.

(vi) Par récurrence sur $n \in \mathbb{N}$. La formule est évidente pour $n = 0$ car $(x+y)^0 = 1_A = \binom{0}{0} x^0 y^0$. Supposons la formule vraie pour $n \in \mathbb{N}$ et montrons la pour $n+1$: si $xy = yx$, alors par hypothèse de récurrence :

$$(x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right).$$

En développant et en utilisant $xy = yx$:

$$(x+y)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} y x^k y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}.$$

En changeant d'indice dans la première somme, ceci se réécrit :

$$(x+y)^{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}$$

$$= x^{n+1} + \sum_{k=1}^{n} \underbrace{\left(\binom{n}{k-1} + \binom{n}{k}\right)}_{=\binom{n+1}{k}} x^k y^{n+1-k} + y^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}.$$

(vii) En développant et changeant d'indice, on peut simplifier par téléscopage :

$$(x-y)\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right) = \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} \underbrace{yx^k}_{=x^k y} y^{n-1-k} = \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} x^k y^{n-k}$$

$$= \sum_{k=1}^{n} x^k y^{n-k} - \sum_{k=0}^{n-1} x^k y^{n-k} = x^n y^0 - x^0 y^n = x^n - y^n.$$

Remarque (Anneau nul)
Si $0_A = 1_A$, alors $A = \{0_A\}$. On parle alors **d'anneau nul**.
En effet, pour tout $x \in A$:

$$x = x \times 1_A = x \times 0_A = 0_A,$$

d'après la propriété précédente.

Propriété 35 (Groupe des inversibles d'un anneau)
Si $(A, +, \times)$ est un anneau, alors l'ensemble des éléments inversibles de A est un groupe pour la loi $\times$. On le notera $A^\times$ ou $U(A)$.

Preuve (non traitée en classe)
Le produit de deux inversibles de A est un inversible de A (d'après la prop. précédente), donc la loi $\times$ est bien une loi de composition interne sur la partie $A^\times \subset A$.
Elle est associative (par restriction), possède un élément neutre (car 1_A est bien dans $A^\times$) et tout élément $x \in A^\times$ a bien un inverse dans $A^\times$ (puisque x^{-1} est lui-même inversible, d'inverse x).

Remarque
Un anneau $(A, +, \times)$ contient donc deux groupes : le groupe additif $(A, +)$ et le groupe multiplicatif $(A^\times, \times)$.

Exemple
$\mathbb{R}^\times = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{Z}^\times = \{-1, 1\}$, $\mathcal{M}_n(\mathbb{R})^\times = GL_n(\mathbb{R})$.

Propriété 36 (Produit fini d'anneaux)
Soit $n \in \mathbb{N}^*$ et $(A_1, +_1, \times_1), \cdots, (A_n, +_n, \times_n)$ des anneaux. Alors, l'ensemble $A_1 \times \cdots \times A_n$ muni des lois de composition interne :

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 +_1 y_1, \cdots, x_n +_n y_n),$$

$$(x_1, \cdots, x_n) \times (y_1, \cdots, y_n) = (x_1 \times_1 y_1, \cdots, x_n \times_n y_n),$$

est un anneau.
L'élément neutre pour $+$ est $(0_{A_1}, \cdots, 0_{A_n})$, et l'élément neutre pour $\times$ est $(1_{A_1}, \cdots, 1_{A_n})$.
Pour tout $(x_1, \cdots, x_n) \in A_1 \times \cdots \times A_n$, on a

$$-(x_1, \cdots, x_n) = (-x_1, \cdots, -x_n).$$

Enfin, un élément $(x_1, \cdots, x_n)$ est inversible si et seulement si tous les x_i le sont, et on a

$$(x_1, \cdots, x_n)^{-1} = (x_1^{-1}, \cdots, x_n^{-1}).$$

Cet anneau $(A_1 \times \cdots \times A_n, +, \times)$ est appelé **anneau produit** *des anneaux $(A_1, +_1, \times_1), \cdots, (A_n, +_n, \times_n)$.*

Preuve laissée en exercice
Vérifications immédiates (mais fastidieuses).

Définition 37 (Sous-anneau)
Soit $(A,+,\times)$ un anneau. Un **sous-anneau** *de A est une partie $B \subset A$ telle que :*
(i) $1_A \in B$;
(ii) $(B,+)$ *est un sous-groupe de* $(A,+)$;
(iii) $\forall (x,y) \in B^2,\ xy \in B$ *(stabilité de B par produit).*

Remarque

- *La condition (i) assure que $B \neq \emptyset$, donc pour vérifier que $(B,+)$ est un sous-groupe de $(A,+)$, il suffit alors de vérifier que $\forall (x,y) \in B^2,\ x-y \in B$.*
- *Un sous-anneau de A contient automatiquement 0_A (en tant que sous-groupe de $(A,+)$).*
- *Tout sous-anneau B est lui-même un anneau (pour les restrictions des lois $+$ et $\times$ à la partie B).*

Exemple

- $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$, qui est lui-même un sous-anneau de $(\mathbb{C},+,\times)$.
- $(\mathcal{M}_n(\mathbb{Z}),+,\times)$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{R}),+,\times)$.
- Si $X \subset \mathbb{R}$, alors l'ensemble des fonctions continues $X \to \mathbb{R}$, noté $\mathcal{C}^0(X,\mathbb{R})$, est un sous-anneau de $\mathcal{F}(X,\mathbb{R})$.

2) Morphismes d'anneaux

Définition 38 (Morphisme d'anneaux)
Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. Un **morphisme d'anneaux** *de A dans B est une application $\varphi : A \to B$ telle que :*
(i) $\varphi(1_A) = 1_B$;
(ii) φ *est un morphisme de groupes de* $(A,+)$ *dans* $(B,+)$
(i.e. $\forall (x,y) \in A^2,\ \varphi(x+y) = \varphi(x)+\varphi(y)$*)* ;
(iii) $\forall (x,y) \in A^2,\ \varphi(xy) = \varphi(x)\varphi(y)$.

Propriété 39 (Propriétés immédiates des morphismes d'anneaux)
Soit $\varphi : (A,+,\times) \to (B,+,\times)$ un morphisme d'anneaux. Alors :
(i) $\varphi(0_A) = 0_B$;
(ii) $\forall x \in A,\ \varphi(-x) = -\varphi(x)$;
(iii) Si $x \in A^\times$, alors $\varphi(x) \in B^\times$ et $(\varphi(x))^{-1} = \varphi(x^{-1})$.

Preuve (non traitée en classe)

(i) Automatique car $\varphi : (A,+) \to (B,+)$ est un morphisme de groupes.

(ii) Idem.

(iii) Si x est inversible, alors $xx^{-1} = 1_A$, donc $\varphi(xx^{-1}) = \varphi(1_A)$, c'est-à-dire $\varphi(x)\varphi(x^{-1}) = 1_B$. On montre de même que $\varphi(x^{-1})\varphi(x) = 1_B$, ce qui prouve que $\varphi(x)$ est inversible et que $(\varphi(x))^{-1} = \varphi(x^{-1})$.

Remarque
Si $\varphi : A \to B$ est un morphisme d'anneaux, alors la restriction $\varphi : (A^\times,\times) \to (B^\times,\times)$ est un morphisme de groupes multiplicatifs.

Propriété 40 (Composée de deux morphismes d'anneaux)
La composée de deux morphismes d'anneaux en est un.

Preuve (non traitée en classe)
Soit $\varphi : A \to B$ et $\psi : B \to C$ deux morphismes d'anneaux.

- $(\psi \circ \varphi)(1_A) = \psi(\varphi(1_A)) = \psi(1_B) = 1_C$;
- $\psi \circ \varphi : (A, +) \to (C, +)$ est un morphisme de groupes, comme composée de deux morphismes de groupes ;
- $\forall (x, y) \in A^2,\ (\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)$.

Donc $\psi \circ \varphi : A \to C$ est un morphisme d'anneaux.

Définition 41 (Image et noyau d'un morphisme d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux.

(i) On appelle **image de** *φ l'ensemble $Im(\varphi) = \varphi(A)$.*

(ii) On appelle **noyau de** *φ l'ensemble $Ker(\varphi) = \varphi^{-1}(\{0_B\})$.*

Remarque
Le noyau d'un morphisme d'anneaux est donc le noyau du morphisme de groupes additifs sous-jacent.

Propriété 42 (Structure algébrique de l'image d'un morphisme d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux. Alors $Im(\varphi)$ est un sous-anneau de B.

Preuve (non traitée en classe)
D'abord $1_B \in Im(\varphi)$ car $1_B = \varphi(1_A)$.
Ensuite $Im(\varphi) = \varphi(A)$ est un sous-groupe de $(B, +)$ d'après la proposition 15.
Enfin, $Im(\varphi)$ est stable par produit car si $(x, y) \in Im(\varphi)^2$, alors il existe $(a, b) \in A^2$ tel que $x = \varphi(a)$ et $y = \varphi(b)$, donc $xy = \varphi(a)\varphi(b) = \varphi(ab) \in Im(\varphi)$.

