CH03 : Structures algébriques usuelles

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 : $\forall (x,y,z) \in G^3,\ y*x = z*x \implies y = z$.

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.

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).

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 : $\forall x \in H,\ x^{-1} \in H$.

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

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.

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 :

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

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.

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

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

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 $n \in \mathbb{N}$.

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

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

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.

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.*

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 $Ker(\varphi) = \{e_G\}$.

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.

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**.

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 :

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

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 :

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

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.

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.*

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.

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 $n = Card(G)$.

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 $ord(x)$.*

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.

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.

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 $Card(G)$.

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 $x \times y$.

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

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

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

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 $U(A)$.

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).*

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 $(\varphi(x))^{-1} = \varphi(x^{-1})$.

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

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 $Ker(\varphi) = \varphi^{-1}(\{0_B\})$.*

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.

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 $Ker(\varphi) = \{0_A\}$.

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.

3) Anneaux intègres

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

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

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 $ba = ca) \implies b = c$.

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.*

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

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 $x \in L$, $x \neq 0_K \implies x^{-1} \in L$.

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) $\forall x \in I,\ \forall a \in A,\ xa \in I$.

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**.

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.

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.

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**.

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 $aA=bA$.

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.

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 $d=a_1\wedge\cdots\wedge a_n$.

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 $a_1u_1+\cdots+a_nu_n=d$.

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 $(i,j)\in[\![1,n]\!]$, $i\neq j\implies pgcd(a_i,a_j)=1$.*

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 $\exists(u_1,\cdots,u_n)\in\mathbb{Z}^n,\ a_1u_1+\cdots+a_nu_n=1$.

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 $a|c$.

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.

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 $m=a_1\vee\cdots\vee a_n$.

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 $\overline{1}$.

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 $mu + nv = 1$.

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 :*

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

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.

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.

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.

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**.

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

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

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

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

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

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

1) Premières propriétés

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

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

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

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 $D = A_1 \wedge \cdots \wedge A_n$.

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 $A_1U_1 + \cdots + A_nU_n = D$.

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 $(i, j) \in [\![1, n]\!]$, $i \neq j \implies pgcd(A_i, A_j) = 1$.*

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
$\exists (U_1, \cdots, U_n) \in \mathbb{K}[X]^n,\ A_1U_1 + \cdots + A_nU_n = 1$.

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 $A|C$.

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 $M = A_1 \vee \cdots \vee A_n$.

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.*

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 $\mathbb{K}[X]$.

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 $\mathbb{K}$.

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.

Lemme 89
Soit $P \in \mathbb{K}[X]$ irréductible. Alors P est premier avec tout polynôme 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 $P_1 P_2$, alors P divise P_1 ou P divise P_2.

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.