

1 Arithmétique dans $\mathbb{Z}$

1.1 Révision de sup sur la division euclidienne et les congruences

Théorème 1.1.1 (Division euclidienne) 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 .

Définition 1.1.1 (Congruences) Soit $n \in \mathbb{Z}$. Deux entiers relatifs a et b sont congrus modulo n , noté $a \equiv b[n]$, s'il existe un entier k tel que $a = b + kn$.

Autrement dit, $a \equiv b[n]$ si et seulement si : $a - b \in n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$.

Proposition 1.1.1 (Congruence et opérations) Soient $a, a', b, b' \in \mathbb{Z}$ et $m, n \in \mathbb{N}^*$.

1. Si $a \equiv b[n]$ et $a' \equiv b'[n]$, alors $a + a' \equiv b + b'[n]$.
2. Si $a \equiv b[n]$ et $a' \equiv b'[n]$, alors $aa' \equiv bb'[n]$.
3. Si $a \equiv b[n]$ et $m \in \mathbb{Z}$, alors $am \equiv bm[nm]$.

Exemple 1.1.1 Déterminer le chiffre des unités de 13^{65363} .

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

Soit $n \in \mathbb{N}$.

Proposition 1.2.1 (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.

Démonstration :

- Elle est réflexive : $\forall a \in \mathbb{Z}, a = a + 0 \times n$, donc $a \equiv a[n]$.
- Elle est symétrique, car si $a \equiv b[n]$, alors il existe $k \in \mathbb{Z}$ tel que $a = b + kn$, donc : $b = a + (-k)n$, puis $b \equiv a[n]$.
- Elle est transitive, car si $a \equiv b[n]$ et $b \equiv c[n]$, alors il existe $k, k' \in \mathbb{Z}$ tels que $a = b + kn$ et $b = c + k'n$. Ainsi $a = c + (k + k')n$ et donc ; $a \equiv c[n]$.

Définition 1.2.1 ($\mathbb{Z}/n\mathbb{Z}$) On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation $\mathcal{R}_n$.

Si on note $\bar{k}$, la classe d'équivalence de k , alors :

$$\bar{k} = \{x \in \mathbb{Z}, x \equiv k[n]\} = \{\dots, k - 2n, k - n, k, k + n, k + 2n, \dots\} = \{k + np, p \in \mathbb{Z}\} = k + n\mathbb{Z}.$$

Autrement dit : $\bar{a} = \bar{b} \Leftrightarrow a \equiv b[n]$.

Exemple 1.2.1 Les classes d'équivalence de 0 et n sont tous les multiples de n à savoir $n\mathbb{Z}$.

Proposition 1.2.2 (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 : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.

Démonstration : Soit $x \in \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ un représentant de x , c'est-à-dire : $x = \overline{k}$. La division euclidienne de k par n s'écrit $k = nq + r$, avec q dans $\mathbb{Z}$ et r dans $\llbracket 0, n-1 \rrbracket$. On a donc $k \equiv r[n]$, donc k et r sont dans la même classe d'équivalence, puis : $x = \overline{r} \in \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Ainsi on a : $\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. L'autre inclusion est immédiate, d'où $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

Cet ensemble comporte bien n éléments car si on considère $a, b \in \llbracket 0, n-1 \rrbracket$ tels que $\overline{a} = \overline{b}$, alors il existe $k \in \mathbb{Z}$ tel que $a = b + kn$, soit $a - b = kn$. Or $a - b$ est dans $\llbracket -(n-1), n-1 \rrbracket$, donc $|k|n = |a - b| < n$. Comme n est non nul, alors : $|k| < 1$ et comme $|k|$ est un entier naturel, alors $|k| = 0$, puis $k = 0$, puis $a = b$. Ainsi les éléments $\overline{0}, \overline{1}, \dots, \overline{n-1}$ sont bien deux à deux distincts.

Remarque 1.2.1 1. Soit $a \in \mathbb{Z}$. On a : $n|a$ si et seulement si $\overline{a} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$.

2. Parfois, pour des raisons de symétrie, il peut être intéressant de considérer des représentants négatifs, par exemple : $\mathbb{Z}/(2m+1)\mathbb{Z} = \{\overline{-m}, \overline{-(m-1)}, \dots, \overline{-1}, \overline{0}, \overline{1}, \dots, \overline{m-1}, \overline{m}\}$.

Proposition 1.2.3 (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 dépendent pas du représentant choisi dans les classes $\overline{x}$ et $\overline{y}$.

Démonstration : Soient $x, y, x', y' \in \mathbb{Z}$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$. Il faut montrer que $\overline{x} + \overline{y} = \overline{x'} + \overline{y'}$ et $\overline{x} \times \overline{y} = \overline{x'} \times \overline{y'}$, soit : $\overline{x+y} = \overline{x'+y'}$ et $\overline{xy} = \overline{x'y'}$.

On a $x \equiv x'[n]$ et $y \equiv y'[n]$ et donc grâce à la proposition 1.1.1, on a : $x+y \equiv x'+y'[n]$ et $xy \equiv x'y'[n]$, d'où $\overline{x+y} = \overline{x'+y'}$ et $\overline{xy} = \overline{x'y'}$.

Exemple 1.2.2 1. Dans $\mathbb{Z}/7\mathbb{Z}$, montrer que $\overline{x}^2 + \overline{y}^2 = \overline{0}$ implique que $\overline{x} = \overline{y} = \overline{0}$.

2. Soit p un nombre premier supérieur ou égal à 5. Calculer dans $\mathbb{Z}/p\mathbb{Z}$: $\sum_{k=1}^p \overline{k}^2$.

1.3 Révisions de sup sur les nombres premiers

Définition 1.3.1 (Nombres premiers) Un entier relatif n non nul est dit **premier** lorsqu'il admet exactement quatre diviseurs, c'est-à-dire 1, -1 , n et $-n$.

Remarque 1.3.1 1. 0 et 1 ne sont pas premiers.

2. Tout entier $n \geq 2$ non premier admet au moins un diviseur premier p tel que $p^2 \leq n$ (soit $p \leq \sqrt{n}$). Par contraposée de la proposition précédente, si un nombre n n'admet pas de diviseurs premiers inférieur ou égal à $\sqrt{n}$, alors il est premier.

Proposition 1.3.1 (Infinité de l'ensemble des nombres premiers) *L'ensemble des nombres premiers est infini. On notera $\mathcal{P}$ l'ensemble des nombre premiers.*

Définition 1.3.2 (Valuation p -adique) *Soient $a \in \mathbb{Z}^*$ 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 1.3.1 (Décomposition en facteurs premiers) *Tout entier $n \geq 2$ admet une décomposition en facteurs premiers, c'est-à-dire qu'il existe $p_1, p_2, \dots, p_k$ des entiers premiers deux à deux distincts et $(\alpha_1, \alpha_2, \dots, \alpha_k) \in (\mathbb{N}^*)^k$ tels que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = \prod_{l=1}^k p_l^{\alpha_l}$.*

Autrement dit : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ et cette décomposition est unique. La décomposition est unique à l'ordre près des facteurs.

Exemple 1.3.1 1. Il y a une infinité de nombres premiers de la forme $4k - 1$, avec $k \in \mathbb{N}^*$.

Les nombres premiers impairs sont congrus à 1 ou -1 modulo 4.

Supposons qu'il n'y a qu'un nombre fini de tels nombres premiers : $3 = p_1 < \dots < p_r$. Soit $P = \prod_{i=1}^r p_i$.

Comme $P \equiv (-1)^r [4]$.

Si $P \equiv 1[4]$, comme $P + 2 \equiv -1[4]$, alors $P + 2$, qui est impair, possède au moins un diviseur premier q différent de 2 et tel que $q \equiv -1[4]$, sinon on aurait $P + 2 \equiv 1[4]$. Or $q|P$ donc $q|2$, car $P + 2 - P = 2$, ce qui est impossible.

On a donc $P \equiv -1[4]$. Le même raisonnement appliqué à $N + 4$ nous fournit un diviseur premier q tel que $q \equiv -1[4]$ tel que $q|4$, ce qui est aussi impossible.

On a donc une nombre infini de nombres premiers de la forme $4k - 1$, avec $k \in \mathbb{N}^$.*

2. Soit a un entier tel que : $a \geq 2$. On suppose qu'il existe $m \in \mathbb{N}^*$ tel que $a^m + 1$ soit un nombre premier. Montrer que a est pair et que m est une puissance de 2.

Proposition 1.3.2 (Critère de divisibilité à l'aide de la valuation) *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ et $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $p_1, p_2, \dots, p_k$ des entiers premiers deux à deux distincts. Alors $n|m$ si et seulement si $\forall l \in \llbracket 1, k \rrbracket$, $\alpha_l \leq \beta_l$. Autrement dit : $\forall p \in \mathcal{P}$, $v_p(n) \leq v_p(m)$.*

Remarque 1.3.2 *Avec les notations précédentes, le nombre de diviseurs de n vaut donc : $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$, car un diviseur de n n'a que les p_l dans sa décomposition en facteurs premiers et la puissance associée est comprise entre 0 et α_l .*

Exemple 1.3.2 Soit q un nombre premier. Montrer que : $v_q(m!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{m}{q^i} \right\rfloor$.

1.4 Révisions de sup sur le PGCD, le PPCM et applications

1.4.1 PGCD

Définition 1.4.1 (Diviseurs communs) Soit $(a, b) \in (\mathbb{N}^*)^2$. Tout entier non nul d vérifiant $d|a$ et $d|b$ est appelé diviseur commun de a et b . On note $\text{Div}(a, b)$ l'ensemble des diviseurs communs dans $\mathbb{N}^*$ de a et b .

Définition 1.4.2 (PGCD) Soit $(a, b) \in (\mathbb{N}^*)^2$. Le plus grand élément de $\text{Div}(a, b)$ est appelé pgcd de a et b . On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.

Remarque 1.4.1 1. Nous verrons dans la proposition 4.7.6 une autre définition du PGCD.

2. On a $a|b \Leftrightarrow a \wedge b = a$.

Proposition 1.4.1 (Expression du PGCD avec les valuations) Soient $p_1, p_2, \dots, p_k$ des entiers premiers deux à deux distincts et $(\alpha_1, \alpha_2, \dots, \alpha_k) \in \mathbb{N}^k$ et $(\beta_1, \beta_2, \dots, \beta_k) \in \mathbb{N}^k$ tels que $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ et

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}. \text{ Alors } a \wedge b = \prod_{l=1}^k p_l^{\min(\alpha_l, \beta_l)}.$$

Autrement dit $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$.

Proposition 1.4.2 (Lien entre les diviseurs du PGCD et les diviseurs d'un couple) Soient $a, b \in \mathbb{Z}$. On a : $\text{Div}(a) \cap \text{Div}(b) = \text{Div}(a \wedge b)$.

Définition 1.4.3 (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 signifie que les seuls diviseurs communs de a et b sont 1 et -1 .

Remarque 1.4.2 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 1.4.3 (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 $r_0, r_1, r_2, r_3, \dots$ 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 $r_0, r_1, r_2, r_3, \dots$ 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 : $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \dots = r_k \wedge r_{k-1} = \dots r_{k_0} \wedge r_{k_0-1} = r_{k_0}$. Ainsi le pgcd de a et b est le dernier reste non nul de la succession de divisions euclidiennes que l'on a effectuées.

Exemple 1.4.1 Soit $n \in \mathbb{N}$ et on pose $F_n = 2^{2^n} + 1$. Montrer que pour n, m dans $\mathbb{N}^*$ distincts on a : $F_n \wedge F_m = 1$.

Définition 1.4.4 (PGCD d'une famille d'entiers) L'entier $a_1 \wedge \dots \wedge a_n$ est le plus grand commun diviseur des entiers $a_1, \dots, a_n$, soit $\max(\text{Div}(a_1) \cap \dots \cap \text{Div}(a_n))$.

Exemple 1.4.2 $28 \wedge 42 \wedge 98 = 14$, car $28 = 14 \times 2$, $42 = 14 \times 3$ et $98 = 14 \times 7$.

Définition 1.4.5 (Entiers premiers entre eux dans leur ensemble) Si le pgcd de $a_1, \dots, a_n$ vaut 1, alors ces entiers sont premiers entre eux dans leur ensemble.

1.4.2 Applications du PGCD

Proposition 1.4.4 (Relation de Bézout) Soient $a, b \in \mathbb{Z}^*$ et on pose $d = a \wedge b$. Il existe deux entiers u, v tels que $d = au + bv$. De plus, $\{am + bn, (m, n) \in \mathbb{Z}^2\} = d\mathbb{Z}$.

Exemple 1.4.3 Soient $n, m \in \mathbb{N}^*$. Déterminer $\mathbb{U}_n \cap \mathbb{U}_m$, avec $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$.

Théorème 1.4.1 (Bézout) Soient $a, b \in \mathbb{Z}^*$. On a : $a \wedge b = 1$ si et seulement s'il existe $m, n \in \mathbb{Z}$ tels que $1 = ma + nb$.

Remarque 1.4.3 Pour trouver u et v dans les cas simples, on peut remonter à la main les calculs faits dans l'algorithme d'Euclide.

Proposition 1.4.5 (Nombre premier entre eux et divisibilité) 1. Soient

$a, b, p \in \mathbb{Z}$. Si $a \wedge p = 1$ et $b \wedge p = 1$, alors $(ab) \wedge p = 1$.

2. Soit a et b deux entiers naturels premiers entre eux. Soit $c \in \mathbb{N}$. On a : $(a|c \text{ et } b|c) \Leftrightarrow ab|c$.

Exemple 1.4.4 Résoudre : $\begin{cases} x \equiv 6[17] \\ x \equiv 4[15] \end{cases}$, dans lequel l'inconnue x appartient à $\mathbb{Z}$.

Cherchons d'abord une solution particulière.

Soit $x \in \mathbb{Z}$. x est solution de (S) si et seulement s'il existe $(k, k') \in \mathbb{Z}^2$ tels que $\begin{cases} x = 6 + 17k \\ x = 4 + 15k' \end{cases}$ si et seulement s'il existe $(k, k') \in \mathbb{Z}^2$ tels que $\begin{cases} x = 6 + 17k \\ 6 + 17k = 4 + 15k' \end{cases}$

Or : $6 + 17k = 4 + 15k' \Leftrightarrow 15k' - 17k = 2$. Pour déterminer une solution particulière x_0 de (S), il suffit de trouver une solution particulière (k_0, k'_0) de $15k' - 17k = 2$.