Remarque
De façon générale, on peut montrer que si $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux, alors pour tout sous-anneau C de A, $\varphi(C)$ est un sous-anneau de B, et pour tout sous-anneau D de B, $\varphi^{-1}(D)$ est un sous-anneau de A (exercice facile).

ATTENTION !
$Ker(\varphi)$ n'est pas un sous-anneau de A, car $1_A \notin Ker(\varphi)$ en général (sauf si $1_B = 0_B \ldots$)

Propriété 43 (Caractérisation de l'injectivité/la surjectivité d'un morphisme d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux.

(i) φ est surjectif ssi $Im(\varphi) = B$;

(ii) φ est injectif ssi $Ker(\varphi) = \{0_A\}$.

Preuve (non traitée en classe)
Direct car $\varphi : (A, +) \to (B, +)$ est un morphisme de groupes.

Définition 44 (Isomorphisme d'anneaux)
Un **isomorphisme d'anneaux** *est un morphisme d'anneaux bijectif.*

Propriété 45 (Réciproque d'un isomorphisme d'anneaux)
Si $\varphi : A \to B$ est un isomorphisme d'anneaux, alors $\varphi^{-1} : B \to A$ est aussi un isomorphisme d'anneaux.

Preuve (non traitée en classe)
Soit $\varphi : A \to B$ un isomorphisme d'anneaux.
Tout d'abord $\varphi : (A, +) \to (B, +)$ est un isomorphisme de groupes, donc $\varphi^{-1} : (B, +) \to (A, +)$ aussi.
Ensuite, $\varphi(1_A) = 1_B$, donc $\varphi^{-1}(1_B) = 1_A$.

Enfin, étant donnés deux éléments $(x, y) \in B^2$, on a, en notant $a = \varphi^{-1}(x)$ et $b = \varphi^{-1}(y)$:

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

Exemple

- La conjugaison complexe $z \mapsto \overline{z}$ est un (iso)morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{C}$.
- Pour toute partie X de $\mathbb{R}$ telle que $0 \in X$, l'application $\left\{ \begin{array}{ccc} \mathcal{F}(X,\mathbb{R}) & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(0) \end{array} \right.$ est un morphisme d'anneaux (il s'agit de l'évaluation en 0).

3) Anneaux intègres

Définition 46 (Anneau intègre)
Un anneau $(A, +, \times)$ est dit **intègre** *lorsqu'il est non réduit à $\{0_A\}$ et lorsque :*

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

Remarque
Dans un anneau non intègre, il y a des **diviseurs de zéro**, *c'est-à-dire des couples $(x, y) \in A^2$ avec $x \neq 0_A$, $y \neq 0_A$ et $xy = 0_A$.*

Propriété 47 (Simplification dans un anneau intègre)
Si $(A, +, \times)$ est un anneau intègre, alors pour tous $(a, b, c) \in A^3$, on a :
(i) $(a \neq 0_A$ et $ab = ac) \implies b = c$;
(ii) $(a \neq 0_A$ et $ba = ca) \implies b = c$.

Preuve (non traitée en classe)
Evident car $ab = ac \iff a(b - c) = 0_A$ et $ba = ca \iff (b - c)a = 0_A$.

Exemple

- $(\mathbb{C}, +, \times)$ est intègre.
- Tout sous-anneau d'un anneau intègre est lui-même un anneau intègre.
- Pour tout entier $n \geq 2$, $(\mathcal{M}_n(\mathbb{R}), +, \times)$ n'est pas intègre.
- Pour tout espace vectoriel E de dimension $n \geq 2$, $(\mathcal{L}(E), +, \circ)$ n'est pas intègre.
- $(\mathbb{C}[X], +, \times)$ est intègre.
- $(\mathcal{F}(X, \mathbb{R}), +, \times)$ n'est pas intègre.

4) Corps

Définition 48 (Corps)
Un **corps** *est un anneau $(K, +, \times)$ commutatif, non réduit à $\{0_K\}$, dans lequel tout élément $x \neq 0_K$ est inversible.*

Remarque
Dans un corps, $K^\times = K \setminus \{0_K\}$.

Propriété 49 (Intégrité d'un corps)
Tout corps K est un anneau intègre.

Preuve (non traitée en classe)
Déjà, K est un anneau non nul par définition. Soit $(x, y) \in K^2$ tels que $xy = 0_K$.
Si $x \neq 0_K$, alors x est inversible donc $y = x^{-1}(xy) = x^{-1}0_K = 0_K$. Ceci montre l'implication $xy = 0_K \implies x = 0_K$ ou $y = 0_K$.

Définition 50 (Sous-corps)
Soit $(K, +, \times)$ un corps. Un **sous-corps** *de K est une partie $L \subset K$ telle que :*

(i) L est un sous-anneau de K ;

(ii) Pour tout $x \in L$, $x \neq 0_K \implies x^{-1} \in L$.

Remarque
Tout sous-corps L est lui-même un corps (pour les lois induites sur L).

Exemple
$\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$.
$\mathbb{Z}$ n'est pas un corps, puisque par exemple $2 \in \mathbb{Z}$ mais 2 n'est pas inversible dans $\mathbb{Z}$ (étant donné que 2 ne divise pas 1).

III Idéaux d'un anneau commutatif

1) Généralités

Définition 51 (Idéal)
Soit $(A,+,\times)$ un anneau commutatif. Un **idéal** *de A est une partie $I \subset A$ telle que :*
(i) $(I,+)$ est un sous-groupe de $(A,+)$;
(ii) $\forall x \in I,\ \forall a \in A,\ xa \in I$.

Vocabulaire
La propriété (ii) est appelée "propriété d'absorption".

Propriété 52 (Caractérisation d'un idéal)
Soit $(A,+,\times)$ un anneau commutatif et soit $I \subset A$. Alors, I est un idéal de A si et seulement si
(a) $0_A \in I$;
(b) $\forall (x,y) \in I^2,\ x+y \in I$;
(c) $\forall x \in I,\ \forall a \in A,\ xa \in I$.

Preuve
Il est clair que la propriété (i) entraîne (a) et (b).
Réciproquement : la condition (c) entraîne en particulier (avec $a = -1_A$) que $(x \in I \implies -x \in I)$.
Combiné aux conditions (a) et (b), cela entraîne que $(I,+)$ est un sous-groupe de $(A,+)$.

Propriété 53 (Exemple fondamental : idéal engendré par un élément)
Soit $(A,+,\times)$ un anneau commutatif.
Pour tout $a \in A$, l'ensemble $aA = \{ax,\ x \in A\}$ est un idéal de A, et c'est le plus petit idéal de A contenant a. On dit que aA est **l'idéal engendré par a**.

Preuve
Posons $I = aA$.

- I est un idéal de A :
  $0_A = a0_A$ donc $0_A \in I$. Si $(y,y') \in I^2$, alors il existe $(x,x') \in A^2$ tels que $y = ax$ et $y' = ax'$, donc $y - y' = a(x-x') \in I$ puisque $x - x' \in A$. En outre, pour tout $z \in A$, on a $yz = (ax)z = a(xz) \in I$, puisque $xz \in A$.
- I contient a car $a = a1_A \in I$.
- Soit J un idéal quelconque de A tel que $a \in J$. Montrons que $I \subset J$: si $y \in I$, alors il existe $x \in A$ tel que $y = ax$. Mais a est dans l'idéal J, donc $y = ax \in J$, ce qui montre l'inclusion voulue.

Propriété 54 (Structure algébrique du noyau d'un morphisme d'anneaux)
Soit $\varphi : (A,+,\times) \to (B,+,\times)$ un morphisme d'anneaux, avec A commutatif.
Alors $Ker(\varphi)$ est un idéal de A.

Preuve
Déjà, $(Ker(\varphi),+)$ est un sous-groupe de $(A,+)$ en tant que noyau du morphisme de groupes $\varphi : (A,+) \to (B,+)$.
Ensuite, pour tout $x \in Ker(\varphi)$ et pour tout $a \in A$, on a $xa \in Ker(\varphi)$ car $\varphi(xa) = \varphi(x)\varphi(a) = 0_B \times \varphi(a) = 0_B$.

Propriété 55 (Opérations algébriques sur les idéaux)
Soit $(A,+,\times)$ un anneau commutatif, et I et J deux idéaux de A. Alors :

(i) l'ensemble $I\cap J$ est un idéal de A ;

(ii) l'ensemble $I+J=\{x+y,\ x\in I,\ y\in J\}$ est un idéal de A, appelé **somme des idéaux I et J**. *C'est le plus petit idéal de A contenant I et J.*

Plus généralement, si $I_1,\cdots,I_n$ sont des idéaux de A, on peut définir les idéaux :

$$I_1\cap\cdots\cap I_n=\{x\in A,\ \forall j\in[\![1,n]\!],\ x\in I_j\},$$

$$I_1+\cdots+I_n=\{x_1+\cdots+x_n,\ x_1\in I_1,\cdots,x_n\in I_n\},$$

et ces opérations sur les idéaux sont associatives.

