1 Arithmétique dans $\mathbb{Z}$

1.1 Division euclidienne et congruences

Théorème 1.1.1 (Division eucldienne) *Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}.$$

*q est le **quotient** et r le **reste** de la division euclidienne de a par b.*

Proposition 1.1.1 (Congruence et opérations) *Soient a, a', b, $b' \in \mathbb{Z}$ et m, $n \in \mathbb{N}^\star$.*
Si $a \equiv b[n]$ et $a' \equiv b'[n]$, alors $a + a' \equiv b + b'[n]$. et $aa' \equiv bb'[n]$.

Exemple 1.1.1 *Le chiffre des unités de 13^{65363} est 7.*

1.2 Nombres premiers

Définition 1.2.1 (Valuation p-adique) *Soient $a \in \mathbb{Z}^\star$ et p un nombre premier. Il existe un unique entier naturel n tel que p^n divise a et p^{n+1} ne divise pas a. L'entier n est appelé la valuation de p dans a et est noté $v_p(a)$.*

Théorème 1.2.1 (Décomposition en facteurs premiers) *Tout entier $n \geq 2$ admet une décomposition en facteurs premiers, c'est-à-dire qu'il existe $p_1, p_2, ..., p_k$ des entiers premiers deux à deux distincts et $(\alpha_1, \alpha_2, ..., \alpha_k) \in (\mathbb{N}^*)^k$ tels que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} = \prod_{l=1}^{k} p_l^{\alpha_l}$.*
Autrement dit : $n = \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et cette décomposition est unique. La décomposition est unique à l'ordre près des facteurs.

Proposition 1.2.1 (Critère de divisibilité à l'aide de la valuation) *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ et $m = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$, avec $p_1, p_2, ..., p_k$ des entiers premiers deux à deux distincts. Alors $mn | m$ si et seulement si : $\forall l \in [\![1,k]\!]$, $\alpha_l \leq \beta_l$.*

Exemple 1.2.1 *Soient $a, b \in \mathbb{N}^*$. Montrer que $a^2 | b^2$ implique que : $a|b$, puis $\sqrt{2}$ est irrationnel.*

1.3 PGCD, PPCM et applications

1.3.1 PGCD

Définition 1.3.1 (PGCD) *Soit $(a,b) \in (\mathbb{N}^*)^2$. Le plus grand élément diviseur commun de a et b est appelé pgcd de a et b. On le note $pgcd(a,b)$ ou $a \wedge b$.*

Proposition 1.3.1 (Expression du PGCD avec les valuations) *Soient $p_1, p_2, ..., p_k$ des entiers premiers deux à deux distincts et $(\alpha_1, \alpha_2, ..., \alpha_k) \in \mathbb{N}^k$ et $(\beta_1, \beta_2, ..., \beta_k) \in \mathbb{N}^k$ tels que $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ et $b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$. Alors $a \wedge b = \prod_{l=1}^{k} p_l^{\min(\alpha_l, \beta_l)}$.*

Définition 1.3.2 (Couple d'entiers premiers entre eux) *Soient a et b deux entiers. On dit qu'ils sont premiers entre eux si $a \wedge b = 1$, ce qui siginifie que les seuls diviseurs communs de a et b sont 1 et -1.*

Remarque 1.3.1 *Si $d = a \wedge b$, si et seulement si il existe donc a' et b' dans $\mathbb{Z}^*$ tels que $a = da'$ et $b = db'$ et on a : $a' \wedge b' = 1$.*

Proposition 1.3.2 (Algorithme d'Euclide) *Soit $(a, b) \in (\mathbb{N}^*)^2$. Soit r le reste de la division euclidienne de a par b. Alors on a : $a \wedge b = b \wedge r$.*

Soit $(a, b) \in (\mathbb{N}^*)^2$. On veut calculer $a \wedge b$. Pour ceci nous allons appliquer l'algorithme d'Euclide : on forme une suite d'entier $r_0, r_1, r_2, r_3, ...$ en commençant par $r_0 = a$ et $r_1 = b$. Pour k dans $\mathbb{N}^*$, on suppose les deux entiers naturels non nuls r_{k-1} et r_k construits. On note r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k ($r_{k-1} = q_{k+1}r_k + r_{k+1}$ avec q_{k+1} un entier) et nous avons : $0 \leq r_{k+1} < r_k$. De plus grâce à la proposition précédente, nous avons : $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$. La suite d'entiers $r_0, r_1, r_2, r_3, ...$ est strictement décroissante et donc il existe k_0 tel que : $r_{k_0} > 0$ et $r_{k_0+1} = 0$. Ainsi on a : $r_{k_0} | r_{k_0-1}$ et donc : $r_{k_0} \wedge r_{k_0-1} = r_{k_0}$. Or nous avons : $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = ... = r_k \wedge r_{k-1} = ... r_{k_0} \wedge r_{k_0-1} = r_{k_0}$. Ainsi le pgcd de a et b est le dernier reste non nul de la succession de divisions euclidiennes que l'on a effectuées.

Définition 1.3.3 (PGCD d'une famille d'entiers) *L'entier $a_1 \wedge \cdots \wedge a_n$ est le plus grand commun diviseur des entiers $a_1, \ldots, a_n$, soit* $\max(Div(a_1) \cap ... \cap Div(a_n))$.