Nous allons donc d'abord chercher une solution de $15u + 17v = 1$ (cela est possible, car 15 et 17 sont premiers entre eux). Nous allons appliquer l'algorithme d'Euclide.

On a : $17 = 15 \times 1 + 2$, puis $15 = 7 \times 2 + 1$.

Alors $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15 \times 1) = 15 - 17 \times 7 + 15 \times 7 = 15 \times 8 - 17 \times 7$.

En multipliant cette relation par 2, on trouve : $16 \times 15 - 14 \times 17 = 2$ et donc $k'_0 = 16$ et $k_0 = 14$ conviennent.

Ainsi $x_0 = 6 + 17 \times k_0 = 6 + 17 \times 14 = 244$ est une solution particulière de (S).

On a donc : $\begin{cases} x_0 \equiv 6[17] \\ x_0 \equiv 4[15] \end{cases}$.

On en déduit que x est solution de (S) si et seulement si $\begin{cases} x \equiv x_0[17] \\ x \equiv x_0[15] \end{cases}$, si et seulement si : $\begin{cases} x - x_0 \equiv 0[17] \\ x - x_0 \equiv 0[15] \end{cases}$, si et seulement si : $17|(x - x_0)$, $15|(x - x_0)$. Or 17 et 15 sont premiers entre eux, donc le deuxième point de la proposition précédente nous permet d'affirmer que x est solution de (S) si et seulement si : $17 \times 15|(x - x_0)$ Donc l'ensemble des solutions de (S) est $\{x_0 + 17 \times 15k, k \in \mathbb{Z}\} = \{-11 + 255k, k \in \mathbb{Z}\}$.

Proposition 1.4.6 (Relation de Bézout pour une famille d'entiers) Si d est le pgcd de $a_1, \dots, a_n$, alors il existe des entiers relatifs $u_1, \dots, u_n$ tels que $a_1u_1 + \dots + a_nu_n = d$.

Théorème 1.4.2 (Bézout pour une famille d'entiers) $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si et seulement s'il existe des entiers relatifs $u_1, \dots, u_n$ tels que $a_1u_1 + \dots + a_nu_n = 1$.

Théorème 1.4.3 (Gauss) Soient $a, b, c \in \mathbb{Z}^*$. Si $a|bc$ et $a \wedge c = 1$, alors $a|b$.

Exemple 1.4.5 1. Soient p un nombre premier et $k \in \llbracket 1, p-1 \rrbracket$. Montrer que p divise $\binom{p}{k}$.

2. Trouver tous les couples $(u, v) \in \mathbb{Z}^2$ tels que : $15u + 17v = 6$.

Nous allons donc d'abord chercher une solution de $15u + 17v = 1$ (cela est possible, car 15 et 17 sont premiers entre eux). Nous allons appliquer l'algorithme d'Euclide.

On a : $17 = 15 \times 1 + 2$, puis $15 = 7 \times 2 + 1$.

Alors $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15 \times 1) = 15 - 17 \times 7 + 15 \times 7 = 15 \times 8 - 17 \times 7$.

En multipliant par 6 :

$15u_0 + 17v_0 = 6$, avec $u_0 = 48$ et $v_0 = -42$.

Si $(u, v) \in \mathbb{Z}^2$ vérifie : $15u + 17v = 6$, alors : $15u + 17v = 15u_0 + 17v_0$, , puis :

$15(u - u_0) = 17(v_0 - v)$. Comme 15 et 17 sont premiers entre eux, le lemme de Gauss permet d'affirmer que : $15|v_0 - v$ et $17|u - u_0$, donc il existe k, k' dans $\mathbb{Z}$ tels que : $v_0 - v = 15k$ et $u - u_0 = 17k'$, soit : $v = v_0 - 15k$ et $u = 17k' + u_0$. En injectant cela dans $15(u - u_0) = 17(v_0 - v)$, on trouve que $k = k'$.

Réciproquement, soit $k \in \mathbb{Z}$ et on pose $v = v_0 - 15k$ et $u = 17k + u_0$. Alors on a :

$15u + 17v = 15 \times 17k + 15u_0 + 17v_0 - 17 \times 15k = 15u_0 + 17v_0 = 6$. Ainsi (u, v) est solution.

L'ensemble cherché est donc $\{(17k + 48, -42 - 15k), k \in \mathbb{Z}\}$.

1.4.3 PPCM

Définition 1.4.6 (Multiples communs) Soit $(a, b) \in \mathbb{Z}^2$. Tout entier non nul m vérifiant $a|m$ et $b|m$ est appelé multiple commun de a et b . On note $Mul(a, b)$ l'ensemble des multiples communs dans $\mathbb{N}^*$ de a et b non nuls.

Définition 1.4.7 Soit $(a, b) \in (\mathbb{N}^*)^2$. Le plus petit élément de $Mul(a, b)$ est appelé ppcm de a et b . On le note $ppcm(a, b)$ ou $a \vee b$.

Remarque 1.4.4 On a : $a|b$ si et seulement si $a \vee b = b$.

Proposition 1.4.7 (Expression du PPCM avec les valuations) Soient $p_1, p_2, \dots, p_k$ des entiers premiers deux à deux distincts et $(\alpha_1, \alpha_2, \dots, \alpha_k) \in \mathbb{N}^k$ et $(\beta_1, \beta_2, \dots, \beta_k) \in \mathbb{N}^k$ tels que $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$. Alors $a \vee b = \prod_{l=1}^k p_l^{\max(\alpha_l, \beta_l)}$.
Autrement dit $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$.

Remarque 1.4.5 Soit $(a, b) \in (\mathbb{N}^*)^2$. Alors $(a \wedge b)(a \vee b) = ab$.

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

Dans ce paragraphe, $\mathbb{K}$ désigne un corps inclus dans $\mathbb{C}$ (on verra plus tard que l'on appelle cela sous-corps de $\mathbb{C}$). On suppose acquise la construction de $\mathbb{K}[X]$ qui se fait de la même manière que $\mathbb{C}[X]$ ou $\mathbb{R}[X]$.

Les notions de degré, de coefficients dominants ainsi que les opérations $+$, $\times$ et $\circ$ se définissent aussi de la même façon.

Cela fait de $(\mathbb{K}[X], +, \times)$ un anneau commutatif.

On le suppose intègre (on verra plus tard cette notion) :

$\forall P, Q \in \mathbb{K}[X], PQ = 0 \Rightarrow (P = 0) \text{ ou } (Q = 0)$.

On rappelle qu'un polynôme unitaire est un polynôme de coefficient dominant un.

2.1 Divisibilité et division euclidienne

Proposition 2.1.1 (Polynômes associés) Soient $P, Q \in \mathbb{K}[X]$. On a $(P|Q \text{ et } Q|P)$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$. Dans ce cas, on dit que P et Q sont associés.

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

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

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

2.2 PGCD, PPCM

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

- On note $Div(A)$ l'ensemble des diviseurs de A .
- On note $Mul(A)$ l'ensemble des multiples de A .

Proposition 2.2.1 (Existence du 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 si $D \neq 0$, alors D est le polynôme unitaire de plus haut degré de $Div(A) \cap Div(B)$.

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

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

Démonstration : Calquer la démonstration de sup sur $\mathbb{R}$ ou $\mathbb{C}$. Nous verrons une autre preuve à la fin du cours dans le paragraphe sur les idéaux.

Définition 2.2.1 (PGCD et PPCM) On reprend les notations de la proposition précédente :

1. Le polynôme D est le **plus grand commun diviseur** de A et B , noté $A \wedge B$.

2. 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 2.2.2 (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 $AU + BV = D$.

Démonstration : Calquer la démonstration de sup sur $\mathbb{R}$ ou $\mathbb{C}$. Nous verrons à la fin du cours sur les idéaux une autre preuve.

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

Démonstration : Transposer la démonstration vue sur $\mathbb{Z}$.

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

Exemple 2.2.1 1. Soient $m, n \in \mathbb{N}^*$, avec $m < n$. Déterminer $(X^n - 1) \wedge (X^m - 1)$.

2. Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Soient $A, B \in \mathbb{K}[X]$. Montrer que le PGCD de A et B dans $\mathbb{K}[X]$ et $\mathbb{C}[X]$ sont les mêmes.

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 $\phi : \begin{cases} \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X] & \rightarrow \mathbb{C}_{m+n-1}[X] \\ (U, V) & \mapsto UF + VG \end{cases}$. Donner une condition nécessaire et suffisante pour que ϕ est un isomorphisme d'espaces vectoriels.

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

Proposition 2.2.3 (Relation de Bézout) Soient n un entier supérieur ou égal à 2, $A_1, \dots, A_n$ une famille de n polynômes et D leur PGCD. Il existe des polynômes $U_1, \dots, U_n$ tels que

$$A_1 U_1 + \dots + A_n U_n = D.$$

Démonstration : Voir démonstration faite en sup.

Définition 2.2.4 (Premiers entre eux dans leur ensemble) Soient n un entier supérieur ou égal à 2, $A_1, \dots, A_n$ 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, $A_1, \dots, A_n$ une famille de n polynômes. Les propositions suivantes sont équivalentes.

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

Démonstration : Voir démonstration faite en sup.

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 $\mathbb{K}^*$).

Lemme 2.3.1 Tout polynôme non constant admet au moins un diviseur irréductible.

Démonstration : Soit P un polynôme non constant. L'ensemble des degrés des diviseurs non constants de P est une partie non vide de $\mathbb{N}^*$ (il contient $d^\circ(P)$, car P divise P), qui possède donc un plus petit élément n_0 . Soit D_0 un diviseur de P de degré n_0 , prouvons que D_0 est irréductible.

Un diviseur de D_0 non constant et non associé à D_0 serait un diviseur de P de degré strictement inférieur à n_0 , ce qui contredit la définition de n_0 . Par conséquent D_0 est irréductible.

Théorème 2.3.1 (Décomposition d'un polynôme comme produit d'irréductibles) *Tout polynôme non constant se décompose comme produit de facteurs irréductibles. La décomposition est unique, sauf à changer un facteur en un facteur associé ou à modifier l'ordre des facteurs.*

On peut affirmer de façon équivalente que tout polynôme non constant A se décompose de façon unique comme le produit d'un scalaire par un produit de polynômes unitaires irréductibles :

$$A = \lambda P_1^{n_1} \dots P_k^{n_k},$$

avec $\lambda \in \mathbb{K}^*$, $P_1, \dots, P_k$ des polynômes unitaires irréductibles deux à deux non associés et $n_1, \dots, n_k$ dans $\mathbb{N}^*$. Ici λ est le coefficient dominant de A .

Démonstration :

1. **Existence.** Effectuons une récurrence forte sur le degré. L'initialisation est triviale : un polynôme de degré 1 est irréductible.

Supposons que tout polynôme de degré inférieur à n non constant se décompose comme produit de facteurs irréductibles. Soit P un polynôme non constant de degré $n + 1$.

- Si P est irréductible, alors il est produit d'un seul facteur irréductible.
- Supposons P non irréductible. Il existe deux polynômes Q et R non constants tels que $P = QR$. Étant non constants et diviseurs de P , ils sont de fait de degré inférieur ou égaux à n . En appliquant l'hypothèse de récurrence à Q et à R , on obtient leur décomposition en produit de facteurs irréductibles. Il s'ensuit que $P = QR$ est lui-même produit de facteurs irréductibles.

Ceci achève la récurrence.

2. **Unicité.** Supposons que P admette deux décompositions

$$P = \lambda \prod_{i=1}^r Q_i = \mu \prod_{j=1}^s R_j,$$

où les Q_i et R_j sont irréductibles (les Q_i et les P_j peuvent être répétés dans la décomposition). Tout d'abord, les Q_i et R_j étant unitaires, il est immédiat que $\lambda = \mu$ (c'est le coefficient dominant de P). Sans nuire à la généralité, on peut supposer $r \leq s$.

Supposons maintenant que Q_1 ne divise aucun des R_j . Ce Q_1 étant irréductible, ceci implique qu'il est premier avec tous les R_j .

Montrons par récurrence que Q_1 est premier avec tous les $\prod_{k=1}^j R_k$, pour j dans $\llbracket 1, s \rrbracket$.

Pour $j = 1$, c'est clair.

Soit $j \in \llbracket 1, s - 1 \rrbracket$ et on suppose Q_1 premier avec $\prod_{k=1}^j R_k$. Comme Q_1 est premier avec R_{j+1} ,

alors on a les deux relations de Bézout suivantes : $Q_1 U + \prod_{k=1}^j R_k V = 1$ et $Q_1 T + R_{j+1} W = 1$,

avec $T, U, V, W \in \mathbb{K}[X]$. En multipliant ces deux relations, on a :

$$Q_1(Q_1 UT + U R_{j+1} W + T \prod_{k=1}^j R_k V) + \prod_{k=1}^{j+1} R_k VW = 1. \text{ Donc } Q_1 \text{ premier avec } \prod_{k=1}^{j+1} R_k, \text{ ce qui achève}$$

la récurrence.

Ainsi pour $j = s$, Q_1 est premier avec le produit $\prod_{k=1}^s R_k$, à savoir P : absurde.

Par conséquent Q_1 divise un des R_j . Quitte à renuméroter les R_j , on peut supposer que $Q_1 | R_1$. Or R_1 est irréductible et Q_1 n'est pas constant, donc $Q_1 = R_1$ (leurs deux coefficients dominants valent un). Ceci permet d'obtenir

$$\prod_{i=2}^r Q_i = \prod_{j=2}^s R_j.$$

On effectue ensuite une récurrence finie sur le nombre r de facteurs de la première décomposition, afin d'obtenir après simplification par $Q_2, \dots, Q_r$:

$$1 = \prod_{j=r+1}^s R_j.$$

Cette égalité n'est possible que pour $r = s$. On a finalement obtenu que les Q_i et R_j sont égaux, à renumérotation près. L'unicité de la décomposition est finalement établie.