Preuve

(i) Déjà, $I\cap J$ est un sous-groupe de $(A,+)$ comme intersection de sous-groupes. Ensuite, si $x\in I\cap J$ et $a\in A$, alors on a $xa\in I$ (car $x\in I$ et I est un idéal) et $xa\in J$, donc $xa\in I\cap J$. Donc $I\cap J$ est bien un idéal de A.

(ii) • Montrons que $I+J$ est un sous-groupe de $(A,+)$: on a $0_A=0_A+0_A\in I+J$ (puisque 0_A est dans les sous-groupes I et J). Ensuite, si $(z,z')\in(I+J)^2$, alors il existe $(x,x')\in I^2$ et $(y,y')\in J^2$ tel que $z=x+y$ et $z'=x'+y'$, donc $z-z'=(x-x')+(y-y')\in I+J$ car $x-x'\in I$ et $y-y'\in J$ (les sous-groupes I et J étant stables par différence).

• Si $z=x+y\in I+J$ et $a\in A$, alors $za=xa+ya\in I+J$, car $xa\in I$ et $ya\in J$.

Donc $I+J$ est un idéal de A.

• $I+J$ contient I et J car $\forall x\in I,\ x=x+0_A\in I+J$, et de même pour J.

• Enfin, si K est un idéal de A contenant I et J, alors vu que K est stable par somme, il contient nécessairement $I+J$.

Donc $I+J$ est bien le plus petit idéal de A contenant I et J.

Signalons enfin que la généralisation à la somme de n idéaux fonctionne car dans un anneau, la somme est associative.

ATTENTION !
La réunion de deux idéaux n'est pas un idéal en général (comme pour les sous-espaces vectoriels d'un espace vectoriel).

2) Idéaux et divisibilité

Définition 56 (Divisibilité dans un anneau commutatif)
Dans un anneau commutatif $(A,+,\times)$, étant donnés $(a,b)\in A^2$, on dit que **b divise a** *lorsqu'il existe $c\in A$ tel que $a=bc$. On note alors $b|a$.*

Propriété 57 (Eléments associés dans un anneau commutatif intègre)
Soit $(A,+,\times)$ un anneau commutatif et **intègre**. *Alors, pour tout $(a,b)\in A^2$, on a*

$$(b|a \text{ et } a|b)\iff\exists u\in A^\times,\ b=ua.$$

On dit dans ce cas que a et b sont **associés**.

Preuve

$\boxed{\Rightarrow}$ Si $b|a$ et $a|b$, alors il existe $(c,d)\in A^2$ tel que $a=bc$ et $b=ad$, donc $b=b(cd)$, c'est-à-dire $b(cd-1_A)=0_A$. Vu que A est intègre, cela entraîne $b=0_A$ ou $cd=1_A$.
Si $b=0_A$, alors $a=b=0_A$ donc $b=ua$ avec $u=1_A\in A^\times$.
Si $b\neq 0_A$, alors $cd=1_A$, donc $d\in A^\times$ et $b=ad=da$.
Dans tous les cas, on a $b=ua$ avec $u\in A^\times$.

$\boxed{\Leftarrow}$ Puisque $b=ua$, on a déjà $a|b$. Ensuite, u étant inversible, on a $a=u^{-1}(ua)=u^{-1}b$ donc $b|a$.

Propriété 58 (Interprétation de la divisibilité en termes d'idéaux)
Soit $(A,+,\times)$ un anneau commutatif et **intègre**, *et soit $(a,b)\in A^2$.*
Alors :

(i) $b|a \iff aA\subset bA$.

(ii) a et b sont associés si et seulement si $aA=bA$.

Remarque
Deux élements sont associés si et seulement si ils engendrent le même idéal.

Preuve

(i) Si $b|a$, alors $a=bc$ avec $c\in A$, donc $a\in bA$. Vu que bA est un idéal de A, on a $\forall x\in A$, $ax\in bA$, et donc $aA\subset bA$.
Réciproquement, si $aA\subset bA$, alors $a\in bA$ (puisque $a\in aA$), donc $b|a$.

(ii) Direct d'après (i).

3) Idéaux de $\mathbb{Z}$ et applications à l'arithmétique

Théorème 59 (Idéaux de $\mathbb{Z}$)
Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont exactement les $n\mathbb{Z}$ avec $n\in\mathbb{N}$, et tous ces idéaux sont distincts.

Preuve
Si I est un idéal de $\mathbb{Z}$, alors $(I,+)$ est un sous-groupe de $(\mathbb{Z},+)$, donc (d'après le théorème 11) il existe $n\in\mathbb{N}$ tel que $I=n\mathbb{Z}$.
Ensuite, tous les $n\mathbb{Z}$ sont bien des idéaux de $\mathbb{Z}$ d'après la prop. 53.
Enfin, si $n\mathbb{Z}=n'\mathbb{Z}$ avec $n,n'\in\mathbb{N}$, alors d'après les prop. 57 et 58, il existe $u\in\mathbb{Z}^\times=\{-1,1\}$ tel que $n'=un$. On a donc $n'=\pm n$, ce qui entraîne $n'=n$ si on impose n et n' positifs.

Remarque
Ainsi, les idéaux de l'anneau $\mathbb{Z}$ coïncident avec les sous-groupes de $(\mathbb{Z},+)$.

Vocabulaire (HP)
On dit qu'un anneau commutatif A est **principal** s'il est intègre et si tous ses idéaux sont "monogènes", c'est-à-dire de la forme $I=aA$ avec $a\in A$. Ainsi, l'anneau $\mathbb{Z}$ possède cette propriété, et on verra plus loin que l'anneau de polynômes $\mathbb{K}[X]$ également.

Propriété 60 (Définition du PGCD d'entiers par les idéaux)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$. Alors il existe un unique $d\in\mathbb{N}$ tel que $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}=d\mathbb{Z}$.
L'entier d est alors le **plus grand diviseur commun** *de $a_1,\cdots,a_n$, c'est-à-dire que :*

(i) $\forall i\in[\![1,n]\!],\ d|a_i$;

(ii) $\forall c\in\mathbb{Z},((\forall i\in[\![1,n]\!],\ c|a_i)\implies c|d)$.

On notera $d=pgcd(a_1,\cdots,a_n)$ ou $d=a_1\wedge\cdots\wedge a_n$.

Preuve
Par la prop. 55, l'ensemble $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc d'après le théorème 59, il existe $d\in\mathbb{N}$ (unique) tel que $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}=d\mathbb{Z}$.
Montrons ensuite les deux propriétés de cet entier d :

(i) Puisque $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}$ contient tous les $a_i\mathbb{Z}$, on a $a_i\mathbb{Z}\subset d\mathbb{Z}$ donc (d'après la prop. 58), d divise a_i pour tout i.

(ii) Si $c\in\mathbb{Z}$ divise tous les a_i, alors $a_i\mathbb{Z}\subset c\mathbb{Z}$ donc $d\mathbb{Z}=a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}\subset c\mathbb{Z}$ (puisque $c\mathbb{Z}$ est stable par somme), ce qui montre que c divise d.

Remarque (Associativité du PGCD)

De par sa définition, l'opération pgcd() est associative. Par exemple :

$$pgcd(a, pgcd(b, c)) = pgcd(pgcd(a, b), c)$$

Propriété 61 (Relation de Bézout)
Soit $(a_1, \cdots, a_n) \in \mathbb{Z}^n$ *et* $d = pgcd(a_1, \cdots, a_n)$.
Alors, il existe $(u_1, \cdots, u_n) \in \mathbb{Z}^n$ *tel que* $a_1u_1 + \cdots + a_nu_n = d$.

Preuve
Direct : $d \in d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, donc d s'écrit sous la forme voulue.

ATTENTION !
La réciproque est fausse. Une relation de Bézout du type $a_1u_1 + \cdots + a_nu_n = d$ indique seulement que $pgcd(a_1, \cdots, a_n)$ **divise** d (en effet, $pgcd(a_1, \cdots, a_n)$ divise tous les a_i, donc divise $a_1u_1 + \cdots + a_nu_n$).

Définition 62 (Entiers premiers entre eux)
Soit $(a_1, \cdots, a_n) \in \mathbb{Z}^n$ *avec* $n \geq 2$.
On dit que $a_1, \cdots, a_n$ *sont* **premiers entre eux dans leur ensemble** *lorsque* $pgcd(a_1, \cdots, a_n) = 1$.
On dit que $a_1, \cdots, a_n$ *sont* **premiers entre eux deux à deux** *lorsque pour tout* $(i, j) \in [\![1, n]\!]$, $i \neq j \implies pgcd(a_i, a_j) = 1$.