Définition 1.3.4 (Entiers premiers entre eux dans leur ensemble) *Si le pgcd de $a_1, \ldots, a_n$ vaut 1, alors ces entiers sont premiers entre eux dans leur ensemble.*

1.3.2 Applications du PGCD

Proposition 1.3.3 (Relation de Bézout) *Soient a, $b \in \mathbb{Z}^\star$ et on pose $d = a \wedge b$. Il existe deux entiers u, v tels que $d = au + bv$. De plus, $\{am + bn, (m, n) \in \mathbb{Z}^2\} = d\mathbb{Z}$.*

Théorème 1.3.1 (Bézout) *Soient a, $b \in \mathbb{Z}^\star$. On a : $a \wedge b = 1$ si et seulement s'il existe m, $n \in \mathbb{Z}$ tels que $1 = ma + nb$.*

Exemple 1.3.1 *Résoudre* $(S) : \begin{cases} x \equiv 6[17] \\ x \equiv 4[15] \end{cases}$, *dans lequel l'inconnue x appartient à $\mathbb{Z}$.*

Proposition 1.3.4 (Relation de Bézout pour une famille d'entiers) *Si d est le pgcd de $a_1, \ldots, a_n$, alors il existe des entiers relatifs $u_1, \ldots, u_n$ tels que $a_1u_1 + \cdots + a_nu_n = d$.*

Théorème 1.3.2 (Bézout pour une famille d'entiers) *$a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble si et seulement s'il existe des entiers relatifs $u_1, \ldots, u_n$ tels que $a_1u_1 + \cdots + a_nu_n = 1$.*

Théorème 1.3.3 (Gauss) *Soient a, b, $c \in \mathbb{Z}^\star$. Si $a|bc$ et $a \wedge c = 1$, alors $a|b$.*

Exemple 1.3.2 *Soit p un nombre premier. Soit $k \in [\![1, p-1]\!]$, alors p divise* $\binom{p}{k}$.

1.3.3 PPCM

Définition 1.3.5 *Soit $(a, b) \in (\mathbb{N}^*)^2$. Le plus petit multiple commun est appelé ppcm de a et b. On le note $ppcm(a, b)$ ou $a \vee b$.*

Proposition 1.3.5 (Expression du PPCM avec les valuations) *Soient $p_1, p_2, ..., p_k$ des entiers premiers deux à deux distincts et $(\alpha_1, \alpha_2, ..., \alpha_k) \in \mathbb{N}^k$ et $(\beta_1, \beta_2, ..., \beta_k) \in \mathbb{N}^k$ tels que $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ et $b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$. Alors $a \vee b = \prod_{l=1}^{k} p^{\max(\alpha_l, \beta_l)}$.*

2 L'anneau $\mathbb{K}[X]$

2.1 Divisibilité et division euclidienne

Théorème 2.1.1 (Division euclidienne) *Soient A et B deux polynômes sur $\mathbb{K}$, avec B non nul. Il existe un unique couple (Q, R) de polynômes sur $\mathbb{K}$ telles que*

$$A = BQ + R \quad et \quad d^\circ R < d^\circ B.$$

C'est la division euclidienne de A par B. On appelle Q le quotient et R le reste.

2.2 PGCD, PPCM

Définition 2.2.1 (PGCD et PPCM) *1. Il existe un unique polynôme nul ou unitaire D tel que*

$$\forall P \in \mathbb{K}[X],\ (P|A \text{ et } P|B) \Leftrightarrow P|D.$$

Autrement dit D est le polynôme unitaire de plus haut degré de qui divise A et B.
*Le polynôme D est le **plus grand commun diviseur** de A et B, noté $A \wedge B$.*

2. Il existe un unique polynôme M nul ou unitaire tel que que

$$\forall P \in \mathbb{K}[X],\ (A|P \text{ et } B|P) \Leftrightarrow M|P.$$

*Le polynôme M est le **plus petit commun multiple** de A et B, noté $A \vee B$.*

Définition 2.2.2 (Polynômes premiers entre eux) *Les polynômes A et B sont premiers entre eux si $A \wedge B = 1$.*

Remarque 2.2.1 *Si $A \wedge B = D$, alors il existe A_1 et B_1 dans $\mathbb{K}[X]$ tels que $A = DA_1$ et $B = DB_1$ et $A_1 \wedge B_1 = 1$.*

Proposition 2.2.1 (Relation de Bézout) *Soient $A, B \in \mathbb{K}[X]$. On pose $D = A \wedge B$. Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$.*

Théorème 2.2.1 (Théorème de Bézout) *$A \wedge B = 1$ si et seulement s'il existe deux polynômes U, V tels que $AU + BV = 1$.*

Remarque 2.2.2 *(IMPORTANTE) L'algorithme d'Euclide vu sur $\mathbb{Z}$ est le même sur $\mathbb{K}[X]$.*

Exemple 2.2.1 $(X^4 - 3X^3 + X^2 + 4) \wedge (X^3 - 3X^2 + 3X - 2) = X - 2$.

Théorème 2.2.2 (Théorème de Gauss) *Soient $(A, B, C) \in \mathbb{K}[X]^2$ tels que A divise BC et $A \wedge B = 1$. Alors, A divise C.*

Exemple 2.2.2 *Soient $m, n \in \mathbb{N}^*$ et $(F, G) \in \mathbb{C}_n[X] \times \mathbb{C}_m[X]$ avec $d^\circ F = n$ et $d^\circ G = m$. Soit $\phi : \begin{cases} \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X] & \to & \mathbb{C}_{m+n-1}[X] \\ (U, V) & \mapsto & UF + VG \end{cases}$. Montrer que ϕ est un isomorphisme d'espaces vectoriels si et seulement si : $F \wedge G = 1$.*

Définition 2.2.3 (PGCD d'une famille finie de polynômes) *Soient $A_1, ..., A_n \in \mathbb{K}[X]$ des polynômes dont l'un au moins est non nul. On appelle plus grand commun diviseur (ou PGCD) de $A_1, ..., A_n$ le diviseur commun unitaire de $A_1, ..., A_n$ de degré maximal. On note celui-ci $A_1 \wedge ... \wedge A_n$.*