Remarque 2.3.1 Soient $A, B \in \mathbb{K}[X]$, non nuls. On suppose que $A = \lambda P_1^{n_1} \dots P_k^{n_k}$ et $B = \mu P_1^{m_1} \dots P_k^{m_k}$, avec $n_1, \dots, n_k, m_1, \dots, m_k$ dans $\mathbb{N}$ et $P_1, \dots, P_k$ des polynômes unitaires irréductibles deux à deux non associés. Alors :

- $B|A \Leftrightarrow \forall i \in \llbracket 1, k \rrbracket, m_i \leq n_i$.
- $A \wedge B = P_1^{\min(n_1, m_1)} \dots P_k^{\min(n_k, m_k)}$.
- $A \vee B = P_1^{\max(n_1, m_1)} \dots P_k^{\max(n_k, m_k)}$.

Nous rappelons comment les résultats précédents s'adaptent sur $\mathbb{R}$ ou $\mathbb{C}$:

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 $\lambda \prod_{i=1}^r (X - \alpha_i)^{k_i} \prod_{i=1}^s (X^2 + b_i X + c_i)^{l_i}$, où $\alpha_1, \dots, \alpha_r$ dans $\mathbb{R}$ deux à deux distincts, les polynômes réels $X^2 + b_i X + c_i$ sont deux à deux distincts et à discriminant strictement négatif et les k_i et l_i sont des entiers naturels non nuls.

Remarque 2.3.2 Soit $\alpha \in \mathbb{C}$. On a : $(X - \alpha)(X - \bar{\alpha}) = X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2$ qui est un polynôme réel. Ainsi une méthode pour factoriser un polynôme réel consiste à le factoriser dans $\mathbb{C}[X]$ et de regrouper les termes conjugués.

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

2. Le polynôme $4X^8 + 4$ est-il irréductible dans $\mathbb{R}[X]$? S'il ne l'est pas décomposez-le dans $\mathbb{R}[X]$ par deux méthodes.

Les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont de degré un ou deux, donc $4X^8 + 4$ n'est pas irréductible dans $\mathbb{R}[X]$.

Première méthode :

On a : $4X^8 + 4 = 4(X^8 + 1) = 4((X^4 + 1)^2 - 2X^4) = 4((X^4 + 1)^2 - (\sqrt{2}X^2)^2) = 4(X^4 + 1 - \sqrt{2}X^2)(X^4 + 1 + \sqrt{2}X^2) = 4((X^2 + 1)^2 - (\sqrt{2} + 2)X^2)((X^2 + 1)^2 - (2 - \sqrt{2})X^2) = 4(X^2 + 1 - \sqrt{2 + \sqrt{2}}X)(X^2 + 1 + \sqrt{2 + \sqrt{2}}X)(X^2 + 1 - \sqrt{2 - \sqrt{2}}X)(X^2 + 1 + \sqrt{2 - \sqrt{2}}X)$. Ces quatre polynômes sont irréductibles dans $\mathbb{R}[X]$, car il sont de degré deux sans racines réelles (s'ils avaient une racine réelle, alors $4X^8 + 4$ en aurait aussi, ce qui est impossible, car : $\forall x \in \mathbb{R}, 4x^8 + 4 > 0$). On a donc la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$.

Deuxième méthode :

Cherchons les racines $z \in \mathbb{C}$ de $4X^8 + 4$. On a :

$$4z^8 + 4 = 0 \Leftrightarrow z^8 = -1 = e^{i\pi} = \left(e^{\frac{i\pi}{8}}\right)^8 \Leftrightarrow (z/e^{\frac{i\pi}{8}})^8 = 1 \Leftrightarrow \exists k \in \llbracket -4, 3 \rrbracket, z/e^{\frac{i\pi}{8}} = e^{\frac{2ik\pi}{8}} \Leftrightarrow \exists k \in \llbracket -4, 3 \rrbracket, z = e^{\frac{(2k+1)i\pi}{8}}. \text{ Ainsi :}$$

$$4X^8 + 4 = 4(X - e^{-\frac{7i\pi}{8}})(X - e^{-\frac{5i\pi}{8}})(X - e^{-\frac{3i\pi}{8}})(X - e^{-\frac{i\pi}{8}})(X - e^{\frac{i\pi}{8}})(X - e^{\frac{3i\pi}{8}})(X - e^{\frac{5i\pi}{8}})(X - e^{\frac{7i\pi}{8}}) = 4 \prod_{k=0}^3 (X - e^{\frac{(2k+1)i\pi}{8}})(X - e^{-\frac{(2k+1)i\pi}{8}}),$$

qui est la décomposition dans $\mathbb{C}[X]$.

Dans $\mathbb{R}[X]$, la remarque précédente nous dit que :

$$(X - e^{\frac{(2k+1)i\pi}{8}})(X - e^{-\frac{(2k+1)i\pi}{8}}) = X^2 - 2\operatorname{Re}(e^{\frac{(2k+1)i\pi}{8}})X + |e^{\frac{(2k+1)i\pi}{8}}|^2 = X^2 - 2\cos\left(\frac{(2k+1)\pi}{8}\right)X + 1, \text{ ceci donne une autre décomposition dans } \mathbb{R}[X] :$$

$$4X^8 + 4 = 4 \prod_{k=0}^3 \left(X^2 - 2\cos\left(\frac{(2k+1)\pi}{8}\right)X + 1 \right).$$

Remarque 2.3.3 Nous pouvons prouver grâce à cela que : $\cos(\pi/8) = \frac{\sqrt{2+\sqrt{2}}}{2}$.

On a unicité de la décomposition en facteurs irréductibles, donc on peut identifier cette décomposition à la précédente. Regardons les termes en $-X$ pour les identifier dans les deux décompositions.

$\cos$ est décroissante sur $[0, \pi]$, donc $\cos(\pi/8) > \cos(3\pi/8) > \cos(5\pi/8) > \cos(7\pi/8)$ et dans l'autre décomposition :

$$\sqrt{2+\sqrt{2}} > \sqrt{2-\sqrt{2}} > -\sqrt{2-\sqrt{2}} > -\sqrt{2+\sqrt{2}}, \text{ ainsi } 2\cos(\pi/8) = \sqrt{2+\sqrt{2}}, \text{ soit :}$$

$$\cos(\pi/8) = \frac{\sqrt{2+\sqrt{2}}}{2}.$$

3. Soit $P \in \mathbb{R}[X]$ non constant tel que : $\forall x \in \mathbb{R}, P(x) \geq 0$. Montrer qu'il existe $A, B \in \mathbb{R}[X]$ tels que : $P = A^2 + B^2$.

4. Si $P = a_0 + \dots + a_n X^n$ est dans $\mathbb{Z}[X]$, on définit son « contenu » noté c_P qui est $a_0 \wedge \dots \wedge a_n$. Soient $P, Q \in \mathbb{Z}[X]$.

(a) Si $c_P = c_Q = 1$, montrer que : $c_{PQ} = 1$.

(b) Montrer que $c_{PQ} = c_P c_Q$ dans tous les cas.

(c) On dit qu'un polynôme P est irréductible dans $\mathbb{Z}[X]$, s'il n'existe pas de polynômes U, V dans $\mathbb{Z}[X]$ tels que $UV = P$ et $d^\circ(U) < d^\circ(P)$ et $d^\circ(V) < d^\circ(P)$. Montrer que si P est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$.

2.4 Révision de sup sur les fractions rationnelles

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

Définition 2.4.1 (Degré) Si $F = \frac{P}{Q}$, 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 $E, P_1, Q_1 \in \mathbb{K}[X]$ et $F_1 \in \mathbb{K}(X)$ tels que $F = E + F_1 = E + \frac{P_1}{Q_1}$ et $\deg(F_1) < 0$, soit $\deg(P_1) < \deg(Q_1)$. E est la **partie entière** de F .

Définition 2.4.2 (Pôle) Soit $F \in \mathbb{K}(X)$ de forme irréductible $\frac{P}{Q}$. 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 $F = \frac{P}{Q}$ une fraction rationnelle à coefficients réels, écrite sous forme irréductible, avec $Q = \lambda \prod_{k=1}^p (X - \alpha_k)^{r_k}$. Alors F s'écrit de

manière unique $F = E + \sum_{k=1}^n \sum_{j=1}^{r_k} \frac{\lambda_{k,j}}{(X - \alpha_k)^j}$, où E est la partie entière de F et pour tout $k \in \llbracket 1, n \rrbracket$, $\sum_{j=1}^{r_k} \frac{\lambda_{k,j}}{(X - \alpha_k)^j}$ est la partie polaire de F relative à α_k . C'est sa décomposition en éléments simples.

Proposition 2.4.3 (Dérivée logarithmique) Si $P = \lambda \prod_{k=1}^p (X - \alpha_k)^{n_k}$, alors $\frac{P'}{P} = \sum_{k=1}^p \frac{n_k}{X - \alpha_k}$.

Exemple 2.4.1 Soit $P \in \mathbb{C}[X]$ de degré au moins 2. Pour $z_1, \dots, z_p \in \mathbb{C}$ l'ensemble

$\left\{ \sum_{i=1}^p \lambda_i z_i, \lambda_1, \dots, \lambda_p \in \mathbb{R}_+, \sum_{i=1}^p \lambda_i = 1 \right\}$ est appelé enveloppe convexe de $z_1, \dots, z_p$.

1. (**Théorème de Gauss-Lucas**) Montrer que les racines de P' sont incluses dans l'enveloppe convexe des racines de P .
2. Si P est dans $\mathbb{R}[X]$ est scindé sur $\mathbb{R}$, montrer que P' l'est aussi.

Proposition 2.4.4 (Décomposition en éléments simples dans $\mathbb{R}(X)$) Soit $F = \frac{P}{Q}$ 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

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

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 décomposition 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 2.4.5 (Coefficient d'un pôle simple) Si $F = P/Q \in \mathbb{K}(X)$ et α est racine simple de Q , alors $Q = (X - \alpha)S$, avec $S(\alpha) \neq 0$ et le coefficient de $\frac{1}{X - \alpha}$ dans la décomposition en élément simple de F : $\frac{P(\alpha)}{S(\alpha)} = \frac{P(\alpha)}{Q'(\alpha)}$.

Exemple 2.4.2 Soit $\omega_k = e^{\frac{2ik\pi}{n}}$, avec k dans $\llbracket 0, n-1 \rrbracket$ et $n \geq 2$. Réduire au même dénominateur

$$F = \sum_{k=0}^{n-1} \frac{1}{X - \omega_k}.$$

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 $x^{-1} = x'$.

On dit que la loi $*$ est commutative si : $\forall x, y \in G, x * y = y * x$) et dans ce cas, le groupe est dit commutatif ou abélien.

Remarque 3.1.1 1. Il y a unicité de l'élément neutre et de l'inverse de chaque élément.

2. Lorsque le groupe est commutatif, la loi de composition interne peut être notée $+$. Dans ce cas l'inverse de x se note $-x$.
3. On a : $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$.
4. On note parfois xy l'opération $x * y$.
5. On note $x^m = x * x * \dots * x$, m fois et si le groupe est additif, on note $mx = x + x + \dots + x$, m fois.
6. Comme G n'est pas forcément commutatif, en général pour $x, y \in G$, on a : $(x * y)^m \neq x^m * y^m$.

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. Soit X un ensemble. On note $\mathcal{S}_X$ l'ensemble des bijections de X dans lui-même (appelées aussi permutations de X). Alors $(\mathcal{S}_X, \circ)$ a une structure de groupe pour la composition. On rappelle que si f et g sont deux bijections de X dans X , alors $f \circ g$ et f^{-1} le sont aussi. Ici l'élément neutre est $Id_X : x \mapsto x$.
Si $X = [1, n]$, on note $\mathcal{S}_n$ l'ensemble des permutations de $[1, n]$.
 3. $(GL_n(\mathbb{K}), \cdot)$ est un groupe de matrices pour la multiplication matricelle, d'élément neutre I_n .
 4. $GL(E)$, avec E un espace vectoriel, d'élément neutre Id_E .
 5. Soit $a \in G$. Les applications $\varphi_a : \begin{cases} G & \rightarrow G \\ x & \mapsto ax \end{cases}$ et $\psi : \begin{cases} G & \rightarrow G \\ x & \mapsto x^{-1} \end{cases}$ sont bijectives.
On remarque que : $\psi \circ \psi = Id_G$.

Proposition 3.1.1 (Le groupe $\mathbb{Z}/n\mathbb{Z}$) Soit $n \in \mathbb{Z}$, alors $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

Démonstration : La proposition 1.2.3 nous dit que la loi $+$ est bien définie et que c'est un loi de composition interne.

- Soient $x, y, z \in \mathbb{Z}$. Comme la loi $+$ est associative sur $\mathbb{Z}$, alors : $(\overline{x + y}) + \overline{z} = \overline{x + y + z} = \overline{(x + y) + z} = \overline{x + (y + z)} = \overline{x} + \overline{(y + z)} = \overline{x} + (\overline{y} + \overline{z})$.
- L'élément neutre est : $\overline{0}$.
- Soit $x \in \mathbb{Z}$, alors l'inverse de $\overline{x}$ est : $\overline{-x}$.

Ce groupe est commutatif, car $\forall x, y \in \mathbb{Z}, \overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}$.

Remarque 3.1.2 1. On note $\overline{-x} = -\overline{x}$, en tant qu'inverse de $\overline{x}$ pour une loi additive.

2. $\underbrace{\overline{x} + \dots + \overline{x}}_{k \text{ fois}} = \overline{\underbrace{x + \dots + x}_{k \text{ fois}}}$ se note $k\overline{x}$ et donc $k\overline{x} = \overline{kx}$.

Définition 3.1.2 (Produit fini de groupes) Soient $(G_1, *_1), \dots, (G_n, *_n)$ n groupes. Soit $*$ la loi de composition interne définie sur $G_1 \times \dots \times G_n$ par :

$$\forall (g_1, h_1, \dots, g_n, h_n) \in G_1^2 \times \dots \times G_n^2, (g_1, \dots, g_n) * (h_1, \dots, h_n) = (g_1 *_1 h_1, \dots, g_n *_n h_n).$$

$(G_1 \times \dots \times G_n, *)$ est le groupe produit de $G_1, \dots, G_n$.

Remarque 3.1.3 L'élément neutre est $(e_{G_1}, \dots, e_{G_n})$ et $(g_1, \dots, g_n)^{-1} = (g_1^{-1}, \dots, g_n^{-1})$.

3.1.2 Sous-groupes

Définition 3.1.3 (Sous-groupe) Une partie H d'un groupe $(G, *)$ est un sous-groupe de G lorsqu'elle vérifie les assertions suivantes :

- $e \in H$, avec e l'élément neutre de G .
- H est stable pour $*$: $\forall x, y \in H, x * y \in H$.
- Le symétrique de tout élément de H est encore dans H : $\forall x \in H, x^{-1} \in H$.