Remarque

- *Si* $n = 2$, *les deux notions coïncident, et on dit simplement "premiers entre eux".*
- *Si les* (a_i) *sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble.*
  En effet, $pgcd(a_1, \cdots, a_n)$ *divise* a_1 *et* a_2, *donc divise* $pgcd(a_1, a_2) = 1$.
  D'où $pgcd(a_1, \cdots, a_n) = 1$.

ATTENTION !
Réciproque fausse. Par exemple, $40, 6, 15$, sont premiers entre eux dans leur ensemble, mais pas premiers entre eux deux à deux.
En effet :

$$pgcd(40, 6) = 2, \qquad pgcd(40, 15) = 5, \qquad pgcd(6, 15) = 3,$$
$$pgcd(40, 6, 15) = pgcd(pgcd(40, 6), 15) = pgcd(2, 15) = 1.$$

Propriété 63 (Théorème de Bézout)
Soit $(a_1, \cdots, a_n) \in \mathbb{Z}^n$. *Alors :*
$a_1, \cdots, a_n$ *sont premiers entre eux dans leur ensemble ssi* $\exists (u_1, \cdots, u_n) \in \mathbb{Z}^n,\ a_1u_1 + \cdots + a_nu_n = 1$.

Preuve

$\boxed{\Rightarrow}$ C'est la relation de Bézout (cf. prop 61) dans le cas où $pgcd(a_1, \cdots, a_n) = 1$.

$\boxed{\Leftarrow}$ Réciproquement, s'il existe $(u_1, \cdots, u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^{n} a_iu_i = 1$, alors $pgcd(a_1, \cdots, a_n)$ divise 1, donc vaut 1.

Exemple
Déterminer $(u, v, w) \in \mathbb{Z}^3$ *tels que* $40u + 6v + 15w = 1$.
Déjà c'est possible car $pgcd(40, 6, 15) = 1$ (calcul déjà fait).
Ensuite, on procède par associativité : $pgcd(40, 6) = 2$, et on trouve facilement une relation de Bézout (soit à tâtons, soit en remontant l'algorithme d'Euclide) :

$$40 \times 2 - 6 \times 13 = 2.$$

Puis on trouve une deuxième relation de Bézout entre $pgcd(40,6)=2$ et 15 :

$$2\times(-7)+15\times 1=1,$$

donc finalement :

$$1=2\times(-7)+15\times 1=(40\times 2-6\times 13)\times(-7)+15\times 1,$$

c'est-à-dire

$$40\times(-14)+6\times 91+15\times 1=1.$$

Corollaire 64 (Lemme de Gauss)
Soit $(a,b,c)\in\mathbb{Z}^3$. Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Preuve
Puisque a et b sont premiers entre eux, il existe d'après le théorème précédent $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$. Par hypothèse, on a également $bc=ka$ avec $k\in\mathbb{Z}$, donc

$$c=c(au+bv)=cau+(bc)v=cau+(ka)v=a(cu+kv).$$

Corollaire 65 (Lemme d'Euclide)
Soit p un nombre premier et $(a,b)\in\mathbb{Z}^2$. Si p divise ab, alors p divise a ou b.

Preuve
Si p ne divise pas a, alors p est premier avec a (car les seuls diviseurs de p sont $\pm p$, ± 1). Donc par le lemme de Gauss, p divise b (puisque p divise déjà ab).

Remarque
Cela se généralise immédiatement : si un nombre premier divise un produit d'entiers, alors il divise au moins l'un des facteurs.

Propriété 66 (Définition du PPCM d'entiers par les idéaux)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$. Alors il existe un unique $m\in\mathbb{N}$ tel que $a_1\mathbb{Z}\cap\cdots\cap a_n\mathbb{Z}=m\mathbb{Z}$.
L'entier m est alors le **plus petit multiple commun** *de $a_1,\cdots,a_n$, c'est-à-dire que :*

(i) $\forall i\in[\![1,n]\!],\ a_i|m$;

(ii) $\forall c\in\mathbb{Z},((\forall i\in[\![1,n]\!],\ a_i|c)\implies m|c)$.

On notera $m=ppcm(a_1,\cdots,a_n)$ ou $m=a_1\vee\cdots\vee a_n$.

Preuve (non traitée en classe)
Par la prop. 55, l'ensemble $a_1\mathbb{Z}\cap\cdots\cap a_n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc d'après le théorème 59, il existe $m\in\mathbb{N}$ (unique) tel que $a_1\mathbb{Z}\cap\cdots\cap a_n\mathbb{Z}=m\mathbb{Z}$.
Montrons ensuite les deux propriétés de cet entier m :

(i) Puisque $a_1\mathbb{Z}\cap\cdots\cap a_n\mathbb{Z}$ est inclus dans tous les $a_i\mathbb{Z}$, on a $m\mathbb{Z}\subset a_i\mathbb{Z}$, donc (d'après la prop. 58), a_i divise m pour tout i.

(ii) Si $c\in\mathbb{Z}$ est multiple de tous les a_i, alors $c\mathbb{Z}\subset a_i\mathbb{Z}$ pour tout i, donc $c\mathbb{Z}\subset a_1\mathbb{Z}\cap\cdots\cap a_n\mathbb{Z}=m\mathbb{Z}$, ce qui montre que m divise c.

Remarque (Associativité du PPCM)
Tout comme le pgcd, le ppcm est associatif.

ATTENTION !
La propriété $pgcd(a_1,\cdots,a_n)\times ppcm(a_1,\cdots,a_n)=|a_1\times\cdots\times a_n|$ est fausse !
Elle n'est vraie que pour $n=2$ (voir cours MP2I).
Par exemple, $ppcm(4,9,10)\times pgcd(4,9,10)=180\times 1=180\neq 4\times 9\times 10$.

IV Anneau $\mathbb{Z}/n\mathbb{Z}$ et applications à l'arithmétique

1) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On rappelle que l'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$ peut être muni d'une structure de groupe additif (cf. prop. 23). On peut également munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau.

Théorème 67 (Structure d'anneau commutatif de $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. Les lois de composition interne $+ : \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ et $\times : \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ données par

$$\forall (x,y) \in \mathbb{Z}^2, \qquad \overline{x} + \overline{y} = \overline{x+y},$$
$$\forall (x,y) \in \mathbb{Z}^2, \qquad \overline{x} \times \overline{y} = \overline{xy},$$

sont bien définies, et $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, de neutres respectifs $\overline{0}$ et $\overline{1}$.

Preuve

- On sait déjà que $+$ est bien définie et que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.
- La loi $\times$ est bien définie car la classe $\overline{x} \times \overline{y}$ ne dépend pas des représentants x, y choisis : en effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors on a $x \equiv x'\ [n]$ et $y \equiv y'\ [n]$, donc facilement $xy \equiv x'y'\ [n]$, ce qui montre que $\overline{xy} = \overline{x'y'}$.
- La loi $\times$ est commutative puisque pour tout $(x,y) \in \mathbb{Z}^2$: $\overline{x} \times \overline{y} = \overline{xy} = \overline{yx} = \overline{y} \times \overline{x}$.
- La loi $\times$ est associative car pour tout $(x,y,z) \in \mathbb{Z}^3$:

$$(\overline{x} \times \overline{y}) \times \overline{z} = \overline{xy} \times \overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x} \times \overline{yz} = \overline{x} \times (\overline{y} \times \overline{z}).$$

- La loi $\times$ possède un élément neutre : $\overline{1}$, car

$$\forall x \in \mathbb{Z}, \quad \overline{x} \times \overline{1} = \overline{1} \times \overline{x} = \overline{x1} = \overline{x}.$$

- La loi $\times$ est distributive sur la loi $+$ car

$$\forall (x,y,z) \in \mathbb{Z}^3, \quad \overline{x} \times (\overline{y} + \overline{z}) = \overline{x} \times \overline{y+z} = \overline{x(y+z)} = \overline{xy+xz} = \overline{xy} + \overline{xz} = \overline{x} \times \overline{y} + \overline{x} \times \overline{z}.$$

  et de même dans l'autre sens (la loi $\times$ est de toute façon commutative).

Remarque
Si $n = 1$, alors $\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$ est l'anneau nul.

Remarque (Surjection canonique)
L'application $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array} \right.$ *est un morphisme d'anneaux surjectif.*
On l'appelle ***surjection canonique****.*

2) Théorème chinois

Théorème 68 (Théorème chinois)
Soient $(m,n) \in (\mathbb{N}^*)^2$ deux entiers **premiers entre eux**. *Alors l'application*

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x}, \hat{x}) \end{array} \right.$$

est un isomorphisme d'anneaux, où $\overline{x}$ (resp. $\dot{x}$, resp. $\hat{x}$) désigne la classe de l'entier x modulo mn (resp. modulo m, resp. modulo n). L'isomorphisme réciproque est :

$$\psi^{-1} : \left\{ \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} \\ (\dot{a}, \hat{b}) & \longmapsto & \overline{anv + bmu} \end{array} \right. ,$$

où $(u,v) \in \mathbb{Z}$ sont tels que $mu + nv = 1$.