Proposition 2.2.2 (Relation de Bézout) *Soient n un entier supérieur ou égal à 2, $A_1, \ldots, A_n$ une famille de n polynômes et D leur PGCD. Il existe des polynômes $U_1, \ldots, U_n$ tels que*

$$A_1U_1 + \cdots + A_nU_n = D.$$

Définition 2.2.4 (Premiers entre eux dans leur ensemble) *Soient n un entier supérieur ou égal à 2, $A_1, \ldots, A_n$ une famille de n polynômes. Ces polynômes sont premiers entre eux dans leur ensemble si leur PGCD vaut 1.*

Théorème 2.2.3 (Théorème de Bézout) *Soient n un entier supérieur ou égal à 2, $A_1, \ldots, A_n$ une famille de n polynômes. Les propositions suivantes sont équivalentes.*

1. *Les polynômes $A_1, \ldots, A_n$ sont premiers entre eux dans leur ensemble.*
2. *Il existe des polynômes $U_1, \ldots, U_n$ tels que $A_1U_1 + \cdots + A_nU_n = 1$.*

2.3 Polynômes irréductibles

Définition 2.3.1 (Polynômes irréductibles) *Un polynôme A de $\mathbb{K}[X]$ est dit irréductible dans $\mathbb{K}[X]$ lorsque :*

1. *$d^\circ A \geq 1$ (c'est-à-dire A est non constant).*
2. *Les seuls diviseurs de A sont les polynômes constants et les polynômes associés à A (les polynômes de la forme λA avec λ dans $\mathbb{K}^*$).*

Théorème 2.3.1 (Décomposition d'un polynôme comme produit d'irréductibles) *Soit A un polynôme non constant. Il se décompose de façon à l'ordre des facteurs près : $A = \lambda P_1^{n_1}...P_k^{n_k}$,*
avec $\lambda \in \mathbb{K}^*$, $P_1, ..., P_k$ des polynômes unitaires irréductibles deux à deux non associés et $n_1, ..., n_k$ dans $\mathbb{N}^*$.

Proposition 2.3.1 (Polynômes irréductibles et décomposition sur $\mathbb{C}$)

1. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.*
2. *Soit A polynôme non constant de $\mathbb{C}[X]$ avec $n = d^\circ A$ (qui est dans $\mathbb{N}^*$). Alors il existe une unique décomposition à l'ordre près de A sous la forme $\lambda \prod_{i=1}^{r}(X-\alpha_i)^{k_i}$, où λ est le coefficient dominant de A, les α_i sont les racines deux à deux distinctes de A et k_i est l'ordre de multiplicité de α_i.*

Proposition 2.3.2 (Polynômes irréductibles et décomposition sur $\mathbb{R}$)

1. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré deux ayant un discriminant strictement négatif.*
2. *Soit $A \in \mathbb{R}[X]$ non constant. Alors A s'écrit sous la forme $\lambda \prod_{i=1}^{r}(X-\alpha_i)^{k_i} \prod_{i=1}^{s}(X^2+b_iX+c_i)^{l_i}$, où $\alpha_1, ..., \alpha_r$ dans $\mathbb{R}$ deux à deux distincts, les polynômes réels $X^2+b_iX+c_i$ sont deux à deux disctincts et à discriminant strictement négatif et les k_i et l_i sont des entiers naturels non nuls.*

Exemple 2.3.1 *Dans $\mathbb{C}[X]$, on a : $X^n - 1 = \prod_{k=0}^{n-1}(X - e^{\frac{2ik\pi}{n}})$.*

2.4 Fractions rationnelles

Ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Définition 2.4.1 (Degré) *Si $F = \dfrac{P}{Q}$, avec $P, Q \in \mathbb{K}[X]$ est non nulle, alors $\deg(P) - \deg(Q)$ est indépendant du représentant choisi. Cette quantité est le degré de F. Par convention, $\deg(0) = -\infty$.*

Proposition 2.4.1 (Partie entière) *Il existe un unique couple $(E, F_1) \in \mathbb{K}[X] \times \mathbb{K}(X)$ tel que $F = E + F_1$ et $\deg(F_1) < 0$. E est la **partie entière** de F.*

Définition 2.4.2 (Pôle) *Soit $F \in \mathbb{K}(X)$ de forme irréductible $\dfrac{P}{Q}$. Les racines de Q sont les pôles de F. Si α est une racine d'ordre k de Q, on dit que α est un pôle d'ordre k de F.*

Proposition 2.4.2 (Décomposition en éléments simples dans $\mathbb{C}(X)$) *Soit $F \in \mathbb{C}(X)$ et $(\alpha_k)_{1\leq k\leq n} \in \mathbb{C}^n$ les pôles de F d'ordres $(r_k)_{1\leq k\leq n}$. F s'écrit de manière unique $F = E + \sum_{k=1}^{n}\sum_{j=1}^{r_k}\dfrac{\lambda_{k,j}}{(X-\alpha_k)^j}$, où E est la partie entière de F et pour tout $k \in [\![1, n]\!]$, $\sum_{j=1}^{r_k}\dfrac{\lambda_{k,j}}{(X-\alpha_k)^j}$ est la partie polaire de F relative à α_k. C'est sa décomposition en éléments simples.*

Exemple 2.4.1 (Dérivée logarithmique) *Si* $P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{n_k}$, *alors* $\dfrac{P'}{P} = \sum_{k=1}^{p} \dfrac{n_k}{X - \alpha_k}$.