Remarque 3.1.4 ATTENTION, dire que H est un sous-groupe ne veut rien dire. Il faut préciser de quel groupe on est un sous-groupe.

Proposition 3.1.2 (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 fini tel que : $\forall x \in G, x^2 = e$. Montrer que G est commutatif et que $\text{card}(G) = 2^k$, avec un certain k de $\mathbb{N}$ (on pourra montrer que si H est un sous-groupe de G , alors $H \cup aH$ est un sous-groupe de G pour a dans $G \setminus H$).

3.1.3 Intersection de groupes, groupe engendré par une partie

Proposition 3.1.3 (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 .

Démonstration : • $\bigcap_{i \in I} H_i$ est inclus dans G .

• Comme les H_i pour i dans I sont des sous-groupes, alors : $\forall i \in I, e_G \in H_i$, puis $e_G \in \bigcap_{i \in I} H_i$.

• Soient $x, y \in \bigcap_{i \in I} H_i$. Ainsi x et y sont dans tous les H_i pour i dans I , qui sont des sous-groupes de G , donc : $\forall i \in I, xy^{-1} \in H_i$, puis $xy^{-1} \in \bigcap_{i \in I} H_i$.

Remarque 3.1.5 *Attention, la réunion de sous-groupes n'est pas en général pas un sous-groupe. Par exemple $G_1 = \{2k, k \in \mathbb{Z}\} = 2\mathbb{Z}$ et $G_2 = \{3k, k \in \mathbb{Z}\} = 3\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$, mais $G_1 \cup G_2$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$. En effet 2 est dans G_1 , 3 est dans G_2 , mais $2 + 3 = 5$ n'est pas dans $G_1 \cup G_2$, donc ce dernier ensemble n'est pas stable par addition.*

Définition 3.1.4 (Sous-groupe engendré par une partie) Soit $(G, *)$ un groupe et A une partie de G . L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G , appelé sous-groupe engendré par A et noté $\langle A \rangle$. Ainsi $\langle A \rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H$.

Proposition 3.1.4 (Caractérisation du sous-groupe engendré par A) Soit $(G, *)$ un groupe et A une partie de G . Alors $\langle A \rangle$ est, au sens de l'inclusion, le plus petit sous-groupe de G contenant A . Autrement dit, si H est un sous-groupe de G tel que $A \subset H$, alors $\langle A \rangle \subset H$.

Démonstration : • D'après le théorème d'intersection $\langle A \rangle$ est bien un sous-groupe de G et il contient A par construction.

• Soit H un sous-groupe de G contenant A . Puisque $\langle A \rangle$ est l'intersection de tous les sous-groupes de G contenant A , on a $\langle A \rangle \subset H$. Ainsi $\langle A \rangle$ est contenu dans tout sous-groupe contenant A , c'est donc bien le plus petit au sens de l'inclusion.

Définition 3.1.5 (Partie génératrice) Soit A une partie de G . On dit que A engendre G si $\langle A \rangle = G$.

Remarque 3.1.6 1. $\langle \emptyset \rangle = \{e_G\}$.

2. Si A est non-vide alors on peut montrer que

$$\langle A \rangle = \{ \alpha_1^{\varepsilon_1} * \cdots * \alpha_n^{\varepsilon_n}, \quad n \in \mathbb{N}^*, (\alpha_1, \dots, \alpha_n) \in A^n, (\varepsilon_1, \dots, \varepsilon_n) \in \{1, -1\}^n \}.$$

En effet si on pose $B = \{ \alpha_1^{\varepsilon_1} * \cdots * \alpha_n^{\varepsilon_n}, \quad n \in \mathbb{N}^*, (\alpha_1, \dots, \alpha_n) \in A^n, (\varepsilon_1, \dots, \varepsilon_n) \in \{1, -1\}^n \}$, on montre que B est un sous-groupe de G qui contient A , donc $\langle A \rangle \subset B$, par minimalité de $\langle A \rangle$. Par ailleurs comme $A \subset \langle A \rangle$ et que $\langle A \rangle$ est un sous-groupe de G , alors il est stable par opérations, puis $B \subset \langle A \rangle$.

En d'autres termes $\langle A \rangle$ est l'ensemble des éléments de G qui sont des produits finis d'éléments de A ou d'inverses d'éléments de A . Ce sont toutes les combinaisons possibles d'opérations effectuées à partir d'éléments de A .

Exemple 3.1.3 Le groupe $(\mathbb{Q}, +)$ peut-il être engendré par une partie finie ?

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

Proposition 3.1.5 (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.

Démonstration :

- $n\mathbb{Z}$ est inclus dans $\mathbb{Z}$.

On a : $0 = n \times 0 \in n\mathbb{Z}$.

Soient $nx, ny \in n\mathbb{Z}$, avec x, y dans $\mathbb{Z}$. On a $nx - ny = n(x - y)$ qui reste dans $n\mathbb{Z}$.

Par la caractérisation des sous-groupes, $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

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

1. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.

2. Si $H \neq \{0\}$, alors il existe m dans H non nul. Si m est dans H , alors $-m$ aussi et donc l'ensemble $\{m, -m\} \subset H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$. Elle possède donc un plus petit élément $n > 0$, qui est dans H . Comme H est un sous-groupe de $\mathbb{Z}$, ainsi le sous-groupe $n\mathbb{Z}$ engendré par n vérifie par stabilité des opérations dans H :

$$n\mathbb{Z} \subset H.$$

Montrons aussi que $H \subset n\mathbb{Z}$. Soit $m \in H$. Alors

$$\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}, \begin{cases} m = nq + r \\ 0 \leq r < n \end{cases}$$

Comme $m \in H$ et $nq \in H$ donc $r = m - nq \in H$. Mais $r < n$ et n est le plus petit élément strictement positif de H . Donc $r = 0$ et $m = nq \in n\mathbb{Z}$.

Finalement $H \subset n\mathbb{Z}$ et on conclut $H = n\mathbb{Z}$.

3.2 Morphisme de groupe

3.2.1 Définition et exemples

Définition 3.2.1 (Morphisme de groupes) Soient $(G, *)$ et $(H, \top)$ deux groupes et une application $f : G \rightarrow H$. 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 $f : (G, *) \rightarrow (H, \top)$ 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 $f : G \rightarrow H$ un morphisme de groupes. Alors :

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

Remarque 3.2.1 La composition de morphismes de groupes est un morphisme de groupes.

Exemple 3.2.1 1. $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times), x \mapsto e^x$, est un morphisme de groupes.

En effet : $\forall x, y \in \mathbb{R}, f(x + y) = e^{x+y} = e^x e^y = f(x) \times f(y)$.

2. $g : (\mathbb{C}, +) \rightarrow (\mathbb{C}, +), z \mapsto \bar{z}$, est un morphisme de groupes.

En effet : $\forall z, z' \in \mathbb{C}, g(z + z') = \overline{z + z'} = \bar{z} + \bar{z}' = g(z) + g(z')$.

3. Le déterminant $\det : (GL_n(\mathbb{C}), \times) \mapsto (\mathbb{C}^*, \times)$ est un morphisme de groupes.

En effet : $\forall M, N \in GL_n(\mathbb{C}), \det(M \times N) = \det(M) \times \det(N)$.

4. Déterminer les morphismes de groupes $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$ qui sont continus en 0.

5. Soient Γ, Γ' des groupes finis et $\varphi : \Gamma \rightarrow \Gamma'$ un morphisme de groupes. Soit $H = \ker \varphi$. Démontrer que $\text{card}(\Gamma) = \text{card}(\varphi(\Gamma)) \text{card}(H)$.

3.2.2 Image et noyau d'un morphisme

Proposition 3.2.2 (Image directe et image réciproque de sous-groupes par un morphisme) *L'image directe et l'image réciproque de sous-groupes par un morphisme de groupes sont des sous-groupes.*

*Plus précisément soit $f : (G, *) \rightarrow (H, \top)$ 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 $f : (G, *) \rightarrow (H, \top)$ un morphisme de groupes.*

1. *On appelle noyau de f , noté $\text{Ker}(f)$, l'ensemble des antécédents par f de e_H dans G :*

$$\text{Ker}(f) = f^{-1}(\{e_H\}) = \{x \in G ; f(x) = e_H\}.$$

C'est d'après la proposition précédente un sous-groupe de G .

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

$$\text{Im}(f) = f(G) = \{y \in H ; \exists x \in G, y = f(x)\}.$$

C'est d'après la proposition précédente un sous-groupe de H .

Remarque 3.2.2 *Un noyau n'est jamais vide. En effet, il contient toujours e_G , car $f(e_G) = e_H$.*

Exemple 3.2.2 *Montrer que $SL_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{C}), \det(M) = 1\}$ est un groupe.*

Proposition 3.2.3 (Caractérisation des morphismes injectifs/surjectifs) Soit

$f : (G, *) \rightarrow (H, \top)$ un morphisme de groupes.

1. f est injective si et seulement si $\text{Ker}(f) = \{e_G\}$.
2. f est surjective si et seulement si $\text{Im}(f) = H$.

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.

Exemple 3.2.3 1. Les groupes $(\mathbb{R}_+^*, \times)$ et $(\mathbb{R}, +)$ sont isomorphes via $\ln$

$$(\forall x, y \in \mathbb{R}_+^*, \ln(xy) = \ln(x) + \ln(y)).$$

2. Soit G un groupe. Soit $g \in G$. Alors $\varphi_g : \begin{cases} G & \rightarrow G \\ x & \mapsto gxg^{-1} \end{cases}$ est un isomorphisme de groupe

Montrer que φ_g est un morphisme de groupe.

$$\text{On a : } \forall x, y \in G, \varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y).$$

$$\text{Nous remarquons que : } \forall x \in G, \varphi_g \circ \varphi_{g^{-1}}(x) = \varphi_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x. \text{ Ainsi :}$$

$$\varphi_g \circ \varphi_{g^{-1}} = \text{Id}_G. \text{ De même on a : } \varphi_{g^{-1}} \circ \varphi_g = \text{Id}_G. \text{ Ainsi } \varphi_g \text{ est bijective et } (\varphi_g)^{-1} = \varphi_{g^{-1}}.$$

3. Soit G un sous-groupe non réduit à $\{0\}$ de $(\mathbb{Z}^n, +)$. Montrer qu'il existe $r \in \llbracket 1, n \rrbracket$ tel que G soit isomorphe à $\mathbb{Z}^r$, on pourra considérer le morphisme de groupes $f : \begin{cases} \mathbb{Z}^n & \rightarrow \mathbb{Z} \\ (x_1, \dots, x_n) & \mapsto x_n \end{cases}$ et raisonner par récurrence sur n .

Procédons par récurrence.

Pour $n = 1$, on a $G = k\mathbb{Z}$, avec $k \in \mathbb{N}^*$ et on a l'isomorphisme $m \mapsto km$ dans $\mathbb{Z}$ dans G .

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.

Exemple 3.2.4 L'isomorphisme réciproque de $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$ est $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$, qui est bien un morphisme de groupes.

Proposition 3.2.5 (La surjection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$) L'application $a \mapsto \bar{a}$ est un morphisme surjectif de groupe de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$.

Le noyau de cette application est $n\mathbb{Z}$.

Démonstration : • Cette application est un morphisme de groupe car par définition des opérations dans $\mathbb{Z}/n\mathbb{Z}$ (proposition 1.2.3), on a : $\forall a, b \in \mathbb{Z}, \overline{a+b} = \overline{a} + \overline{b}$.

• Soit $x \in \mathbb{Z}/n\mathbb{Z}$. Il existe un représentant k dans $\mathbb{Z}$ de la classe $x : x = \overline{k}$. Ainsi l'application $a \mapsto \overline{a}$ est bien surjective de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

• On a $\overline{a} = 0$ si et seulement si $a \equiv 0[n]$ si et seulement si $n|a$ si et seulement si a est dans $n\mathbb{Z}$. Donc le noyau de l'application $a \mapsto \overline{a}$ est bien $n\mathbb{Z}$.

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 lorsqu'il est engendré par un seul de ses éléments. En d'autres termes, il existe $g \in G$ tel que $G = \langle \{g\} \rangle$. On note souvent $G = \langle g \rangle$. Dans ce cas tout élément $g \in G$ tel que $G = \langle g \rangle$ est appelé générateur de G .*

Proposition 3.3.1 (Description des groupes monogènes) *Soit $G = \langle \{g\} \rangle$ un groupe monogène engendré par g . Alors $G = \{g^k, k \in \mathbb{Z}\}$.*

Démonstration : • Comme G est un groupe, il est stable par multiplications, donc : $\forall k \in \mathbb{N}, g^k \in G$. Il est aussi stable par passage à l'inverse, donc $g^{-1} \in G$, puis : $\forall k \in \mathbb{N}, g^{-k} = (g^{-1})^k \in G$. Ainsi on a : $\{g^k, k \in \mathbb{Z}\} \subset G$.

• Montrons que $H = \{g^k, k \in \mathbb{Z}\}$ est un sous-groupe de G .

On a $e_G = g^0 \in H$ et pour $x = g^k$ et $y = g^l$, avec k, l dans $\mathbb{Z}$, on a : $x * y^{-1} = g^k * g^{-l} = g^{k-l} \in H$. Donc par la caractérisation des sous groupes H est un sous-groupe de G contenant g .

Or $\langle g \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) de G contenant g , par définition d'un sous-groupe engendré par une partie, donc : $\langle g \rangle \subset H$, puis $G \subset \{g^k, k \in \mathbb{Z}\}$.

Remarque 3.3.1 *Soient $G = \langle \{g\} \rangle$ un groupe monogène, G' un groupe et $f : G \rightarrow G'$ un morphisme de groupe. Alors $H = f(G)$ est*

Proposition 3.3.2 (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 $\mathbb{Z}/n\mathbb{Z} = \{p\overline{k}, p \in \mathbb{Z}\} = \{\overline{0}, \overline{k}, 2\overline{k}, \dots, (n-1)\overline{k}\}$, si k est premier avec n .