Preuve

- ψ est bien définie car la valeur de $(\dot{x}, \hat{x})$ ne dépend pas du représentant x choisi dans $\overline{x}$. En effet, si $\overline{x} = \overline{x'}$, alors $x \equiv x'\ [mn]$, donc mn divise $x' - x$. Cela entraîne que m et n divisent $x' - x$, donc $x \equiv x'\ [m]$ et $x \equiv x'\ [n]$, c'est-à-dire $(\dot{x}, \hat{x}) = (\dot{x'}, \hat{x'})$.
- ψ est un morphisme d'anneaux car :
  $\psi(\overline{1}) = (\dot{1}, \hat{1})$ est bien le neutre multiplicatif de l'anneau produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, et pour tout $(x, y) \in \mathbb{Z}^2$, on a

$$\psi(\overline{x} + \overline{y}) = \psi(\overline{x+y}) = (\dot{x+y}, \hat{x+y}) = (\dot{x} + \dot{y}, \hat{x} + \hat{y}) = (\dot{x}, \hat{x}) + (\dot{y}, \hat{y}) = \psi(\overline{x}) + \psi(\overline{y}),$$

$$\psi(\overline{x}\ \overline{y}) = \psi(\overline{xy}) = (\dot{xy}, \hat{xy}) = (\dot{x}\dot{y}, \hat{x}\hat{y}) = (\dot{x}, \hat{x}) \times (\dot{y}, \hat{y}) = \psi(\overline{x})\psi(\overline{y}),$$

- ψ est injectif car

$$\overline{x} \in Ker(\psi) \iff (\dot{x}, \hat{x}) = (\dot{0}, \hat{0}) \iff x \equiv 0\ [m] \text{ et } x \equiv 0\ [n] \iff m|x \text{ et } n|x.$$

  Vu que m et n sont premiers entre eux, cela équivaut à $mn|x$. Donc $\overline{x} \in Ker(\psi) \iff \overline{x} = \overline{0}$, ce qui montre que $Ker(\psi) = \{\overline{0}\}$.
- Enfin, les ensembles finis $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont de même cardinal mn, donc l'injection ψ est automatiquement bijective.
- Soit $(u, v) \in \mathbb{Z}^2$ tels que $mu + nv = 1$.
  Etant donné un couple $(\dot{a}, \hat{b})$ dans l'anneau produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, on constate que l'entier $x = anv + bmu$ vérifie $x \equiv anv \equiv a(1 - mu) \equiv a\ [m]$ et de même $x \equiv b\ [n]$. Donc $\psi(\overline{x}) = (\dot{a}, \hat{b})$, ce qui montre que $\overline{x}$ est l'unique antécédent de $(\dot{a}, \hat{b})$ par ψ, donnant ainsi l'expression voulue de l'isomorphisme réciproque.

Remarque
Lorsque m et n ne sont pas premiers entre eux, le morphisme d'anneaux $\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est quand même bien défini, mais pas injectif (et pas surjectif pour des raisons de cardinal).
En effet, en notant $q = ppcm(m, n)$, on a $1 \leq q < mn$ (puisque m et n ne sont pas premiers entre eux) donc $\overline{q} \neq \overline{0}$ mais $\psi(\overline{q}) = (\dot{0}, \hat{0})$, puisque q est multiple de m et de n. Donc $Ker(\psi) \neq \{\overline{0}\}$.

Exemple
Résolution dans $\mathbb{Z}$ du système $\begin{cases} x \equiv 1 & [5] \\ x \equiv 7 & [9] \end{cases}$.
Puisque $pgcd(5, 9) = 1$, le théorème chinois donne un isomorphisme :

$$\psi : \begin{cases} \mathbb{Z}/45\mathbb{Z} & \longrightarrow & \mathbb{Z}/5\mathbb{Z} \times Z/9\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x}, \hat{x}) \end{cases}.$$

Le problème se réécrit : $\psi(\overline{x}) = (\dot{1}, \hat{7})$, donc la solution est l'unique antécédent de $(\dot{1}, \hat{7})$ par ψ.
Pour le trouver, on passe par l'identité de Bézout :

$$5 \times 2 + 9 \times (-1) = 1.$$

Conformément au théorème, l'entier $x = 1 \times 9 \times (-1) + 7 \times 5 \times 2 = 61$ vérifie bien $\dot{x} = -\dot{9} = \dot{1}$ et $\hat{x} = \hat{70} = \hat{7}$, donc $\overline{x} = \overline{61} = \overline{16}$ est l'unique solution dans $\mathbb{Z}/45\mathbb{Z}$.
Finalement, dans $\mathbb{Z}$, on obtient comme solutions tous les $x = 16 + 45k$ avec $k \in \mathbb{Z}$.

Théorème 69 (Théorème chinois généralisé)
Soit $k \geq 2$ et $m_1, \cdots, m_k$ des entiers **premiers entre eux deux à deux**. *Alors l'application :*

$$\psi : \begin{cases} \mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x}_{(1)}, \cdots, \dot{x}_{(k)}) \end{cases}$$

est un isomorphisme d'anneaux, où $\overline{x}$ désigne la classe de l'entier x modulo $m_1 \cdots m_k$ et pour tout $i \in [\![1, k]\!]$, $\dot{x}_{(i)}$ désigne la classe de x modulo m_i.

Preuve
Le fait que ψ soit bien défini et soit un morphisme d'anneaux se montre exactement comme dans le cas $k = 2$.
Pour l'injectivité :

$$\overline{x} \in Ker(\psi) \iff (\forall i \in [\![1,k]\!],\ m_i | x) \iff \left(\prod_{i=1}^{k} m_i\right) | x \iff \overline{x} = \overline{0},$$

l'équivalence entre les divisibilités étant vraie dans le cas où les m_i sont premiers entre eux **deux à deux**.
Enfin, l'injectivité de ψ et l'égalité des cardinaux des ensembles de départ et d'arrivée donne la bijectivité de ψ.

ATTENTION !
Ca ne marche pas si $m_1, \cdots, m_k$ sont seulement supposés premiers entre eux dans leur ensemble.
Par exemple, pour $(m_1, m_2, m_3) = (4, 9, 10)$, les entiers divisibles par $4, 9$ et 10 ne sont pas nécessairement divisibles par $4 \times 9 \times 10 = 360$ (par exemple 180).

Remarque
L'expression de ψ^{-1} est compliquée à établir pour $k \geq 3$, mais pour résoudre des systèmes de congruences, on peut s'en passer en pratique, en raisonnant par associativité comme dans l'exemple suivant.

Exemple
Résolution dans $\mathbb{Z}$ du système $\begin{cases} x \equiv 2 \quad [3] \\ x \equiv 3 \quad [5] \\ x \equiv 2 \quad [7] \end{cases}$.
Puisque les entiers $3, 5, 7$ sont premiers entre eux deux à deux, ce système possède une unique solution modulo $3 \times 5 \times 7 = 105$.
Pour la déterminer, on résout facilement (par exemple) :

$$\begin{cases} x \equiv 2 \quad [3] \\ x \equiv 3 \quad [5] \end{cases} \iff x \equiv 8 \ [15].$$

(ça marche car 3 et 5 sont premiers entre eux).
On a donc :

$$\begin{cases} x \equiv 2 \quad [3] \\ x \equiv 3 \quad [5] \\ x \equiv 2 \quad [7] \end{cases} \iff \begin{cases} x \equiv 8 \quad [15] \\ x \equiv 2 \quad [7] \end{cases}$$

Puis, vu que 15 et 7 sont premiers entre eux, on peut réappliquer la même méthode de résolution.
On obtient que les solutions sont les entiers $x = 23 + 105k$ avec $k \in \mathbb{Z}$.

Remarque
Le fonctionnement de cette méthode par associativité repose sur le fait suivant : si $m_1, \cdots, m_k$ sont premiers entre eux deux à deux, alors pour tous $I, J \subset [\![1,k]\!]$ tels que $I \cap J = \emptyset$, on a

$$\left(\prod_{i \in I} m_i\right) \wedge \left(\prod_{i \in J} m_i\right) = 1.$$

En effet, si ce n'était pas le cas, il existerait un diviseur premier p commun à $\prod_{i \in I} m_i$ et $\prod_{i \in J} m_i$, et donc d'après le lemme d'Euclide, p diviserait un des m_i avec $i \in I$ et un des m_i avec $i \in J$, ce qui est impossible car les $(m_i)_{1 \leq i \leq k}$ sont deux à deux premiers entre eux.

3) Elements inversibles, indicatrice d'Euler

Propriété 70 (Eléments inversibles de $(\mathbb{Z}/n\mathbb{Z},+,\times)$)
Soit $k\in\mathbb{Z}$. L'élément $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.

Remarque
On a donc $(\mathbb{Z}/n\mathbb{Z})^\times=\{\overline{k}\in\mathbb{Z}/n\mathbb{Z},\ 1\leq k\leq n,\ pgcd(k,n)=1\}$.