Proposition 2.4.3 (Décomposition en éléments simples dans $\mathbb{R}(X)$) *Soit* $F = \dfrac{P}{Q}$ *une fraction rationnelle à coefficients réels, écrite sous forme irréductible. Notons*
$Q = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{r_k} \prod_{k=1}^{q} (X^2 + \beta_k X + \gamma_k)^{s_k}$ *la factorisation de* Q *en produits de polynômes irréductibles dans* $\mathbb{R}[X]$. *Alors* F *s'écrit de manière unique*

$$F = E + \sum_{k=1}^{p} \sum_{j=1}^{r_k} \frac{\lambda_{k,j}}{(X - \alpha_k)^j} + \sum_{k=1}^{q} \sum_{j=1}^{s_k} \frac{c_{k,j} X + d_{k,j}}{(X^2 + \beta_k + \gamma_k)^j},$$

où E *est la partie entière de* F *et les* $\lambda_{k,j}$, $c_{k,j}$, $d_{k,j}$ *sont des réels. C'est la déomposition en éléments simples de* F *dans* $\mathbb{R}(X)$.

La proposition suivante est valable pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$:

Proposition 2.4.4 (Coefficient d'un pôle simple) *Si* $F = P/Q \in \mathbb{K}(X)$ *et* α *est racine* <u>simple</u> *de* Q, *alors* $Q = (X - \alpha)S$, *avec* $S(\alpha) \neq 0$ *et le coefficient de* $\dfrac{1}{X - \alpha}$ *dans la décomposition en élément simple de* F : $\dfrac{P(\alpha)}{S(\alpha)} = \dfrac{P(\alpha)}{Q'(\alpha)}$.

3 Groupes

3.1 Groupes et sous-groupes

3.1.1 Groupes

Définition 3.1.1 (Groupe) *Soit* G *un ensemble muni d'une loi de composition interne* $*$
$(\forall x, y \in G,\ x * y \in G)$.
On dit que G *a une structure de groupe si :*

- *La loi* $*$ *est associative :* $\forall x, y, z \in G,\ x * (y * z) = (x * y) * z$.
- *La loi* $*$ *est munie d'un élément neutre* $e \in G$: $\forall x \in G,\ x * e = e * x = x$.
- *Tout élément* x *de* G *possède un symétrique ou inverse :* $\exists x' \in G,\ x * x' = x' * x = e$.
  On note $x^{-1} = x'$.

Remarque 3.1.1 $\forall x, y \in G,\ (x * y)^{-1} = y^{-1} * x^{-1}$.

Exemple 3.1.1

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$ *sont des groupes. Ils sont tous commutatifs.*
   $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *admettent* 0 *pour élément neutre et pour* x *dans l'un de ces groupes, l'inverse est* $-x$.
   $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$ *admettent* 1 *pour élément neutre et pour* x *dans l'un de ces groupes, l'inverse est* $1/x$.
2. $(GL_n(\mathbb{K}), .)$ *est un groupe de matrices pour la multiplication matricelle, d'élément neutre* I_n.
3. $GL(E)$, *avec* E *un espace vectoriel, d'élément neutre* Id_E.

Définition 3.1.2 (Produit fini de groupes) *Soient* $(G_1, *_1)$,...,$(G_n, *_n)$ n *groupes. Soit* $*$ *la loi de composition interne définie sur* $G_1 \times ... \times G_n$ *par :*
$\forall (g_1, h_1, ..., g_n, h_n,) \in G_1^2 \times ... \times G_n^2,\ \ (g_1, ..., g_n) * (h_1, ..., h_n) = (g_1 *_1 h_1, ..., g_n *_n h_n)$.
$(G_1 \times ... \times G_n, *)$ *est le groupe produit de* $G_1, ..., G_n$.

3.1.2 Sous-groupes

Proposition 3.1.1 (Caractérisation des sous-groupes) *Soit H une partie d'un groupe $(G,*)$. H est un sous-groupe de G si et seulement si :*

- $e \in H$.
- $\forall x, y \in H,\ x * y^{-1} \in H$.

Exemple 3.1.2 *Soit $(G,*)$ un groupe. Montrer que $Z = \{g \in G,\ \forall x \in G,\ xg = gx\}$ est un sous-groupe de G.*

3.1.3 Intersection de groupes, groupe engendré par une partie

Proposition 3.1.2 (Intersection de sous-groupes) *Soit $(H_i)_{i\in I}$ une famille (finie ou infinie) de sous-groupes d'un groupe $(G,*)$. Alors $\bigcap_{i\in I} H_i$ est sous-groupe de G.*

Définition 3.1.3 (Sous-groupe engendré par une partie) *Soit $(G,*)$ un groupe et A une partie de G. On note $\langle A\rangle$ le sous-groupe engendré par A qui est, au sens de l'inclusion, le plus petit sous-groupe de G contenant A.*

3.1.4 Les sous-groupes du groupe $(\mathbb{Z},+)$

Proposition 3.1.3 (Sous-groupes de $\mathbb{Z}$) *Pour $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$ des multiples de n est un sous-groupe de $(\mathbb{Z},+)$. De plus, tout sous-groupe de $(\mathbb{Z},+)$ est de cette forme.*

3.2 Morphisme de groupe

3.2.1 Définition et exemples

Définition 3.2.1 (Morphisme de groupes) *Soient $(G,*)$ et $(H,\top)$ deux groupe et une application $f : G \to H$. On dit que f est un morphisme de groupe si $\forall (x,y) \in G^2$, $f(x*y) = f(x)\top f(y)$.*
On note en général $f : (G,*) \to (H,\top)$ un morphisme entre $(G,*)$ et $(H,\top)$.