Démonstration :

Exemple 3.3.1 *Donner les générateurs de $(\mathbb{Z}/6\mathbb{Z}, +)$. Quel est le sous-groupe engendré par $\overline{2}$?*

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

Exemple 3.3.2 1. $(\mathbb{Z}, +)$ est , engendré par

2. $(\mathbb{U}_n, \times)$ est , engendré par

3. $(\mathbb{Z}/n\mathbb{Z}, +)$ est , engendré par

Proposition 3.3.3 (Description des groupes monogènes) 1. *Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.*

2. 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 $G = \{e, g, g^2, \dots, g^{n-1}\}$, pour un certain g dans G et n est le plus petit entier naturel k non nul tel que $g^k = e$.

Démonstration : Soit $G = \langle \{g\} \rangle = \{g^k, k \in \mathbb{Z}\}$. On pose $\varphi : \begin{cases} (\mathbb{Z}, +) & \rightarrow (G, *) \\ k & \mapsto g^k \end{cases}$. Cette application

est bien un morphisme de groupes : $\forall k, l \in \mathbb{Z}, \varphi(k+l) = g^{k+l} = g^k * g^l = \varphi(k) * \varphi(l)$.

Cette application est par ailleurs surjective, car : $\forall k \in \mathbb{Z}, \varphi(k) = g^k$ et $G = \{g^k, k \in \mathbb{Z}\}$.

Le noyau de φ est un sous-groupe de $(\mathbb{Z}, +)$ grâce à la proposition 3.2.2. La proposition 3.1.5 nous dit qu'il existe n dans $\mathbb{N}$ tel que $\text{Ker } \varphi = n\mathbb{Z}$.

• Premier cas : $n = 0$. Ainsi $\text{Ker } \varphi = \{0\}$, donc φ est injective (proposition 3.2.3). Cela fait que φ est un isomorphisme de $(\mathbb{Z}, +)$ dans $(G, *)$.

• Deuxième cas : $n > 0$. Soit $\psi : \begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) & \rightarrow (G, *) \\ \bar{k} & \mapsto g^k \end{cases}$.

Remarque 3.3.2 (IMPORTANTE) Soit $f : G \rightarrow G'$ un isomorphisme. Alors G est monogène si et seulement si G' est monogène. On a vu dans la remarque 3.3.1 que si G est monogène, alors G' l'est aussi. Réciproquement $f^{-1} : G' \rightarrow G$ est aussi un morphisme de groupe et donc si G' est monogène, alors G l'est aussi.

Dans ce cas, G est cyclique si et seulement si G' l'est aussi, car ces deux groupes sont infinis ou finis en même temps, car f est bijective.

Exemple 3.3.3 1. Dans $GL_2(\mathbb{R})$, le groupe engendré par $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ est-il monogène ou cyclique ?

2. $(\mathbb{U}_n, \times)$ est cyclique avec $\mathbb{U}_n = \{1, e^{\frac{2i\pi}{n}}, (e^{\frac{2i\pi}{n}})^2, \dots, (e^{\frac{2i\pi}{n}})^{n-1}\}$. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$, via l'application $\begin{cases} \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{U}_n \\ \bar{k} & \mapsto & e^{\frac{2ik\pi}{n}} \end{cases}$.
- Quels sont les éléments générateurs de $(\mathbb{U}_n, \times)$?

3. Montrer qu'un sous-groupe H d'un groupe monogène $G = \{g^k, k \in \mathbb{Z}\}$ est monogène. Montrer qu'un sous-groupe d'un groupe cyclique est cyclique.

Si G est cyclique, alors il est fini, donc H aussi, puis H est cyclique.

4. Soient $m, n \in \mathbb{N}^*$. Déterminer les morphismes et isomorphismes de groupes $\varphi : (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m\mathbb{Z}, +)$.

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 : $g^n = e_G$.

Exemple 3.4.1 Soient $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. On se place dans le groupe $GL_2(\mathbb{R})$. On constate que $A^2 = -I_2$, $A^3 = -A$ et $A^4 = I_2$, donc A est d'ordre 4. On a : $B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ et $B^3 = I_2$, donc B est d'ordre 3.

Mais $AB = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ qui n'est pas d'ordre fini, grâce à l'exemple précédent. Ainsi le produit de deux éléments d'ordre fini n'est pas forcément fini.

Proposition 3.4.1 (Sous-groupe engendré par un élément d'ordre fini) *Un élément g d'un groupe G est d'ordre fini si et seulement si le sous-groupe engendré par g est fini.*

Dans ce cas, l'ordre n de g est le cardinal du sous-groupe engendré par g : $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$ et :

$$\forall k \in \mathbb{N}, g^k = e_G \Leftrightarrow n|k.$$

Démonstration : Grâce à la démonstration de la proposition 3.3.3, g est d'ordre fini si et seulement si $\varphi : \begin{cases} (\mathbb{Z}, +) & \rightarrow (G, *) \\ k & \mapsto g^k \end{cases}$ n'est pas injective si et seulement si le groupe monogène $\langle g \rangle$ est fini. Dans ce cas, si on note n le plus petit entier k tel que $g^k = e_G$, alors n est l'ordre de g et la proposition 3.3.3 nous dit que ce groupe est de cardinal n . La dernière équivalence est donnée par la même proposition.

Exemple 3.4.2 1. Soit a un élément d'ordre n . Soit $k \in \mathbb{N}^*$ et on pose $d = k \wedge n$. Montrer que l'ordre de a^k est n/d .

On remarque que si k divise n , alors l'ordre de a^k est n/k .

2. Soient G un groupe et $a, b \in G$ tels que $ab = ba$ avec a d'ordre p et b d'ordre q .

(a) Si p et q sont premiers entre eux, quel est l'ordre de ab ?

(b) Dans le cas général, est-ce que l'ordre de ab est $p \vee q$?

3. Les groupes $(\mathbb{Z}/8\mathbb{Z}, +)$ et $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ sont-ils isomorphes bien qu'ils aient le même cardinal ?

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 : $p|n$. En particulier $a^n = e_G$.

Démonstration : Voici une démonstration simple dans le cas où G est commutatif :

Pour la preuve dans le cas général, nous allons démontrer le théorème de Lagrange, qui dit que pour tout sous-groupe H de G , on a $\text{card}(H) \mid \text{card}(G)$.

Soient $x, y \in G$. Montrons que $xH = yH$ ou $(xH) \cap (yH) = \emptyset$.

Supposons que $(xH) \cap (yH) \neq \emptyset$. Il existe donc $h, h' \in H$ tels que $xh = yh'$, soit $x = yh'h^{-1}$. Soit $k \in H$. On a donc $xk = y \underbrace{h'h^{-1}k}_{\in H} \in yH$. Ainsi $xH \subset yH$. On montre de même l'autre inclusion et donc

$xH = yH$.

Or on a : $G = \bigcup_{g \in G} gH$ que l'on peut donc écrire comme une union disjointe $x_1H \cup \dots \cup x_pH$. Ainsi

on a : $|G| = \sum_{k=1}^p |x_iH|$. Par suite pour $i \in \llbracket 1, p \rrbracket$ comme $f : \begin{cases} H & \rightarrow & x_iH \\ h & \mapsto & x_ih \end{cases}$ est une bijection (de

réciroque $z \mapsto x_i^{-1}z$), alors $|x_iH| = |H|$, puis $|G| = p|H|$, ce qui donne le théorème de Lagrange.

On en déduit que pour $H = \langle a \rangle$, alors $p = |H|$ divise G .

Exemple 3.4.3 1. (a) Montrer que $\mathbb{U}_n$ est le seul sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal n .

(b) Soit G un sous-groupe fini de $GL_2(\mathbb{C})$ tel que $G \cap SL_2(\mathbb{C}) = \{I_2\}$, avec $SL_2(\mathbb{C}) = \{M \in \mathcal{M}_2(\mathbb{C}), \det(M) = 1\}$. Montrer que G est cyclique.

2. Soit G un groupe de cardinal p , avec p un nombre premier. Montrer que G est cyclique.

3. Déterminer les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal k avec $k \mid n$.

4. Soit $(G, .)$ un groupe commutatif fini de cardinal n et de neutre e . Pour $d \in \mathbb{N}^*$ divisant n , soit

$G_d = \{x \in G, x^d = e\}$. On écrit $n = \prod_{i=1}^r p_i^{\alpha_i}$ la décomposition de n en facteurs premiers.

(a) Montrer que $f : \begin{cases} \prod_{i=1}^r G_{p_i^{\alpha_i}} & \rightarrow G \\ (x_1, \dots, x_r) & \mapsto x_1 \dots x_r \end{cases}$ est un isomorphisme.

(b) On suppose désormais que pour tout diviseur d de n dans $\mathbb{N}^*$, on a : $|G_d| \leq d$. Montrer que pour tout i dans $\llbracket 1, r \rrbracket$, il existe g_i dans G d'ordre $p_i^{\alpha_i}$, puis que G est cyclique.

(a)

(b) Soit $i \in \llbracket 1, r \rrbracket$. L'isomorphisme entre ensembles finis de la question précédente implique

$|G| = \prod_{i=1}^r |G_{p_i^{\alpha_i}}|$ avec $|G| = \prod_{i=1}^r p_i^{\alpha_i}$ et : $\forall i \in \llbracket 1, r \rrbracket, |G_{p_i^{\alpha_i}}| \leq p_i^{\alpha_i}$. On a donc nécessairement $|G_{p_i^{\alpha_i}}| = p_i^{\alpha_i}$ pour tout i . On rappelle une fois encore que l'ordre des éléments de $G_{p_i^{\alpha_i}}$ divise $p_i^{\alpha_i}$, notons $p_i^{\beta_i}$ l'ordre maximal des éléments de $G_{p_i^{\alpha_i}}$ (qui sont en nombre fini), avec : $\beta_i \leq \alpha_i$. On

a donc : $\forall x \in G_{p_i^{\alpha_i}}, x^{p_i^{\beta_i}} = e$, alors $G_{p_i^{\alpha_i}} \subset G_{p_i^{\beta_i}}$.

Par hypothèse, $p_i^{\alpha_i} = |G_{p_i^{\alpha_i}}| = |G_{p_i^{\beta_i}}| \leq p_i^{\beta_i}$, donc $\alpha_i \leq \beta_i$, puis $\beta_i = \alpha_i$. Ainsi, G a un élément d'ordre $p_i^{\alpha_i}$ que l'on note g_i . Posons $x = g_1 \dots g_r$.

L'ordre N de x divise n , et d'après l'isomorphisme établi à la question précédente, si $x^N = e = f(g_1^N, \dots, g_r^N)$ alors pour tout $i \in \llbracket 1, r \rrbracket$, on a $g_i^N = e$ d'où $p_i^{\alpha_i} | N$, et ainsi les p_i étant des nombres premiers, $n | N$, puis $N = n$. En conclusion x est d'ordre n , donc G est cyclique.

3.5 Rappels de sup sur 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 $\llbracket 1, n \rrbracket$. $(\mathcal{S}_n, \circ)$ est un groupe de cardinal $n!$. Si $n \geq 3$, ce groupe est non commutatif.

Remarque 3.5.1 Intuitivement, cet ensemble est de cardinal $n!$, car pour une bijection σ de $\llbracket 1, n \rrbracket$ dans $\llbracket 1, n \rrbracket$, pour $\sigma(1)$, nous avons n choix, puis pour $\sigma(2)$, nous avons $n - 1$ choix, pour $\sigma(3)$, on a $n - 2$ choix, ..., pour $\sigma(n - 1)$, il reste deux choix et pour $\sigma(n)$, on n'a qu'un choix. Par cette construction, le nombre de permutations σ possibles est $n \times (n - 1) \times \dots \times 2 \times 1 = n!$.

Exemple 3.5.1 Est-ce que $\mathcal{S}_7$ possède un élément d'ordre 160 ?

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 $i, j \in \llbracket 1, n \rrbracket$ 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 $\tau = (i, j)$.

Remarque 3.5.2 Une transposition est d'ordre 2.

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

Remarque 3.5.3 Un cycle c de longueur p est d'ordre p . En effet, nous constatons qu'en appliquant p fois c on revient au point de départ : $\forall x \in \llbracket 1, n \rrbracket, c^p(x) = x$. Ainsi $c^p = Id$, puis c est d'ordre au plus p .

Par ailleurs $c(a_1) = a_2, c^2(a_1) = a_3, \dots, c^{p-1}(a_1) = a_p$, donc : $\forall k \in \llbracket 1, p-1 \rrbracket, c^k(a_1) \neq a_1$ et donc : $\forall k \in \llbracket 1, p-1 \rrbracket, c^k \neq Id$. Donc l'ordre de c n'est pas strictement inférieur à p . Ainsi c est d'ordre p et $\langle c \rangle = \{Id, c, \dots, c^{p-1}\}$.

Exemple 3.5.2 Soit $c = (a_1, \dots, a_p)$ un p -cycle de $\mathcal{S}_n$. Soit $\sigma \in \mathcal{S}_n$. Montrer que $\sigma \circ c \circ \sigma^{-1}$ est un cycle dont on donnera les caractéristiques.

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.

Exemple 3.5.3 Soit $\sigma \in \mathcal{S}_n$. Pour $k \in \llbracket 1, n \rrbracket$, on note $n_k(\sigma)$ le nombre de cycles de longueur k dans la décomposition en cycles de σ . Soit $\tau \in \mathcal{S}_n$. Montrer qu'il existe $\rho \in \mathcal{S}_n$ tel que $\tau = \rho \circ \sigma \circ \rho^{-1}$ si et seulement si : $\forall k \in \llbracket 1, n \rrbracket, n_k(\tau) = n_k(\sigma)$.

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.

Démonstration : Soit H le sous-groupe de $\mathcal{S}_n$ engendré par les permutations. Par définition d'un sous-groupe, nous avons $H \subset \mathcal{S}_n$.

Nous savons par ailleurs que toute permutation est un produit de transpositions. Ainsi $\mathcal{S}_n \subset H$. Ainsi $H = \mathcal{S}_n$.

Exemple 3.5.4 Montrer que $\{(1, i), 2 \leq i \leq n\}$ engendre $\mathcal{S}_n$.

Définition 3.5.4 (Signature) Il existe un et un seul morphisme de groupes $\varepsilon : (\mathcal{S}_n, \circ) \rightarrow (\{1, -1\}, \times)$ 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 3.5.5 1. L'ensemble des permutations de $\mathcal{S}_n$ de signature un noté $\mathcal{A}_n$ est un sous-groupe de $\mathcal{S}_n$ de cardinal $n!/2$, pour $n \geq 2$.