Preuve
L'inversibilité de $\overline{k}$ équivaut à l'existence de $l\in\mathbb{Z}$ tel que $\overline{k}\times\overline{l}=\overline{1}$, ou encore $kl\equiv 1\ [n]$, c'est-à-dire l'existence d'une relation de Bézout : $kl+nq=1$ avec $(l,q)\in\mathbb{Z}^2$, ce qui revient à dire que k et n sont premiers entre eux.

Théorème 71 (Structure de corps de $(\mathbb{Z}/n\mathbb{Z})$)
L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps si et seulement si n est un nombre premier.

Preuve

$\boxed{\Rightarrow}$ Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors $n\geq 2$ (un corps n'est pas réduit à 0), et $\overline{1},\cdots,\overline{n-1}$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire que $1,\cdots,n-1$ sont premiers avec n (d'après la proposition précédente). Ceci implique que les seuls diviseurs positifs de n sont n et 1, donc n est un nombre premier.

$\boxed{\Leftarrow}$ Si n est premier, alors $n\geq 2$ (donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas l'anneau nul) et n est premier avec tous les $k\in[\![1,n-1]\!]$ (puisque les seuls diviseurs positifs de n sont 1 et n), donc d'après la proposition précédente, $\overline{1},\cdots,\overline{n-1}$ (donc toutes les classes $\overline{x}\neq\overline{0}$) sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$, ce qui montre $\mathbb{Z}/n\mathbb{Z}$ est un corps.

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

Définition 72 (Indicatrice d'Euler)
Pour tout $n\in\mathbb{N}^*$, on note $\varphi(n)=Card\{k\in[\![1,n]\!],\ pgcd(k,n)=1\}$.
La fonction $\varphi:\mathbb{N}^*\to\mathbb{N}^*$ est appelée **indicatrice d'Euler**.

Remarque
$\varphi(n)$ est donc le cardinal du groupe fini $((\mathbb{Z}/n\mathbb{Z})^\times,\times)$.
$\varphi(n)$ est aussi le nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z},+)$.

Propriété 73 (Propriétés de l'indicatrice d'Euler)
L'indicatrice d'Euler $\varphi:\mathbb{N}^*\to\mathbb{N}^*$ possède les propriétés suivantes :

(i) $\varphi(1)=1$.

(ii) Pour tout nombre premier p et pour tout $\alpha\in\mathbb{N}^*$, on a $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

(iii) Pour tous entiers $m,n\geq 1$ premiers entre eux, on a $\varphi(mn)=\varphi(m)\varphi(n)$.

Preuve

(i) Evident car 1 est premier avec 1.

(ii) Si p est un nombre premier et $\alpha\in\mathbb{N}^*$, alors les seuls diviseurs de p^α sont $1,p,\cdots,p^\alpha$, donc les entiers de $[\![1,p^\alpha]\!]$ non premiers avec p^α sont les multiples de p inférieurs ou égaux à p^α, c'est-à-dire

$$p,2p,\cdots,p^{\alpha-1}p.$$

Donc le nombre d'entiers de $[\![1,p^\alpha]\!]$ premiers avec p^α est :

$$\varphi(p^\alpha)=Card\left([\![1,p^\alpha]\!]\setminus\{p,2p,\cdots,p^{\alpha-1}p\}\right)=p^\alpha-p^{\alpha-1}.$$

(iii) Par le théorème chinois, on a un isomorphisme d'anneaux

$$\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

D'après la prop. 39, les inversibles de $\mathbb{Z}/mn\mathbb{Z}$ sont envoyés sur les inversibles de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, qui sont d'après la prop. 36 les couples de $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. On obtient donc par restriction un isomorphime de groupes multiplicatifs :

$$\psi^\times : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,$$

ce qui entraîne

$$\varphi(mn) = Card(\mathbb{Z}/mn\mathbb{Z})^\times = Card\left((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times\right) = Card(\mathbb{Z}/m\mathbb{Z})^\times Card(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(m)\varphi(n).$$

Corollaire 74 (Expression de $\varphi(n)$ à partir de la décomposition en facteurs premiers)
Soit $n \geq 2$. Si la décomposition en facteurs premiers de n est

$$n = p_1^{\alpha_1} \cdots p_N^{\alpha_N},$$

avec $p_1, \cdots, p_N$ des nombres premiers deux à deux distincts et $\alpha_1, \cdots, \alpha_N \in \mathbb{N}^*$, alors

$$\varphi(n) = n \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

Preuve
Vu que $p_1, \cdots, p_N$ sont des nombres premiers distincts, les entiers $p_1^{\alpha_1}, \cdots, p_N^{\alpha_N}$ sont premiers entre eux deux à deux, donc par la proposition précédente et par récurrence immédiate, on obtient

$$\varphi(n) = \prod_{i=1}^{N} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{N} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{N} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{N} p_i^{\alpha_i} \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

Théorème 75 (Théorème d'Euler)
Soit $n \in \mathbb{N}^*$ et soit $a \in \mathbb{Z}$ un entier premier avec n. Alors $a^{\varphi(n)} \equiv 1\ [n]$.

Preuve
Puisque a est premier avec n, on a $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Or, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est fini de cardinal $\varphi(n)$, donc on obtient avec la prop. 30 : $\overline{a}^{\varphi(n)} = \overline{1}$, ce qui est la relation voulue.

Remarque
Dans le cas où n est un nombre premier p, alors $\varphi(p) = p - 1$, donc on retrouve le ***petit théorème de Fermat*** *: pour tout entier a non multiple de p, $a^{p-1} \equiv 1\ [p]$.*

V Anneau $\mathbb{K}[X]$ et arithmétique des polynômes

$\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

1) Premières propriétés

Rappel
On rappelle que l'ensemble des polynômes à coefficients dans $\mathbb{K}$, noté $\mathbb{K}[X]$, est un **anneau commutatif** pour les lois suivantes : si $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{k=0}^{d'} b_k X^k$ avec $(d, d') \in \mathbb{N}^2$, alors

$$P + Q = \sum_{k=0}^{\max(d,d')} (a_k + b_k) X^k, \qquad PQ = \sum_{k=0}^{d+d'} \left(\sum_{l=0}^{k} a_{k-l} b_l \right) X^k,$$

en posant $a_k = 0$ pour $k > d$ et $b_k = 0$ pour $k > d'$.
Les éléments neutres sont le polynôme nul $0_{\mathbb{K}[X]}$ (pour la somme), et le polynôme constant égal à 1 (pour le produit).
On dit qu'un polynôme P est **unitaire** s'il est non nul et si son coefficient dominant est 1.
On adoptera la convention suivante : $\deg(0_{\mathbb{K}[X]}) = -\infty$.

Propriété 76 (Intégrité de $\mathbb{K}[X]$)
L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.

Preuve
Si P et Q sont deux polynômes non nuls, alors le produit PQ est non nul car $\deg(PQ) = \deg(P) + \deg(Q) \in \mathbb{N}$. Donc $PQ = 0_{\mathbb{K}[X]} \implies (P = 0_{\mathbb{K}[X]}$ ou $Q = 0_{\mathbb{K}[X]})$.

Propriété 77 (Polynômes inversibles)
Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Preuve
Si P est inversible dans $\mathbb{K}[X]$, alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$, donc P, Q sont non nuls et $\deg(PQ) = \deg(P) + \deg(Q) = \deg(1) = 0$, ce qui entraîne $\deg(P) = \deg(Q) = 0$, donc P est constant non nul (ainsi que Q).

Remarque
Ainsi, $\mathbb{K}[X]^\times = \mathbb{K}_0[X] \setminus \{0\}$, et cet ensemble est en bijection avec $\mathbb{K}^*$.

2) Idéaux, PGCD, PPCM

Théorème 78 (Idéaux de $\mathbb{K}[X]$)
Les idéaux de $\mathbb{K}[X]$ sont exactement les $A\mathbb{K}[X]$, avec $A \in \mathbb{K}[X]$.

Preuve
Soit I un idéal de $\mathbb{K}[X]$.

- Si I est nul, alors $I = A\mathbb{K}[X]$ avec $A = 0_{\mathbb{K}[X]}$.
- Si I est non nul, alors l'ensemble $\{\deg(P),\ P \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément noté $d \in \mathbb{N}$. Ainsi, il existe un polynôme non nul $A \in I$ de degré minimal. Montrons alors que $I = A\mathbb{K}[X]$.
  * $A \in I$ donc par absorption, $A\mathbb{K}[X] \subset I$.
  * Si $P \in I$, alors par division euclidienne, on peut écrire $P = AQ + R$, avec $(Q, R) \in \mathbb{K}[X]^2$ unique et $\deg(R) < \deg(A)$. Or, P et A sont dans I donc $R = P - AQ \in I$. Le caractère minimal de $\deg(A)$ impose alors $R = 0_{\mathbb{K}[X]}$, donc $P = AQ \in A\mathbb{K}[X]$, ce qui prouve $I \subset A\mathbb{K}[X]$.