Proposition 3.2.1 *Soit $(G,*)$ et $(H,\top)$ deux groupes de neutres respectifs e_G et e_H. Soit $f : G \to H$ un morphisme de groupes. Alors :*

1. *$f(e_G) = e_H$.*
2. *$\forall x \in G,\ f(x)^{-1} = f(x^{-1})$.*

Exemple 3.2.1
1. *Le déterminant $\det : (GL_n(\mathbb{C}),\times) \mapsto (\mathbb{C}^*,\times)$ est un morphisme de groupes.*
2. *Les morphismes de groupes $g : (\mathbb{Q},+) \to (\mathbb{R},+)$ sont de la forme $g : x \mapsto x\alpha$, avec $\alpha \in \mathbb{R}$.*

3.2.2 Image et noyau d'un morphisme

Proposition 3.2.2 (Image directe et image réciproque de sous-groupes par un morphisme) *Soit $f : (G,*) \to (H,\top)$ un morphisme de groupes, et G' et H' des sous-groupes de G et H respectivement. Alors $f(G')$ est un sous-groupe de H et $f^{-1}(H')$ est un sous-groupe de G.*

Définition 3.2.2 (Noyau et image d'un morphisme) *Soit $f : (G,*) \to (H,\top)$ un morphisme de groupes.*

1. *On appelle noyau de f : $\mathrm{Ker}\,(f) = f^{-1}(\{e_H\}) = \{x \in G\,;\, f(x) = e_H\}$ qui est un sous-groupe de G.*
2. *On appelle image de f : $\mathrm{Im}\,(f) = f(G) = \{y \in H\,;\, \exists x \in G,\, y = f(x)\}$ qui est un sous-groupe de H.*

Proposition 3.2.3 (Caractérisation des morphismes injectifs/surjectifs) *Soit $f : (G,*) \to (H,\top)$ un morphisme de groupes.*

1. *f est injective si et seulement si $\mathrm{Ker}\,(f) = \{e_G\}$.*

2. *f est surjective si et seulement si* $\mathrm{Im}(f) = H$.

Définition 3.2.3 (Isomorphisme, automorphismes de groupes) *Soit $(G, *)$ et $(H, \top)$ deux groupes. Un isomorphisme de groupe entre G et H est un morphisme de groupes bijectif entre G et H.*
Dans ce cas, on dit que G et H sont isomorphes.

Proposition 3.2.4 (Réciproque d'un isomorphisme de groupes) *La bijection réciproque d'un isomorphisme de groupes est elle-même un isomorphisme de groupes.*

3.3 Groupes monogènes et cycliques

3.3.1 Définitions des groupes monogènes et cycliques

Définition 3.3.1 (Groupe monogène) *Un groupe $(G, *)$ est monogène s'il existe $g \in G$ tel que :* $G = \{g^k,\ k \in \mathbb{Z}\}$.

Définition 3.3.2 (Groupe cyclique) *Un groupe est dit cyclique lorsqu'il est monogène et fini.*

Exemple 3.3.1 1. *$(\mathbb{Z}, +)$ est monogène, engendré par* 1.
2. *$(\mathbb{U}_n, \times)$ est cyclique, engendré par* $e^{\frac{2i\pi}{n}}$.

Proposition 3.3.1 (Description des groupes monogènes infinis) *Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.*

3.4 Ordre d'un élément dans un groupe

Définition 3.4.1 (Ordre d'un élément) *Soit $(G, *)$ un groupe d'élément neutre e_G. Soit $g \in G$. On dit que g est d'ordre fini s'il existe un entier naturel n non nul tel que $g^n = e_G$.*
L'ordre de g est le plus petit entier naturel n non nul tel que : $g^n = e_G$.

Proposition 3.4.1 (Sous-groupe engendré par un élément d'ordre fini) *Si g est d'ordre n, alors*

$$\forall k \in \mathbb{N},\ g^k = e_G \Leftrightarrow n|k \text{ et } \langle g \rangle = \{e, g, g^2, ..., g^{n-1}\}$$

Exemple 3.4.1 *Soient G un groupe et $a, b \in G$ tels que $ab = ba$ avec a d'ordre p et b d'ordre q. Si p et q sont premiers entre eux, quel est l'ordre de ab ?*

Théorème 3.4.1 (Ordre d'un élément dans un groupe fini) *Soit $(G, *)$ un groupe fini de cardinal n. Soit $a \in G$. Alors a est d'ordre fini p et on a : $p|n$.*

Exemple 3.4.2 *$\mathbb{U}_n$ est le seul sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal n.*

3.5 Le groupe $\mathcal{S}_n$

Définition 3.5.1 (Groupe symétrique) *Le groupe symétrique, noté $\mathcal{S}_n$, est l'ensemble des permutations (bijections) de $[\![1, n]\!]$. $(\mathcal{S}_n, \circ)$ est un groupe de cardinal $n!$. Si $n \geq 3$, ce groupe est non commutatif.*

Notations :
Soit $\sigma \in \mathcal{S}_n$. On note $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Définition 3.5.2 (Transposition) *Une transposition de $\mathcal{S}_n$ est une permutation τ telle qu'il existe $i,\ j \in [\![1, n]\!]$ satisfaisant $i \neq j$, $\tau(i) = j$ et $\tau(j) = i$ et pour tout entier k différent de i, j, $\tau(k) = k$. On note $\tau = (i, j)$.*

Définition 3.5.3 (Cycle) *Soient $p \geq 2$ et $A = \{a_1, \ldots, a_p\} \subset [\![1, n]\!]$. Soit σ la permutation définie par : $\forall x \notin A,\ \sigma(x) = x$ et : $\forall i \in [\![1, p-1]\!],\ \sigma(a_i) = a_{i+1}$ et $\sigma(a_p) = a_1$. σ est appelé cycle de longueur p de support A. On note $\sigma = (a_1, \cdots, a_p)$.*

Proposition 3.5.1 (Décomposition d'une permutation en cycles) *Toute permutation se décompose comme un produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre des facteurs près. Par ailleurs les cycles de ce produit commutent entre eux.*

Proposition 3.5.2 (Partie génératrice de $\mathcal{S}_n$) *Les transpositions engendrent $\mathcal{S}_n$. Ainsi tout élément de $\mathcal{S}_n$ est un produit de transposition.*

Définition 3.5.4 (Signature) *Il existe un et un seul morphisme de groupes $\varepsilon : (\mathcal{S}_n, \circ) \to (\{1, -1\}, \times)$ tel que pour toute transposition τ, on ait : $\varepsilon(\tau) = -1$.*
On a donc : $\forall \sigma, \sigma' \in \mathcal{S}_n,\ \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.