$\mathcal{A}_n$ est le noyau du morphisme de groupe ε , donc $\mathcal{A}_n$ est un sous-groupe de $\mathcal{S}_n$.

On pose $\mathcal{B}_n = \{\sigma \in \mathcal{S}_n, \varepsilon(\sigma) = -1\}$. On a $\mathcal{S}_n = \mathcal{A}_n \cup \mathcal{B}_n$ et cette union est disjointe. Montrons que $|\mathcal{A}_n| = |\mathcal{B}_n|$. Nous allons établir une bijection entre ces deux ensembles. Soit $\tau = (1, 2)$. Soit

$\phi : \begin{cases} \mathcal{A}_n & \rightarrow \mathcal{B}_n \\ \sigma & \mapsto \tau\sigma \end{cases}$ Cette application est bien à valeurs dans $\mathcal{B}_n$, car :

$\forall \sigma \in \mathcal{A}_n, \varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma) = (-1) \times 1 = -1$. On pose $\psi : \begin{cases} \mathcal{B}_n & \rightarrow \mathcal{A}_n \\ \sigma & \mapsto \tau\sigma \end{cases}$.

On a : $\forall \sigma \in \mathcal{A}_n, \psi \circ \phi(\sigma) = \tau^2\sigma = \sigma$ et donc : $\psi \circ \phi = Id_{\mathcal{A}_n}$ et on montre de même que : $\phi \circ \psi = Id_{\mathcal{B}_n}$. Ainsi ϕ est une bijection et donc : $|\mathcal{A}_n| = |\mathcal{B}_n|$. Ainsi $|\mathcal{S}_n| = |\mathcal{A}_n| + |\mathcal{B}_n| = 2|\mathcal{A}_n|$,

puis $|\mathcal{A}_n| = \frac{|\mathcal{S}_n|}{2} = \frac{n!}{2}$.

2. Soit $n \in \mathbb{N}^*$. Déterminer les morphismes de groupes de $(\mathcal{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

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.

Remarque 4.1.1 1. Dans un anneau $(A, +, \times)$ on note $-x$ le symétrique de x pour $+$.

2. **Attention** : a priori un élément n'a pas de symétrique pour $\times$, donc la notation x^{-1} n'a pas de sens en général.

Exemple 4.1.1 1. $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ sont des anneaux commutatifs.

2. $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

3. $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ est un anneau commutatif, d'unité la fonction constante de valeur 1 et l'élément neutre additif la fonction constante nulle.

4. $\mathcal{M}_n(\mathbb{R})$ est un anneau, non commutatif si $n > 1$. L'unité est I_n et d'élément neutre additif 0_n .

5. $(GL_n(\mathbb{R}), +, \cdot)$ n'est pas un anneau. En effet I_n et $-I_n$ sont dans $GL_n(\mathbb{R})$ et $I_n + (-I_n) = 0$, qui n'est pas dans $GL_n(\mathbb{R})$.

4.2 Révisions de sup sur le calcul dans un anneau et les éléments inversibles

Remarque 4.2.1 Soit $(A, +, \times)$ un anneau.

1. On a les règles de calcul

(a) $\forall a \in A, a \times 0_A = 0_A \times a = 0_A$.

(b) $\forall (a, b) \in A^2, (-a) \times b = a \times (-b) = -ab$.

2. Pour $a \in A$ et $n \in \mathbb{N}$, on note :

$$(a) \quad na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ fois}} & \text{si } n \neq 0 \\ 0_A & \text{si } n = 0 \end{cases}.$$

$$(b) \quad (-n)a = n(-a) = \underbrace{(-a) + \cdots + (-a)}_{n \text{ fois}} \text{ si } n \neq 0.$$

$$(c) \quad a^n = \begin{cases} \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}} & \text{si } n \neq 0 \\ 1_A & \text{si } n = 0 \end{cases}.$$

Proposition 4.2.1 (Binôme de Newton) Dans un anneau $(A, +, \times)$, lorsque deux éléments a et b commutent ($a \times b = b \times a$) 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. $\forall (n, p) \in (\mathbb{N}^*)^2, \forall (a_1, \dots, a_n) \in A^n, \forall (b_1, \dots, b_p) \in A^p,$

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

3. Si $\underline{ab = ba}$ alors :

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

Remarque 4.2.2 Quand vous devez calculer $\left(\sum_{i=1}^n a_i \right) \left(\sum_{i=1}^n b_i \right)$, il est conseillé de changer le nom de la variable de la deuxième somme : $\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^n b_j \right)$. Cela évite les confusions avec les indices, car les indices de ces deux sommes sont complètement indépendants.

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) L'ensemble des éléments inversibles d'un anneau est un groupe pour le produit.

En d'autres termes : 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.

Remarque 4.2.3 L'élément neutre du groupe $(\mathcal{U}(A), \times)$ est : 1_A .

Exemple 4.2.1 1. Les inversibles de $\mathbb{Z}$ sont 1 et -1 .

2. Les inversibles de $\mathbb{K}[X]$ sont les constantes non nulles.

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 1. L'ensemble $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

2. L'ensemble des matrices triangulaires supérieures est un anneau en tant que sous-anneau de $\mathcal{M}_n(\mathbb{K})$.

3. L'ensemble $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. Quels sont ses inversibles ?

- $(\mathbb{Z}[i], +)$ est un sous-groupe de $(\mathbb{C}, +)$, car :
 - $0 = 0 + i0 \in \mathbb{Z}[i]$.
 - Soient $a + ib$ et $a' + ib'$ dans $\mathbb{Z}[i]$, avec $a, b, a', b' \in \mathbb{Z}$. On a : $(a + ib) - (a' + ib') = (a - a') + i(b - b') \in \mathbb{Z}[i]$.
- Soient $a + ib$ et $a' + ib'$ dans $\mathbb{Z}[i]$, avec $a, b, a', b' \in \mathbb{Z}$. On a : $(a + ib) \times (a' + ib') = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i]$.
- $1 = 1 + i0 \in \mathbb{Z}[i]$.

4. L'ensemble des applications continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-anneau de l'anneau des applications de $\mathbb{R}$ dans $\mathbb{R}$.
5. L'ensemble des suites bornées, l'ensemble des suites périodiques, sont des sous-anneaux de $\mathbb{R}^{\mathbb{N}}$.

4.4 Produit d'anneaux

Proposition 4.4.1 (Produit de deux anneaux) Soit $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. On définit deux lois de composition interne $+$ et $\times$ sur $A \times B$ en posant :

$$\forall (a_1, a_2) \in A^2, \forall (b_1, b_2) \in B^2, (a_1, b_1) + (a_2, b_2) = (a_1 +_A a_2, b_1 +_B b_2), (a_1, b_1) \times (a_2, b_2) = (a_1 \times_A a_2, b_1 \times_B b_2).$$

Alors $(A \times B, +, \times)$ est un anneau. appelé **anneau produit**.

Démonstration :

- Grâce aux propriétés d'un groupe produit, $(A \times B, +)$ est un groupe abélien.
- Comme pour les groupes produits, on montre que $\times$ est une loi associative.
- $(1_A, 1_B)$ est l'élément unité.
- $\forall (x, y, z, x', y', z') \in A^3 \times B^3, (x, x') \times ((y, y') + (z, z')) = (x, x') \times (y +_A z, y' +_B z') = (x \times_A (y +_A z), x' \times_B (y' +_B z')) = (x \times_A y +_A x \times_A z, x' \times_B y' +_B x' \times_B z') = (x \times_A y, x' \times_B y') + (x \times_A z, x' \times_B z') = (x, x') \times (y, y') + (x, x') \times (z, z').$

De même on montre que :

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

Définition 4.4.1 (Produit fini d'anneaux) Soient $(A_1, +_1, \times_1), \dots, (A_n, +_n, \times_n)$ n anneaux. Soit $+$ et $\times$ les lois de composition interne définies sur $A_1 \times \dots \times A_n$ par :

$$\begin{aligned} \forall (x_1, y_1, \dots, x_n, y_n) \in A_1^2 \times \dots \times A_n^2, \\ (x_1, \dots, x_n) + (y_1, \dots, y_n) &= (x_1 +_1 y_1, \dots, x_n +_n y_n), \\ (x_1, \dots, x_n) \times (y_1, \dots, y_n) &= (x_1 \times_1 y_1, \dots, x_n \times_n y_n). \end{aligned}$$

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

Exemple 4.4.1 Soient A et B deux anneaux commutatifs. Déterminer $\mathcal{U}(A \times B)$.

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 $f : A \rightarrow B$ respectant les structures d'anneaux, c'est-à-dire vérifiant :

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

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

Exemple 4.5.1 Quels sont les morphismes d'anneaux de $(\mathbb{R}, +, \times)$ dans $(\mathbb{R}, +, \times)$?

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

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

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

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

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

Remarque 4.5.1 Un noyau n'est jamais vide. En effet, il contient toujours au moins 0_A , car f est notamment un morphisme de groupe de $(A, +_A)$ dans $(B, +_B)$.

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

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

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.

Exemple 4.5.2 Soient m et n dans $\mathbb{N}^*$, avec $n \neq m$.

Montrer qu'il n'existe pas d'isomorphisme d'anneaux f de $\mathbb{Z}^n$ dans $\mathbb{Z}^m$, on pourra s'aider de $M_n = \{X \in \mathbb{Z}^n, X^2 = (1, \dots, 1)\}$.

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. $\forall (a, b) \in A^2, ab = 0 \implies [(a = 0) \text{ ou } (b = 0)]$.

Ceci équivaut à : si $a \neq 0$ et $b \neq 0$ alors $ab \neq 0$.

Remarque 4.6.1 1. Dans un anneau intègre, on peut donc simplifier ; si a est non nul, alors $ax = ay \implies x = y$.

2. *ATTENTION*, on ne peut pas effectuer des simplifications dans tous les anneaux. Par exemple dans $\mathcal{M}_2(\mathbb{R})$, on a : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, mais $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$. Ainsi on ne peut pas simplifier par $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
3. (IMPORTANT) Un x de $A \setminus \{0\}$ est dit diviseur de zéro s'il existe y dans $A \setminus \{0\}$ tels que $x \times y = 0_A$. Un tel diviseur de zéro n'est pas inversible.

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. $\mathbb{Z}$ et $\mathbb{K}[X]$ ne sont pas des corps.
3. Par contre $(\mathbb{K}(X), +, \times)$ est un corps.
4. Tout anneau intègre fini A est un corps.

5. Soit $(\mathbb{K}, +, \times)$ un corps. Soit $f : (\mathbb{K}, +, \times) \rightarrow (\mathbb{K}, +, \times)$ un morphisme d'anneau (un corps peut être vu comme un anneau). Montrer que f est injective.

6. Soit $(\mathbb{K}, +, .)$ un corps.

- (a) Soit $P : x \mapsto \sum_{k=0}^n a_k x^k$, avec $a_0, \dots, a_{n-1} \in \mathbb{K}$ et $a_n \in \mathbb{K} \setminus \{0\}$, qui est une fonction dite polynomiale. Montrer que P s'annule au plus n sur $\mathbb{K}$.
- (b) Si $\mathbb{K}$ est fini, alors $(\mathbb{K}^*, \times)$ est cyclique.
- (a)

(b) Si on note $G = \mathbb{K}^*$ et n son cardinal, en reprenant l'exemple 3.4.3, on a bien $|G_d| \leq d$ pour tout diviseur d de n , car grâce à ce qui précède, il y a au plus d éléments de $\mathbb{K}$ tel que $x^d = 1$. Ainsi G est cyclique.

Remarque 4.6.2 1. Tout corps commutatif est un anneau intègre. La réciproque est fausse : $(\mathbb{Z}, +, \times)$ est intègre mais pas un corps.

2. $\mathcal{U}(\mathbb{K}) = \mathbb{K}^*$.

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 1. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est un sous-corps de $\mathbb{C}$ (pour les lois $+$ et $\times$ usuelles).

2. Tout sous-corps $\mathbb{K}$ de $\mathbb{C}$ contient $\mathbb{Q}$.

En effet 1 est dans $\mathbb{K}$. Comme $\mathbb{K}$ est stable par addition, alors : $\forall n \in \mathbb{N}^*, n = \underbrace{1 + \dots + 1}_{n \text{ fois}} \in \mathbb{K}$. Comme $\mathbb{K}$ contient 0 et que $\mathbb{K}$ est stable par passage à l'opposé, alors $\mathbb{Z} \subset \mathbb{K}$.

Ensuite pour $q \in \mathbb{Z}^*$, par stabilité par passage à l'inverse, on a : $\frac{1}{q} \in \mathbb{K}$, puis passe stabilité par multiplication : $\forall p \in \mathbb{Z}, \forall q \in \mathbb{Z}^*, \frac{p}{q} = p \times \frac{1}{q} \in \mathbb{K}$.

4.7 Idéal d'un anneau commutatif

4.7.1 Définition et premières propriétés

Soit $(A, +, \times)$ un anneau **commutatif**. Pour $x, y \in A$, on notera aussi $xy = x \times y$.

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 : $\forall x \in I, \forall a \in A, xa = ax \in I$.

Exemple 4.7.1 1. Exemples d'idéaux de A :

2. Si un idéal I de A contient un élément x inversible, alors :

3. Soit A un anneau commutatif. Si I est un idéal de A , on note $R(I) = \{x \in A, \exists n \in \mathbb{N}, x^n \in I\}$.

Montrer que $R(I)$ est un idéal de A contenant I .

Remarque 4.7.1 (IMPORTANT) Soit I_1 et I_2 deux idéaux de A , alors $I_1 + I_2 = \{x + y, x \in I_1, y \in I_2\}$ est un idéal de A .

- $(I_1 + I_2, +)$ est un sous-groupe de $(A, +)$:
 - I_1 et I_2 étant des idéaux de A , ce sont des sous-groupes de $(A, +)$ et ils contiennent donc 0. Ainsi : $0 = \underbrace{0}_{\in I_1} + \underbrace{0}_{\in I_2} \in I_1 + I_2$.
 - Soit $x, y \in (I_1 + I_2)$. Il existe donc $a_1, b_1 \in I_1$ et $a_2, b_2 \in I_2$ tels que $x = a_1 + a_2$ et $y = b_1 + b_2$. Ainsi $x - y = (a_1 - b_1) + (a_2 - b_2)$. Or $a_1 - b_1$ est dans I_1 et $a_2 - b_2$ est dans I_2 , car $(I_1, +)$ et $(I_2, +)$ sont des sous-groupes de $(A, +)$. Donc $x - y$ est dans $I_1 + I_2$.
- Soit $z \in I_1 + I_2$. Il existe $a_1 \in I_1$ et $a_2 \in I_2$ tels que $z = a_1 + a_2$. Soit $a \in A$. On a $az = a_1a + a_2z$. Comme I_1 et I_2 sont des idéaux, alors a_1z et a_2z sont respectivement dans I_1 et I_2 . Ainsi az est dans $I_1 + I_2$.