Dans tous les cas, I est donc du type $A\mathbb{K}[X]$.
Réciproquement, tous les ensembles du type $A\mathbb{K}[X]$ sont des idéaux de $\mathbb{K}[X]$ (cf. prop. 53).

ATTENTION !
A part pour l'idéal nul, le polynôme générateur A n'est pas unique. Par exemple, on a $X\mathbb{K}[X] = 2X\mathbb{K}[X]$. En revanche, tout idéal non nul de $\mathbb{K}[X]$ est engendré par un **unique polynôme unitaire**, puisque d'après les prop. 57, 58 et 77, on a :

$$P\mathbb{K}[X] = Q\mathbb{K}[X] \iff \exists \lambda \in \mathbb{K}^*, \quad Q = \lambda P,$$

ce qui équivaut à $Q = P$ si on impose P et Q unitaires.

Remarque
Ainsi, $\mathbb{K}[X]$ possède les mêmes propriétés que $\mathbb{Z}$: il est commutatif, intègre et tous ses idéaux sont monogènes. C'est lui aussi un "anneau principal".

Propriété 79 (Définition du PGCD de polynômes par les idéaux)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$. Alors, il existe un unique polynôme **unitaire ou nul** *D tel que :*

$$A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X].$$

Le polynôme D est alors le **plus grand diviseur commun** *de $A_1, \cdots, A_n$, c'est-à-dire que :*
(i) $\forall i \in [\![1, n]\!],\ D|A_i$;
(ii) $\forall P \in \mathbb{K}[X],\ ((\forall i \in [\![1, n]\!],\ P|A_i) \implies P|D)$.
On notera $D = pgcd(A_1, \cdots, A_n)$ ou $D = A_1 \wedge \cdots \wedge A_n$.

Preuve (non traitée en classe)
Par la prop. 55, l'ensemble $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$, donc d'après le théorème 78, il existe $D \in \mathbb{K}[X]$ tel que $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$, et ce polynôme D générateur de l'idéal est unique si on le suppose unitaire ou nul.
Montrons ensuite les deux propriétés de D :

(i) Puisque $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$ contient tous les $A_i\mathbb{K}[X]$, on a $A_i\mathbb{K}[X] \subset D\mathbb{K}[X]$, donc (d'après la prop. 58), D divise A_i pour tout i.

(ii) Si $P \in \mathbb{K}[X]$ divise tous les A_i alors $A_i\mathbb{K}[X] \subset P\mathbb{K}[X]$ pour tout i, donc $D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] \subset P\mathbb{K}[X]$, ce qui montre que P divise D.

Remarque (Associativité du PGCD)
Comme dans $\mathbb{Z}$ le pgcd de polynômes est associatif.

Propriété 80 (Relation de Bézout pour les polynômes)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$ et $D = pgcd(A_1, \cdots, A_n)$.
Alors, il existe $(U_1, \cdots, U_n) \in \mathbb{K}[X]^n$ tel que $A_1U_1 + \cdots + A_nU_n = D$.

Preuve (non traitée en classe)
Direct : $D \in D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$, donc D s'écrit sous la forme voulue.

Définition 81 (Polynômes premiers entre eux)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$ avec $n \geq 2$.
On dit que $A_1, \cdots, A_n$ sont **premiers entre eux dans leur ensemble** *lorsque $pgcd(A_1, \cdots, A_n) = 1$.*
On dit que $A_1, \cdots, A_n$ sont **premiers entre eux deux à deux** *lorsque pour tout $(i, j) \in [\![1, n]\!]$, $i \neq j \implies pgcd(A_i, A_j) = 1$.*

Remarque (Analogie avec les entiers premiers entre eux)

Dans l'anneau $\mathbb{K}[X]$, "A et B sont premiers entre eux" signifie que les diviseurs communs à A et B sont les polynômes constants non nuls (donc les éléments inversibles de l'anneau).
C'est tout à fait similaire à l'anneau $\mathbb{Z}$, car pour tous $(a,b) \in \mathbb{Z}^2$, "a et b sont premiers entre eux" signifie que les diviseurs communs à a et b sont -1 et 1 (donc les inversibles de $\mathbb{Z}$).

Propriété 82 (Théorème de Bézout)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$. Alors :
$A_1, \cdots, A_n$ sont premiers entre eux dans leur ensemble ssi
$\exists (U_1, \cdots, U_n) \in \mathbb{K}[X]^n,\ A_1U_1 + \cdots + A_nU_n = 1$.

Preuve (non traitée en classe)

$\boxed{\Rightarrow}$ C'est la relation de Bézout (cf. prop 80) dans le cas où $pgcd(A_1, \cdots, A_n) = 1$.

$\boxed{\Leftarrow}$ Réciproquement, s'il existe $(U_1, \cdots, U_n) \in \mathbb{K}[X]^n$ tel que $\sum_{i=1}^{n} A_iU_i = 1$, alors $pgcd(A_1, \cdots, A_n)$ divise 1, donc vaut 1 (le seul polynôme unitaire divisant 1 est 1).

Corollaire 83 (Lemme de Gauss)
Soit $(A, B, C) \in \mathbb{K}[X]^3$. Si $A|BC$ et si A et B sont premiers entre eux, alors $A|C$.

Preuve (non traitée en classe)
Similaire à la preuve de la prop. 64.

Propriété 84 (Définition du PPCM de polynômes par les idéaux)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$. Alors il existe un unique polynômes **unitaire ou nul** *M tel que*

$$A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X] = M\mathbb{K}[X].$$

Le polynôme M est alors le **plus petit multiple commun** *de $A_1, \cdots, A_n$, c'est-à-dire que :*
(i) $\forall i \in [\![1, n]\!],\ A_i|M$;
(ii) $\forall P \in \mathbb{K}[X], ((\forall i \in [\![1, n]\!],\ A_i|P) \implies M|P)$.
On notera $M = ppcm(A_1, \cdots, A_n)$ ou $M = A_1 \vee \cdots \vee A_n$.

Preuve (non traitée en classe)
Similaire à la preuve de la prop. 66.

Remarque (Associativité du PPCM)
Tout comme le pgcd, le ppcm de polynômes est associatif.

3) Polynômes irréductibles

Définition 85 (Polynôme irréductible)
Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible lorsque :

(i) P est non constant

(ii) $\forall (P_1, P_2) \in \mathbb{K}[X]^2,\ P = P_1 P_2 \implies P_1$ ou P_2 constant.

Remarque

- *Cela revient à dire que P n'est divisible que par les multiples scalaires de P et les polynômes constants.*
- *Les polynômes irréductibles dans $\mathbb{K}[X]$ jouent le même rôle que les nombres premiers dans $\mathbb{Z}$.*
- *On considère qu'un polynôme constant n'est pas irréductible, au même titre que 1 n'est pas un nombre premier.*

Vocabulaire
Un polynôme non constant et non irréductible sera qualifié de "réductible".

Propriété 86 (Exemple fondamental : les polynômes de degré 1)
Tout polynôme de degré 1 est irréductible dans $\mathbb{K}[X]$.

Preuve
Soit P de degré 1 dans $\mathbb{K}[X]$. Si $P = P_1 P_2$, alors $\deg(P_1) + \deg(P_2) = 1$, donc nécessairement $\deg(P_1) = 0$ ou $\deg(P_2) = 0$, ce qui montre que P est irréductible.

Propriété 87 (Lien entre irréductibilité et racines)
Si P est irréductible dans $\mathbb{K}[X]$ et si $\deg(P) \geq 2$, alors P ne possède pas de racines dans $\mathbb{K}$.

Preuve
Si P possède une racine $a \in \mathbb{K}$, alors $X - a$ divise P (faire la division euclidienne, valable dans tout anneau $\mathbb{K}[X]$ avec $\mathbb{K}$ sous-corps de $\mathbb{C}$), donc il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. Comme $\deg(P) \geq 2$, on a $\deg(Q) \geq 1$, donc P se décompose en produit de polynômes non constants : il n'est pas irréductible.

ATTENTION !
La réciproque est fausse. Par exemple, le polynôme $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ ne possède pas de racines dans $\mathbb{R}$ mais n'est pas irréductible dans $\mathbb{R}[X]$.

Théorème 88 (Polynômes irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$)

(*i*) *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

(*ii*) *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.*

Preuve (non traitée en classe)

(*i*) Résulte du **théorème de d'Alembert-Gauss** ("tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$"). Ce théorème difficile, vu en MP2I, sera admis. En l'appliquant, on obtient par la prop. précédente que tout polynôme de $\mathbb{C}[X]$ de degré ≥ 2 est réductible.

(*ii*)
- Soit $P \in \mathbb{R}[X]$ de degré 2. Pour des raisons de degré, P est réductible ssi il possède un diviseur de $\mathbb{R}[X]$ de degré 1, c'est-à-dire au moins une racine réelle. Donc P est irréductible ssi son discriminant est strictement négatif.
- Soit maintenant $P \in \mathbb{R}[X]$ de degré ≥ 3.
  Si P possède une racine réelle, alors P est réductible dans $\mathbb{R}[X]$ d'après la proposition précédente.