Exemple 3.5.1 *Soit $\mathcal{A}_n$ l'ensemble des permutations de $\mathcal{S}_n$ de signature un. Alors $\mathcal{A}_n$ est un sous-groupe de $\mathcal{S}_n$ et de cardinal $n!/2$.*

4 Structures d'anneau, de corps

4.1 Révisions de sup sur les anneaux

Définition 4.1.1 (Structure d'anneau) *Soit A un ensemble muni de deux lois de composition interne notées $+$ et $\times$. On dit que $(A, +, \times)$ est un anneau lorsque :*

- *$(A, +)$ est un groupe commutatif; son neutre est noté 0_A (élément neutre additif).*
- *La loi $\times$ est associative.*
- *La loi $\times$ est distributive par rapport à la loi $+$ ($\forall x, y, z \in A,\ x \times (y + z) = x \times y + x \times z$ et $(x + y) \times z = x \times z + y \times z$).*
- *La loi $\times$ admet un élément neutre, noté 1_A et appelé élément unité de A.*

Si de plus la loi $\times$ est commutative on dit que $(A, +, \times)$ est un anneau commutatif.

Exemple 4.1.1
1. *$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{K}[X], +, \times)$ sont des anneaux commutatifs.*
2. *$\mathcal{M}_n(\mathbb{R})$ est un anneau , non commutatif si $n > 1$.*

4.2 Calculs dans un anneau et les éléments inversibles

Proposition 4.2.1 (Binôme de Newton) *Dans un anneau $(A, +, \times)$, lorsque deux éléments <u>a et b commutent</u> ($a \times b = b \times a$) on a la formule suivante :*

$$\forall n \in \mathbb{N}, \quad (a+b)^n \ = \ \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Proposition 4.2.2 (Formules de factorisation) *Soit $(A, +, \times)$ un anneau.*

1. *$\forall a, b \in A$, $\forall n \in \mathbb{N}$,*

$$1 - a^n \ = \ (1-a)\left(\sum_{k=0}^{n-1} a^k\right) \ = \ \left(\sum_{k=0}^{n-1} a^k\right)(1-a).$$

2. *$\forall (n, p) \in (\mathbb{N}^*)^2$, $\forall (a_1, \ldots, a_n) \in A^n$, $\forall (b_1, \ldots, b_p) \in A^p$,*

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{p} a_i b_j\right) \ = \ \sum_{j=1}^{p}\left(\sum_{i=1}^{n} a_i b_j\right) \ = \ \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{p} b_j\right).$$

3. *Si <u>$ab = ba$</u> alors :*

$$\forall n \in \mathbb{N}^*, \quad a^n - b^n \ = \ (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) \ = \ (a-b)\left(\sum_{k=0}^{n-1} a^k b^{n-k-1}\right).$$

Définition 4.2.1 (Élément inversible) *Soit $(A, +, \times)$ un anneau. Soit $x \in A$. On dit que x est inversible s'il existe y dans A tel que $x \times y = y \times x = 1_A$. Dans ce cas, on note $x^{-1} = y$ (et donc l'inverse de x est unique).*

Proposition 4.2.3 (L'ensemble des éléments inversibles d'un anneau) *Si A est un anneau alors, en notant $\mathcal{U}(A)$ l'ensemble de ses éléments inversibles, le couple $(\mathcal{U}(A), \times)$ est un groupe.*

4.3 Sous-anneau

Définition 4.3.1 (Sous-anneau) *On considère un anneau $(A, +, \times)$ et une sous-partie A' de A. On dit que la partie A' est un sous-anneau de A lorsque :*

1. *$(A', +)$ est un sous-groupe de $(A, +)$.*
2. *La partie A' est stable pour la loi $\times$: $\forall (a, b) \in A'^2$, $ab \in A'$.*
3. *L'élément unité de A est dans A' : $1_A \in A'$.*

A' hérite ainsi d'une structure d'anneau.

Exemple 4.3.1 *L'ensemble $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$ et ses inversibles sont 1, -1, i et $-i$.*

4.4 Produit d'anneaux

Définition 4.4.1 (Produit fini d'anneaux) *Soient $(A_1, +_1, \times_1)$,...,$(A_n, +_n, \times_n)$ n anneaux. Soit $+$ et $\times$ les lois de composition interne définies sur $A_1 \times ... \times A_n$ par :*
$\forall (x_1, y_1, ..., x_n, y_n,) \in A_1^2 \times ... \times A_n^2$,
$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 +_1 y_1, ..., x_n +_n y_n)$,
$(x_1, ..., x_n) \times (y_1, ..., y_n) = (x_1 \times_1 y_1, ..., x_n \times_n y_n)$.

$(A_1 \times ... \times A_n, +, \times)$ est un anneau et c'est l'anneau produit de $A_1, ..., A_n$.