On peut montrer de même que la somme $I_1 + \dots + I_n$ de n idéaux est encore un idéal par récurrence.

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 $\text{Ker } f$ est un idéal de A .

Démonstration :

Remarque 4.7.2 Attention, $\text{Ker } (f)$ n'est pas anneau un sous-anneau de A , car 1_A n'est pas dans $\text{Ker } (f)$, car $f(1_A) = 1_B \neq 0_B$.

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 .

Démonstration : Montrons d'abord que $(xA, +)$ est un sous-groupe de $(A, +)$.

L'application $f : \begin{cases} (A, +) & \rightarrow (A, +) \\ a & \mapsto xa \end{cases}$ est un morphisme de groupe :

$\forall a, b \in A, f(a + b) = x(a + b) = xa + xb = f(a) + f(b)$. Ainsi $\text{Im } (f) = xA$ est un sous-groupe de $(A, +)$.

Soient $y \in xA$ et $z \in A$. Il existe $a \in A$ tel que $y = xa$ et donc $yz = x(az)$ qui est dans xA .

Remarque 4.7.3 Soient $a_1, \dots, a_n \in I$. L'idéal engendré par $a_1, \dots, a_n$ est $a_1A + \dots + a_nA$ qui est bien un idéal grâce à la proposition précédente et la remarque 4.7.1.

Exemple 4.7.2 Un idéal I d'un anneau commutatif A , avec $A \neq \{0\}$ est dit premier si : $\forall x, y \in A, xy \in I \Rightarrow (x \in I) \text{ OU } (y \in I)$. On suppose que tout idéal de A est premier. Montrer que A est intègre puis que A est un corps.

Définition 4.7.2 (Divisibilité dans un anneau intègre) Soit $(A, +, \times)$ un anneau commutatif et intègre. Soient $a, b \in A$. On dit que b divise a s'il existe q dans A tel que : $a = bq$. On dit aussi que a est multiple de b .

Proposition 4.7.3 (Lien entre divisibilité et idéaux) Soit $(A, +, \times)$ un anneau commutatif et intègre. Soient $a, b \in A$. Alors b divise a si et seulement si $aA \subset bA$.

Démonstration : • On suppose que b divise a . Ainsi il existe q dans A tel que : $a = bq$.

On a : $\forall x \in A, ax = b(qx) \in bA$. Ainsi $aA \subset bA$.

• On suppose $aA \subset bA$.

On a $a = a \times 1_A \in aA \subset bA$. Ainsi il existe $q \in A$ tel que $a = bq$.

Proposition 4.7.4 (Idéaux de $\mathbb{Z}$) Les idéaux de l'anneau $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.

Démonstration : Soit I un idéal de $\mathbb{Z}$. Comme $(I, +)$ est un sous-groupe de $\mathbb{Z}$, alors grâce à la proposition 3.1.5, il existe $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.

Réciproquement, soit $n \in \mathbb{N}$, alors $n\mathbb{Z}$ est bien un idéal de $\mathbb{Z}$ grâce à la proposition 4.7.2.

Exemple 4.7.3 1. Montrer que tous les idéaux de l'anneau $D = \left\{ \frac{x}{10^n}, x \in \mathbb{Z}, n \in \mathbb{N} \right\}$ sont engendré par un élément.

2. On reprend l'exemple 4.7.1. Ici $A = \mathbb{Z}$. Déterminer l'ensemble des entiers naturels n non nuls tels que $R(n\mathbb{Z}) = n\mathbb{Z}$.

Proposition 4.7.5 (Définition du PGCD dans $\mathbb{Z}$) Soient $a, b \in \mathbb{N}^*$. Alors $d = a \wedge b$ est l'entier naturel tel que : $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Proposition 4.7.6 (Définition du PGCD dans $\mathbb{Z}$) Soient $a_1, \dots, a_n \in \mathbb{N}^*$, avec $n \in \mathbb{N}^*$. Alors $d = a_1 \wedge \dots \wedge a_n$ est l'entier naturel tel que : $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$.

Démonstration :

Exemple 4.7.4 Soit $(I_n)_{n \in \mathbb{N}}$ une suite d'idéaux de $\mathbb{Z}$ non nuls telle que : $\forall n \in \mathbb{N}, I_n \subset I_{n+1}$. Montrer qu'il existe $n_0 \in \mathbb{N}$ tel que : $\forall n \geq n_0, I_n = I_{n_0}$.

Proposition 4.7.7 (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).

Démonstration :

Exemple 4.7.5 1. L'idéal $\{P \in \mathbb{C}[X], P(i) = P(1) = 0\}$ est bien de la forme $(X - i)(X - 1)\mathbb{C}[X]$.

2. On rappelle d'un idéal I d'un anneau A est dit premier si :

$\forall x, y \in A, xy \in I \Rightarrow (x \in I) \text{ OU } (y \in I)$. Quels sont les idéaux premiers de $\mathbb{K}[X]$ différents de $\{0\}$ et de $\mathbb{K}[X]$?

Soit I un idéal premier de $\mathbb{K}[X]$ différent de $\{0\}$ et de $\mathbb{K}[X]$. Il existe donc $P \in \mathbb{K}[X]$ (non nul et non constant) tel que $I = P\mathbb{K}[X]$. On suppose que P n'est pas irréductible. Il existe donc A, B non associés à P tels que $P = AB$. On a donc $AB \in I$, puis A est dans I ou B est dans I . Ainsi $P|A$ ou $P|B$. Mais comme $A|P$ et $B|P$, alors A ou B est associé à P , ce qui est absurde. Ainsi P est irréductible.

Réciproquement soit P un polynôme irréductible tel que $I = P\mathbb{K}[X]$.

Soient $R, S \in \mathbb{K}[X]$ tels que : $RS \in I$. On a donc $P|RS$. Ainsi comme P est irréductible, il est dans la décomposition en facteur premier de RS , donc de R ou S , puis $P|R$ ou $P|S$, puis $R \in I$ ou $S \in I$, donc I est un idéal premier.

Remarque 4.7.4 De la même manière, on montre que les idéaux premiers de $\mathbb{Z}$ différents de $\{0\}$ et $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$, avec p un nombre premier.

Proposition 4.7.8 (Définition du PGCD dans $\mathbb{K}[X]$) Soient $A_1, \dots, A_n \in \mathbb{K}[X]$ non nuls, alors $D = A_1 \wedge \dots \wedge A_n$ est le polynôme unitaire tel que $A_1\mathbb{K}[X] + \dots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$.

Démonstration : Copier la preuve de 4.7.6.

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

4.8.1 Structure d'anneau, corps

Proposition 4.8.1 (L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$) L'ensemble $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Démonstration : • Nous avons vu dans la proposition 3.1.1 que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

• La loi $\times$ définie sur $\mathbb{Z}/n\mathbb{Z}$ est interne.

• Prouvons l'associativité de la multiplication. Soit a, b, c trois entiers relatifs. Alors :

$$\begin{aligned} \bar{a} \times (\bar{b} \times \bar{c}) &= \bar{a} \times \overline{b \times c} \quad \text{par définition} \\ &= \overline{a(bc)} \quad \text{par définition} \\ &= \overline{(ab)c} \quad \text{par associativité de la multiplication usuelle dans } \mathbb{Z} \\ &= \overline{ab} \times \bar{c} = (\bar{a} \times \bar{b}) \times \bar{c} \quad \text{par définition.} \end{aligned}$$

• Prouvons la distributivité de $\times$ sur $+$ dans $\mathbb{Z}/n\mathbb{Z}$. Soit $(a, b, c) \in \mathbb{Z}^3$. Alors :

$$\begin{aligned} \bar{a} \times (\bar{b} + \bar{c}) &= \bar{a} \times \overline{b + c} \quad \text{par définition de } + \\ &= \overline{a(b + c)} \quad \text{par définition de } \times \\ &= \overline{ab + ac} \quad \text{par distributivité usuelle dans } \mathbb{Z} \\ &= \overline{ab} + \overline{ac} \quad \text{par définition de } + \\ &= \bar{a} \times \bar{b} + \bar{a} \times \bar{c} \quad \text{par définition de } \times. \end{aligned}$$

• La loi $\times$ est commutative car pour tous entiers a, b de $\mathbb{Z}$:

$$\begin{aligned}
\bar{a} \times \bar{b} &= \overline{ab} \quad \text{par définition} \\
&= \overline{ba} \quad \text{par commutativité du produit usuel dans } \mathbb{Z} \\
&= \bar{b} \times \bar{a} \quad \text{par définition.}
\end{aligned}$$

- Le neutre pour la loi $\times$ est $\bar{1}$ car pour tout $a \in \mathbb{Z}$: $\bar{a} \times \bar{1} = \overline{a \cdot 1} = \bar{a}$ et de même $\bar{1} \times \bar{a} = \bar{a}$.

Proposition 4.8.2 (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.*

Si p est premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Démonstration :

Exemple 4.8.1 1. Soient p un nombre premier impair et $Z = \{\bar{x}^2, \bar{x} \in \mathbb{F}_p\}$.

- Déterminer $\text{card}(Z)$.
- Montrer que si $p \equiv 3[4]$, alors : $\overline{-1} \notin Z$.
- Montrer qu'il existe $x, y \in \mathbb{Z}$ tels que $\bar{x}^2 + \bar{y}^2 + \bar{1} = \bar{0}$.

2. Montrer que : p est premier si et seulement si $(p-1)! \equiv -1[p]$.

Théorème 4.8.1 (Théorème chinois) 1. Soit $(m, n) \in (\mathbb{N}^*)^2$. Si m et n sont premiers entre eux, alors les anneaux $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/(mn)\mathbb{Z}$ sont isomorphes, via l'application

$$\varphi : \begin{cases} \mathbb{Z}/(mn)\mathbb{Z} & \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{k} & \mapsto (\tilde{k}, \hat{k}) \end{cases},$$

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

2. Plus généralement, pour $k \in \mathbb{N}^*$ et $n_1, \dots, n_k$ dans $\mathbb{N}^*$ deux à deux premiers entre eux. Alors

$$\varphi : \begin{cases} \mathbb{Z}/(n_1 \dots n_k)\mathbb{Z} & \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ \bar{m} & \mapsto (\bar{m}^1, \dots, \bar{m}^k) \end{cases},$$

est un isomorphisme, avec $\bar{m}^l$ la classe de m dans $\mathbb{Z}/n_l\mathbb{Z}$.

Démonstration :

- φ est bien définie car pour $k_1, k_2 \in \mathbb{Z}$ représentant la même classe dans $\mathbb{Z}/(mn)\mathbb{Z}$: $\bar{k}_1 = \bar{k}_2$, il faut montrer que :
 $\varphi(\bar{k}_1) = \varphi(\bar{k}_2)$. On a : $mn|(k_1 - k_2)$, donc : $m|(k_1 - k_2)$ et $n|(k_1 - k_2)$, puis : $\tilde{k}_1 = \tilde{k}_2$ et $\hat{k}_1 = \hat{k}_2$.
 • φ est bien un morphisme d'anneaux, car $\widetilde{(k+l)} = (\tilde{k} + \tilde{l})$ et $\widehat{(k+l)} = (\hat{k} + \hat{l})$, grâce aux opérations sur $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ainsi $\varphi(\overline{k+l}) = \varphi(\bar{k}) + \varphi(\bar{l})$.
 $(\tilde{k}\tilde{l}, \hat{k}\hat{l}) = (\tilde{k} \times \tilde{l}, \hat{k} \times \hat{l}) = (\tilde{k}, \hat{k}) \times (\tilde{l}, \hat{l})$, grâce aux opérations sur $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ainsi $\varphi(\overline{kl}) = \varphi(\bar{k}) \times \varphi(\bar{l})$.
 $\varphi(\bar{1}) = (\tilde{1}, \hat{1})$.
 • C'est un isomorphisme :

2. Le résultat se montre par récurrence. Pour $k = 2$, le résultat est vrai.

Soit $k \geq 2$ et on suppose le résultat. Soient

$$\varphi : \begin{cases} \mathbb{Z}/(n_1 \dots n_k n_{k+1})\mathbb{Z} & \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}/n_{k+1}\mathbb{Z} \\ \bar{m} & \mapsto (\bar{m}^1, \dots, \bar{m}^k, \bar{m}^{k+1}) \end{cases}$$

et

$$\psi : \begin{cases} \mathbb{Z}/(n_1 \dots n_k)\mathbb{Z} & \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ \bar{m} & \mapsto (\bar{m}^1, \dots, \bar{m}^k) \end{cases},$$

qui est un isomorphisme d'anneaux. Soit $F : \begin{cases} \mathbb{Z}/(n_1 \dots n_k n_{k+1})\mathbb{Z} & \rightarrow \mathbb{Z}/n_1 \dots n_k n_k \mathbb{Z} \times \mathbb{Z}/n_{k+1}\mathbb{Z} \\ \bar{k} & \mapsto (\tilde{k}, \hat{k}) \end{cases}$,

qui est un isomorphisme d'anneau grâce au premier point, car $n_1 \dots n_k$ et n_{k+1} sont premiers entre eux.

L'application $G : \begin{cases} \mathbb{Z}/n_1 \dots n_k n_k \mathbb{Z} \times \mathbb{Z}/n_{k+1}\mathbb{Z} & \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}/n_{k+1}\mathbb{Z} \\ (\bar{a}, \bar{b}^{k+1}) & \mapsto (\psi(\bar{a}), \bar{b}^{k+1}) = (\bar{a}^1, \dots, \bar{a}^k, \bar{b}^{k+1}) \end{cases}$ est bijective, car ψ l'est. Ainsi $\varphi = G \circ F$ est donc bijective et donne le résultat pour $k+1$.