Sinon, vu que $\mathbb{R}[X] \subset \mathbb{C}[X]$, P possède d'après le théorème de d'Alembert-Gauss au moins une racine $\alpha \in \mathbb{C} \setminus \mathbb{R}$, et $\overline{\alpha}$ est aussi racine de P, de même multiplicité que α (voir cours MP2I). Montrons alors que $(X-\alpha)(X-\overline{\alpha})$ divise P : en écrivant une division euclidienne, on a

$$P = (X-\alpha)(X-\overline{\alpha})Q + R,$$

avec $Q, R \in \mathbb{C}[X]$ et $\deg(R) \leq 1$. Puisque $P(\alpha) = P(\overline{\alpha}) = 0$, on déduit $R(\alpha) = R(\overline{\alpha}) = 0$ avec $\alpha \neq \overline{\alpha}$, donc $R = 0$ (pour des raisons de degré), puis

$$P = (X-\alpha)(X-\overline{\alpha})Q.$$

Mais il reste à montrer que cette divisibilité à lieu **dans $\mathbb{R}[X]$**. Déjà, on a

$$P \in \mathbb{R}[X], \qquad (X-\alpha)(X-\overline{\alpha}) = X^2 - 2Re(\alpha)X + |\alpha|^2 \in \mathbb{R}[X].$$

Donc par division euclidienne dans $\mathbb{R}[X]$, il existe $(\tilde{Q}, \tilde{R}) \in \mathbb{R}[X]^2$ tel que

$$P = (X-\alpha)(X-\overline{\alpha})\tilde{Q} + \tilde{R}.$$

Par unicité du couple (Q, R), on en déduit que $Q = \tilde{Q} \in \mathbb{R}[X]$, ce qui établit la divisibilité voulue. Finalement, $P = (X^2 - 2Re(\alpha)X + |\alpha|^2)Q$ dans $\mathbb{R}[X]$ avec $\deg(Q) \geq 1$, ce qui montre que P est réductible.

Remarque

- *Bien sûr, il y a plus de polynômes irréductibles dans $\mathbb{R}[X]$ que dans $\mathbb{C}[X]$, puisque si $P = P_1P_2$ dans $\mathbb{R}[X]$ avec P_1, P_2 non constants, alors la même relation susbsiste dans $\mathbb{C}[X]$ par inclusion.*
- *Dans $\mathbb{Q}[X]$ c'est plus compliqué, il peut y avoir des polynômes irréductibles de degré ≥ 3 : par exemple $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$. En effet, s'il ne l'était pas, il possèderait un diviseur de degré 1, et donc $X^3 - 2$ aurait une racine dans $\mathbb{Q}$, ce qui est impossible car dans $\mathbb{Z}$, l'égalité $a^3 = 2b^3$ est impossible (observer la valuation p-adique de 2 dans cette égalité, elle est à la fois congrue à 0 et à 1 modulo 3, ce qui est impossible).*

Lemme 89
Soit $P \in \mathbb{K}[X]$ irréductible. Alors P est premier avec tout polynôme qu'il ne divise pas.

Preuve (non traitée en classe)
Soit $Q \in \mathbb{K}[X]$ non multiple de P. Si D est un diviseur commun de P et Q, alors puisque P est irréductible, D est constant ou $D = \lambda P$ avec $\lambda \in \mathbb{K}^*$. Mais $D = \lambda P$ entraîne $P|Q$, ce qui est exclu par hypothèse. Donc D est constant, ce qui montre que P et Q sont premiers entre eux.

Remarque
Dans $\mathbb{Z}$, on a la même chose : si p est un nombre premier, alors p est premier avec tout entier qu'il ne divise pas.

Propriété 90 (Lemme d'Euclide)
Soit P, P_1, P_2 dans $\mathbb{K}[X]$. Si P est irréductible et si P divise P_1P_2, alors P divise P_1 ou P divise P_2.

Preuve (non traitée en classe)
Supposons P irréductible et $P|P_1P_2$. Si P ne divise pas P_1, alors P est premier avec P_1 d'après le lemme précédent, donc par le lemme de Gauss, P divise P_2.

Remarque
Ceci se généralise de manière immédiate au cas où P divise un produit fini de polynômes.

Enfin, on dispose comme dans $\mathbb{Z}$ d'un théorème de décomposition en facteurs irréductibles :

Théorème 91 (Décomposition en facteurs irréductibles dans $\mathbb{K}[X]$)
Tout polynôme P non constant peut s'écrire à une constante non nulle près comme produit de polynômes **unitaires et irréductibles** *dans $\mathbb{K}[X]$ (pas nécessairement distincts).*
De plus, cette décomposition est unique à l'ordre des facteurs près.

Remarque

- *On peut inclure les polynômes constants en écrivant un produit vide (qui vaut 1 par convention).*
- *En groupant les facteurs irréductibles identiques dans cette décomposition, on peut donc écrire :*

$$P = \lambda \prod_{i=1}^{p} Q_i^{\alpha_i},$$

avec $\lambda = cd(P) \in \mathbb{K}^*$ (le coefficient dominant de P), $p \in \mathbb{N}^*$, les Q_i unitaires et irréductibles, et les $\alpha_i \in \mathbb{N}^*$. On dit alors (comme dans $\mathbb{Z}$) que les α_i sont les **valuations Q_i-adiques** *de P.*

Preuve (non traitée en classe)

- **Existence** : on montre le résultat par récurrence forte sur $n = \deg(P)$.
  * Si $n = 1$, alors P est irréductible, donc en notant λ son coefficient dominant, on a bien $P = \lambda Q$ avec Q unitaire et irréductible.
  * Soit $n \in \mathbb{N}^*$. Supposons le résultat vrai pour tout polynôme de degré inférieur ou égal à n. Etant donné un polynôme P de degré $n+1$, deux cas se présentent :
    - si P est irréductible, alors en factorisant par son coefficient dominant, on a directement la décomposition souhaitée.
    - sinon, P s'écrit $P = QR$ avec Q et R non constants, $\deg(Q) < n+1$ et $\deg(R) < n+1$. On peut alors appliquer l'hypothèse de récurrence à P et Q et regrouper les deux décompositions pour obtenir le résultat souhaité.
- **Unicité** : comme dans le cas des entiers, on peut définir pour tout polynôme irréductible Q la valuation Q-adique :

$$\forall P \in \mathbb{K}[X] \setminus \{0\}, \quad \nu_Q(P) = max\{k \in \mathbb{N},\ Q^k | P\}.$$

Supposons que Q admette deux décompositions. Quitte à les compléter par des termes du type Q^0, on peut les écrire :

$$P = \lambda \prod_{i=1}^{p} Q_i^{\alpha_i} = \mu \prod_{i=1}^{p} Q_i^{\beta_i},$$

où les Q_i sont unitaires, irréductibles et distincts, les $\alpha_i, \beta_i \in \mathbb{N}$ sont les valuations Q_i-adiques et $\lambda, \mu \in \mathbb{K}^*$.
Tout d'abord λ et μ sont nécessairement égaux au coefficient dominant de P, donc $\lambda = \mu$.
Si par exemple, $\alpha_p > \beta_p$, alors en divisant par $Q_p^{\beta_p}$ et par λ, on obtient

$$Q_p^{\alpha_p - \beta_p} \prod_{i=1}^{p-1} Q_i^{\alpha_i} = \prod_{i=1}^{p-1} Q_i^{\beta_i}.$$

Cela entraîne que Q_p divise $\prod_{i=1}^{p-1} Q_i^{\beta_i}$, donc Q_p divise un des Q_i (avec $i < p$) par le lemme d'Euclide. Vu que Q_i est irréductible, Q_p est soit constant, soit un multiple scalaire de Q_i (donc $Q_p = Q_i$ puisque ces polynômes sont unitaires), et ces deux cas sont inenvisageables.
On conclut que $\alpha_p \leq \beta_p$. Symétriquement, on a $\alpha_p \geq \beta_p$, donc $\alpha_p = \beta_p$.
Ce raisonnement ne dépend pas du facteur choisi dans la décomposition (on a pris le dernier par commodité), donc on peut affirmer que $\alpha_k = \beta_k$ pour tout $1 \leq k \leq p$.

Exemple
Décomposer le polynôme $X^6 - 1$ en facteurs irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.
Sa décomposition en facteurs irréductibles dans $\mathbb{C}[X]$ est

$$X^6 - 1 = \prod_{k=1}^{5} (X - e^{2ik\pi/6}) = (X-1)(X+1)(X-j)(X-\overline{j})(X+j)(X+\overline{j}),$$

où $j = e^{2i\pi/3}$.
En regroupant deux à deux les facteurs complexes conjugués, on obtient la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$:

$$X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1).$$