4.5 Morphisme d'anneaux

Définition 4.5.1 (Morphisme d'anneaux) *Soit $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux.*

1. *Un morphisme d'anneaux est une application $f : A \to B$ respectant les structures d'anneaux, c'est-à-dire vérifiant :*

$$\forall (a, b) \in A^2, \quad f(a +_A b) = f(a) +_B f(b), \quad f(a \times_A b) = f(a) \times_B f(b) \quad \text{et } f(1_A) = 1_B.$$

2. *Un morphisme d'anneaux bijectif est appelé isomorphisme d'anneaux.*

Définition 4.5.2 (Noyau et image d'un morphisme d'anneaux) *Soit $f : A \to B$ un morphisme d'anneaux.*

1. *On appelle noyau de f, noté $\mathrm{Ker}\,(f)$, l'ensemble des antécédents par f de 0_B dans A :*

$$\mathrm{Ker}\,(f) = f^{-1}(\{0_B\}) = \{x \in A\,;\, f(x) = 0_B\}.$$

2. *On appelle image de f, noté $\mathrm{Im}\,(f)$, l'ensemble des images par f des éléments de A :*

$$\mathrm{Im}\,(f) = f(A) = \{y \in B\,;\, \exists x \in A,\, y = f(x)\}.$$

Proposition 4.5.1 (Caractérisation des morphismes injectifs/surjectifs) *Soit $f : A \to B$ un morphisme d'anneaux.*

1. *f est injective si et seulement si $\mathrm{Ker}\,(f) = \{0_A\}$.*
2. *f est surjective si et seulement si $\mathrm{Im}\,(f) = B$.*

Proposition 4.5.2 (Réciproque d'un isomorphisme d'anneaux) *La bijection réciproque d'un isomorphisme d'anneaux est elle-même un isomorphisme d'anneaux.*

4.6 Intégrité, corps

Définition 4.6.1 (Anneau intègre) *Soit $(A, +, \times)$ un anneau. Il est dit intègre lorsque :*

1. $A \neq \{0_A\}$.
2. $\times$ *est commutative.*
3. $\forall (a, b) \in A^2$, $ab = 0 \Longrightarrow [(a = 0) \quad ou \quad (b = 0)]$.
   Ceci équivaut à : si $a \neq 0$ *et* $b \neq 0$ *alors* $ab \neq 0$.

Exemple 4.6.1 $(\mathbb{Z}, +, \times)$ *et* $(\mathbb{K}[X], +, \times)$ *sont des anneaux intègres.*

Définition 4.6.2 (Structure de corps) *Un ensemble* $\mathbb{K}$ *muni de deux lois de composition interne* $+$ *et* $\times$ *est un corps lorsque :*

1. $(\mathbb{K}, +, \times)$ *est un anneau commutatif.*
2. $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$.
3. *Tout élément de* $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$ *admet un inverse pour* $\times$ *dans* $\mathbb{K}$.

Exemple 4.6.2
1. *Les ensembles* $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ *pour les lois* $+$ *et* $\times$ *usuelles sont des corps commutatifs.*
2. *Tout anneau intègre fini* A *est un corps.*

Définition 4.6.3 (Sous-corps) *Soit* $(\mathbb{K}, +, \times)$ *un corps et* $\mathbb{L}$ *une partie de* $\mathbb{K}$. *On dit que* $\mathbb{L}$ *est un sous-corps de* $\mathbb{K}$ *lorsque :*

1. $\mathbb{L}$ *est un sous-anneau de* $\mathbb{K}$.
2. $\forall x \in \mathbb{L} \setminus \{0_{\mathbb{K}}\}$, $x^{-1} \in \mathbb{L}$.

Autrement dit $\mathbb{L}$ *est un sous anneau de* $\mathbb{K}$ *qui a une structure de corps.*

Exemple 4.6.3 *L'ensemble* $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b\,;\, (a, b) \in \mathbb{Q}^2\}$ *est un sous-corps de* $\mathbb{R}$.

4.7 Idéal d'un anneau commutatif

4.7.1 Définition et premières propriétés

Définition 4.7.1 (Structure d'idéal) *On appelle idéal de* A *une partie* I *de* A *telle que :*

1. $(I, +)$ *est un sous-groupe de* $(A, +)$ *;*
2. I *est stable par la multiplication par un élément quelconque de* A *:* $\forall x \in I$, $\forall a \in A$, $ax \in I$.

Proposition 4.7.1 (Noyau d'un morphisme d'anneaux) *Soit* f *un morphisme d'anneaux de* A *dans* B *(*A *et* B *anneaux commutatifs). Alors* $\operatorname{Ker} f$ *est un idéal de* A.

Proposition 4.7.2 (Idéal engendré par un élément) *L'ensemble* $xA = \{xa\,;\, a \in A\}$ *des multiples d'un élément* x *de* A *est un idéal, appelé* ***idéal engendré*** *par* x.

Proposition 4.7.3 (Idéaux de $\mathbb{Z}$) *Les idéaux de l'anneau* $\mathbb{Z}$ *sont les* $n\mathbb{Z}$, *pour* $n \in \mathbb{N}$.

Proposition 4.7.4 *Pour* $a, b \in \mathbb{Z}^*$, *on a :* $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Proposition 4.7.5 (Idéaux de $\mathbb{K}[X]$) *Soit* $\mathbb{K}$ *un sous-corps de* $\mathbb{C}$.
Les idéaux de $\mathbb{K}[X]$ *sont de la forme* $B\mathbb{K}[X] = \{BQ,\ Q \in \mathbb{K}[X]\}$, *avec* B *dans* $\mathbb{K}[X]$.
Si on impose à B *d'être unitaire, alors* B *est unique (pour un idéal non nul).*

Proposition 4.7.6 *Pour* $A, B \in \mathbb{K}[X] \setminus \{0\}$, *on a :* $A\mathbb{K}[X] + B\mathbb{K}[X] = (A \wedge B)\mathbb{K}[X]$.

5 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

5.1 Définition

Proposition 5.1.1 (La congruence est une relation d'équivalence) *Soit $n \in \mathbb{N}$. On définit sur $\mathbb{Z}$ la relation binaire : $a\mathcal{R}_n b$ si $a \equiv b[n]$. Alors $\mathcal{R}_n$ est une relation d'équivalence.*

Définition 5.1.1 ($\mathbb{Z}/n\mathbb{Z}$) *On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation $\mathcal{R}_n$.*
Si on note $\overline{k}$, la classe d'équivalence de k, alors :
$\overline{k} = \{x \in \mathbb{Z},\ x \equiv k[n]\} = \{..., k-2n, k-n, k, k+n, k+2n, ...\} = \{k+np,\ p \in \mathbb{Z}\} = k + n\mathbb{Z}$.
Autrement dit : $\overline{a} = \overline{b} \Leftrightarrow a \equiv b[n]$.

Proposition 5.1.2 (Description de $\mathbb{Z}/n\mathbb{Z}$) *Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ possède n éléments et on a : $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.*

Proposition 5.1.3 (Opérations sur $\mathbb{Z}/n\mathbb{Z}$) *Sur $\mathbb{Z}/n\mathbb{Z}$, on pose les opérations :*

- $\forall x, y \in \mathbb{Z},\ \overline{x} + \overline{y} = \overline{x+y}$.
- $\forall x, y \in \mathbb{Z},\ \overline{x} \times \overline{y} = \overline{xy}$.

Les opérations $+$ et $\times$ sont bien définies sur $\mathbb{Z}/n\mathbb{Z}$, c'est à dire que $\overline{x} + \overline{y}$ et $\overline{x} \times \overline{y}$ ne dépendant pas du représentant choisi dans les classe $\overline{x}$ et $\overline{y}$.

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

Proposition 5.2.1 (Le groupe $\mathbb{Z}/n\mathbb{Z}$) *Soit $n \in \mathbb{Z}$, alors $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.*

Proposition 5.2.2 (Les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$) *Les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les classes $\overline{k}$ où k est un entier premier avec n.*
Autrement dit $\mathbb{Z}/n\mathbb{Z} = \{p\overline{k},\ p \in \mathbb{Z}\} = \{\overline{0}, \overline{k}, 2\overline{k}, ..., (n-1)\overline{k}\}$, si k est premier avec n.

Proposition 5.2.3 (Description des groupes monogènes finis) *Tout groupe monogène fini G (on dit cyclique) est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, avec $n \in \mathbb{N}^*$. Dans ce cas, G est de cardinal n et $G = \{e, g, g^2, ..., g^{n-1}\}$, pour un certain g dans G et n est le plus petit entier naturel k non nul tel que $g^k = e$.*

Exemple 5.2.1 *$(\mathbb{U}_n, \times)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

5.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

5.3.1 Structure d'anneau, corps

Proposition 5.3.1 (L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$) *L'ensemble $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.*

Proposition 5.3.2 (Le corps $\mathbb{Z}/n\mathbb{Z}$) *L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.*

Théorème 5.3.1 (Théorème chinois) *Soit $(m, n) \in \mathbb{N}^2$. Si m et n sont premiers entre eux, alors les anneaux $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/(mn)\mathbb{Z}$ sont isomorphes, via l'application*

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/(mn)\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{k} & \mapsto & (\tilde{k}, \hat{k}) \end{array} \right. ,$$

avec pour k dans $\mathbb{Z}$, $\tilde{k}$ et $\hat{k}$ les classes de k dans respectivement $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.

Corollaire 5.3.1 *Soit $(m, n) \in \mathbb{N}^2$. Si m et n sont premiers entre eux, alors pour tout $(a, b) \in \mathbb{Z}^2$, il existe un entier k_0 vérifiant le système*

$$(S) : \left\{ \begin{array}{l} k_0 \equiv a[m] \\ k_0 \equiv b[n] \end{array} \right.$$

et les solutions de ce système sont exactement $\{k_0 + pmn,\ p \in \mathbb{Z}\}$, c'est-à-dire l'ensemble des entiers congrus à k_0 modulo mn.

Proposition 5.3.3 (Éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$) *L'élément $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ pour $\times$ si et seulement si k est premier avec n.*

5.3.2 Indicatrice d'Euler

Définition 5.3.1 (Fonction indicatrice d'Euler) *On appelle fonction indicatrice d'Euler la fonction* $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *qui à* n *associe le nombre* $\varphi(n)$ *d'entiers de l'intervalle* $[\![1, n]\!]$ *premiers avec* n*. Autrement dit, pour* $n \in \mathbb{N}^*$*, on a :* $\varphi(n) = \{k \in [\![1, n]\!],\ k \wedge n = 1\}$*.*

Remarque 5.3.1 $card(\mathcal{U}(\mathbb{Z}/n\mathbb{Z})) = \varphi(n)$*.*

Corollaire 5.3.2 (Un théorème d'Euler) *Soit* k *un entier premier avec* n*, on a dans* $\mathbb{Z}/n\mathbb{Z}$ *:* $\overline{k}^{\varphi(n)} = \overline{1}$*. Autrement dit* $k^{\varphi(n)} \equiv 1[n]$

Remarque 5.3.2 *On retrouve le petit théorème de Fermat. Soit* p *est un nombre premier, alors :* $\forall k \in \mathbb{Z},\ k^p \equiv k[p]$*.*

Proposition 5.3.4 (Calcul de $\varphi(n)$**)**

1. *Soient* $mn, \in \mathbb{N}^*$ *tels que* $m \wedge n = 1$*. Alors :* $\varphi(mn) = \varphi(m)\varphi(n)$*.*
2. *Soit un entier* $n \geq 2$*. Si la décomposition en facteurs premiers de* n *s'écrit* $n = p_1^{k_1} p_2^{k_2} \cdots p_q^{k_q}$*, alors :*

$$\varphi(n) \ = \ p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1)\cdots p_q^{k_q-1}(p_k - 1) = n\left(1 - \frac{1}{p_1}\right)...\left(1 - \frac{1}{p_q}\right).$$