Corollaire 4.8.1 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

$$(S) : \begin{cases} k_0 \equiv a[m] \\ k_0 \equiv b[n] \end{cases}$$

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

Démonstration : C'est la retraduction en terme de congruence de l'isomorphisme de la proposition précédente. Avec les notations de celle-ci, le système est équivalent à $\varphi(\bar{k}_0) = (\tilde{a}, \hat{b})$ et donc $\bar{k}_0 = \varphi^{-1}((\tilde{a}, \hat{b}))$, ce qui donne une seule solution modulo mn .

Remarque 4.8.1 1. (IMPORTANT) Comment trouver une solution k_0 de (S) ?

On cherche $u, v \in \mathbb{Z}$ vérifiant la relation de Bézout : $mu + nv = 1$. On constate que : $\widehat{mu} + nv = \tilde{1}$, soit $\widehat{nv} = \tilde{1}$ et donc $\widehat{anv} = \tilde{a}$. De même $\widehat{mu} + nv = \hat{1}$, soit $\widehat{mu} = \hat{1}$ et donc $\widehat{bmu} = \hat{b}$. Comme $bmu = \tilde{0}$ (bmu est divisible par m) et $\widehat{anv} = \hat{0}$ (anv est divisible par v), alors $k_0 = bmu + anv$ convient.

2. Ainsi dans le théorème chinois, on a $\varphi^{-1} : \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \rightarrow \mathbb{Z}/mn\mathbb{Z} \\ (\tilde{a}, \hat{b}) & \rightarrow \overline{bmu + anv} \end{cases}$, en reprenant les notations précédentes.
3. Le théorème chinois permet de ramener l'étude d'une équation sur $\mathbb{Z}/l\mathbb{Z}$, lorsque l n'est pas premier, à celles d'équation plus simples dans $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, avec $l = mn$.

Exemple 4.8.2 1. Résoudre $(S) : \begin{cases} x \equiv 9[17] \\ x \equiv 2[15] \end{cases}$

Nous avons vu dans l'exemple 1.4.5 la relation de Bézout : $15 \times 8 + 17 \times (-7) = 1$. On pose $x_0 = 15 \times 8 \times 9 + 17 \times (-7) \times 2 = 120 \times 9 - 119 \times 2$. Ainsi : $x_0 \equiv 15 \times 8 \times 9[17]$ et $x_0 \equiv 17 \times (-7) \times 2[15]$. Mais la relation de Bézout nous donne $15 \times 8 \equiv 1[17]$ et $17 \times (-7) \equiv 1[15]$, donc $x_0 \equiv 9[17]$ et $x_0 \equiv 2[15]$. On calcule : $x_0 = 1080 - 238 = 842$. En concluant comme dans l'exemple 1.4.5, on trouve que l'ensemble des solutions est $\{842 + 255k, k \in \mathbb{Z}\}$.

2. On considère $f : \begin{cases} \mathbb{Z}/255\mathbb{Z} & \rightarrow \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \\ \bar{k} & \mapsto (\tilde{k}, \hat{k}) \end{cases}$, la projection comme dans le théorème chinois, alors $f^{-1}(\tilde{a}, \hat{b}) = \overline{120a - 119b}$, pour $(\tilde{a}, \hat{b}) \in \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, grâce au calcul de l'exemple précédent.
3. Le groupe $(\mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}, +)$ est-il cyclique ?

4. Résoudre dans $\mathbb{Z}/143\mathbb{Z} : x^2 + x + \overline{11} = \bar{0}$ (on remarquera que $143 = 11 \times 13$).

Proposition 4.8.3 (Éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$) *L'élément $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ pour $\times$ si et seulement si k est premier avec n .*

Démonstration :

1. Si $\bar{k}$ est inversible, alors il existe un entier k' tel que $\overline{kk'} = \bar{1}$, c'est-à-dire $kk' \equiv 1[n]$, soit encore $kk' - qn = 1$ pour un certain $q \in \mathbb{Z}$. D'après le théorème de Bézout : $k \wedge n = 1$.
2. Si $k \wedge n = 1$, alors il existe des entiers u et v tels que $ku + nv = 1$, donc $ku \equiv 1[n]$, d'où $\bar{k}\bar{u} = \bar{1}$: ainsi $\bar{k}$ est inversible.

Remarque 4.8.2 *La démarche de la preuve précédente dans le sens retour nous permet de trouver un inverse de $\bar{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 4.8.3 1. (a) *Expliciter $\mathcal{U}(\mathbb{Z}/20\mathbb{Z})$.*

(b) *Soit $\varphi : \begin{cases} \mathbb{Z}/20\mathbb{Z} & \rightarrow \mathbb{Z}/20\mathbb{Z} \\ x & \mapsto \bar{13}x + \bar{2} \end{cases}$. Montrer que φ est bijectif et déterminer φ^{-1} .*

(c) *Montrer que le groupe $\mathcal{U}(\mathbb{Z}/20\mathbb{Z})$ est engendré par $\bar{3}$ et $\bar{11}$.*

(d) *En déduire un isomorphisme de groupes entre $(\mathcal{U}(\mathbb{Z}/20\mathbb{Z}), \times)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$.*

2. *Montrer qu'il n'existe pas $n \geq 2$ tel que $n \mid (2^n - 1)$, en considérant p le plus petit diviseur premier de n .*

4.8.2 Indicatrice d'Euler

Définition 4.8.1 (Fonction indicatrice d'Euler) On appelle fonction indicatrice d'Euler la fonction $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ qui à n associe le nombre $\varphi(n)$ d'entiers de l'intervalle $\llbracket 1, n \rrbracket$ premiers avec n . Autrement dit, pour $n \in \mathbb{N}^*$, on a : $\varphi(n) = \text{card}\{k \in \llbracket 1, n \rrbracket, k \wedge n = 1\}$.

Remarque 4.8.3 (IMPORTANT) D'après proposition 4.8.3, $\varphi(n)$ est le cardinal du groupe $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. Ainsi : $\text{card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z})) = \varphi(n)$.

Proposition 4.8.4 (Relations sur φ) 1. Soient p un nombre premier et $k \in \mathbb{N}^*$. Alors

$$\varphi(p^k) =$$

2. Si n et m sont des entiers naturels premiers entre eux, alors

Démonstration :

1.

2. Les entiers n et m sont premiers entre eux, donc les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes (grâce au théorème chinois). Il en résulte que leurs groupes d'inversibles sont également isomorphes, c'est-à-dire $\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ et $\mathcal{U}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$. Ces deux ensembles ont donc le même cardinal. Grâce à l'exemple 4.4.1, on a : $\mathcal{U}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$. Or la remarque 4.8.3, nous dit que :
 $\text{card}(\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})) = \varphi(mn)$ et $\text{card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})) = \text{card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z})) \times \text{card}(\mathcal{U}(\mathbb{Z}/m\mathbb{Z})) = \varphi(n)\varphi(m)$. Par égalité des cardinaux, on en déduit que : $\varphi(nm) = \varphi(n)\varphi(m)$.

Corollaire 4.8.2 (Un théorème d'Euler) Soit k un entier premier avec n , on a dans $\mathbb{Z}/n\mathbb{Z}$: $k^{\varphi(n)} = \bar{1}$. Autrement dit $k^{\varphi(n)} \equiv 1[n]$

Démonstration :

Remarque 4.8.4 On retrouve le petit théorème de Fermat. Soit p est un nombre premier. On a donc $\varphi(p) = p - 1$, grâce à l'exemple 4.8.4. Pour tout k dans $\mathbb{Z}$, si $k \wedge p = 1$, alors le corollaire précédent nous donne : $k^{\varphi(p)} \equiv 1[p]$, puis : $k^{p-1} \equiv 1[p]$ et donc $k^p \equiv k[p]$. Cette relation reste valable pour tout k dans $\mathbb{Z}$, car si k n'est pas premier avec p , alors comme p est premier, ce dernier intervient dans la décomposition en facteurs premiers de k et donc : $p|k$, puis : $k^p \equiv 0[p]$ et $k \equiv 0[p]$, puis $k^p \equiv k[p]$.

Proposition 4.8.5 (Calcul de $\varphi(n)$) 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 :

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

Démonstration : Grâce à la proposition 4.8.4, on montre par récurrence sur q , que :

$\varphi(p_1^{k_1} p_2^{k_2} \cdots p_q^{k_q}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_q^{k_q}) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \cdots p_q^{k_q-1}(p_q - 1)$, grâce à la proposition 4.8.4.

Exemple 4.8.4 1. Trouver un $r \in \mathbb{N}^*$ tel que $11^r \equiv 1[720]$.

2. Soient $p_1 < p_2 < \dots < p_r$ des nombres premiers et $n = \prod_{i=1}^r p_i$. Montrer que :

$$\forall a \in \mathbb{Z}, \forall k \in \mathbb{Z}, a^{1+k\varphi(n)} \equiv a[n].$$

3. Déterminer les $n \geq 2$ tels que $\varphi(n)|n$.

4. Soit $n \in \mathbb{N}^*$.

(a) Soit d un diviseur de n . Dans $\mathbb{U}_n$, montrer que tout élément d'ordre d est inclus dans $\mathbb{U}_d$ et en déduire qu'il y exactement $\varphi(d)$ éléments d'ordre d .

(b) Montrer que $n = \sum_{d|n} \varphi(d)$.

5 Compléments : les nombres algébriques

Soient $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, α un nombre complexe non nul, et on pose $\mathbb{K}[\alpha] = \{Q(\alpha), Q \in \mathbb{K}[X]\}$, qui est un $\mathbb{K}$ -espace vectoriel. On pose enfin $I_{\mathbb{K}}(\alpha) = \{Q \in \mathbb{K}[X], Q(\alpha) = 0\}$. Si on a : $I_{\mathbb{K}}(\alpha) \neq \{0\}$, on dit que α est $\mathbb{K}$ -algébrique, ce que l'on suppose dans la suite.

Dans le cas contraire, on dit que α est transcendant sur $\mathbb{K}$.

1. Donner l'exemple d'un nombre irrationnel $\mathbb{Q}$ -algébrique.
2. On suppose que α est algébrique. Montrer qu'il existe un unique polynôme unitaire $P \in \mathbb{K}[X]$ tel que $I_{\mathbb{K}}(\alpha) = \{PQ, Q \in \mathbb{K}[X]\}$. Montrer que P est irréductible.

Ce polynôme P sera noté $P_{\mathbb{K}}(\alpha)$ et appelé polynôme $\mathbb{K}$ -minimal de α .

3. Montrer que les racines complexes de P sont simples.

4. Montrer que le degré de $P_{\mathbb{K}}(\alpha)$ vaut $\dim_{\mathbb{K}}(\mathbb{K}[\alpha])$.

5. Montrer que $\mathbb{K}[\alpha]$ est un corps.

Montrons que $\mathbb{K}[\alpha]$ est un anneau commutatif, en montrant que c'est un sous-anneau de $\mathbb{C}$.

- Montrons que $(\mathbb{K}[\alpha], +)$ est un sous-groupe de $(\mathbb{C}, +)$:

- $0 \in \mathbb{K}[\alpha]$, grâce au polynôme nul.
- Soient $P, Q \in \mathbb{K}[X]$. On a $P(\alpha) - Q(\alpha) = (P - Q)(\alpha) \in \mathbb{K}[\alpha]$.
- Soient $P, Q \in \mathbb{K}[X]$. On a $P(\alpha)Q(\alpha) = (PQ)(\alpha) \in \mathbb{K}[\alpha]$.
- $1 \in \mathbb{K}[\alpha]$, grâce au polynôme constant 1.

La commutativité vient de la commutativité dans $\mathbb{C}$.

6. (a) Si $\mathbb{K} = \mathbb{Q}$ et que α est dans $\mathbb{Q}$ et qu'il est annulé par un polynôme $P \in \mathbb{Z}[X]$ unitaire, alors α est dans $\mathbb{Z}$.

- (b) Montrer que $U = X^3 - 3X + 1$ est irréductible sur $\mathbb{Q}$.

Supposons que U soit réductible dans $\mathbb{Q}[X]$, donc il existe $A, B \in \mathbb{Q}[X]$, non constants tels que $U = AB$. L'un de ces polynômes est de degré un et l'autre de degré deux. Le polynôme de degré un est de la forme $aX + b$, donc $-b/a$ serait une racine rationnelle de U . Grâce à la question précédente, celle-ci est dans $\mathbb{Z}$, donc il existe $p \in \mathbb{Z}$ tel que $p^3 - 3p + 1 = 0$, soit $p(3 - p^2) = 1$, donc $p|1$, donc $p = 1$ ou $p = -1$. Il est clair que 1 et -1 ne sont pas racines de U . D'où une contradiction.

7. On pose $w = e^{\frac{2i\pi}{5}}$. Déterminer la dimension du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}[\omega]$.

Montrons qu'effectivement $\sqrt{5}$ n'est pas dans $\mathbb{Q}$.

Si $\sqrt{5} = p/q$, avec p et q premiers entre eux, on a $5q^2 = p^2$. Ainsi $5|p^2$. Comme 5 est un nombre premier, alors par le lemme de Gauss, 5 divise p ou p , donc : $5|p$. Ainsi $p = 5r$, avec $r \in \mathbb{Z}$, puis : $q^2 = 5r^2$ et de même : $5|q$. Ceci contredit l'irréductibilité de p/q .

8. Soit S un polynôme, appartenant à $\mathbb{Q}[X]$, de degré $n \geq 2$, irréductible sur $\mathbb{Q}$.

(a) Démontrer qu'il existe un entier naturel C_S (différent de 0) tel que pour tout rationnel $r = \frac{p}{q}$

(le couple (p, q) appartenant à $\mathbb{Z} \times \mathbb{N}^*$) il vienne : $|S(r)| \geq \frac{1}{C_S q^n}$.

(b) Supposons que le réel α soit une racine de S . Déduire du résultat précédent l'existence d'une constante K , strictement positive, telle que pour tout rationnel $r = \frac{p}{q}$ appartenant à

l'intervalle $[\alpha - 1, \alpha + 1]$, l'inégalité $|\alpha - r| \geq \frac{K}{q^n}$ ait lieu.

(c) Soit $(t_n)_{n \in \mathbb{N}}$ la suite des réels définis par la relation : $t_n = \sum_{k=0}^n 10^{-k!}$, $n \geq 0$.

Démontrer que la suite $(t_n)_{n \in \mathbb{N}}$ est convergente ; soit t sa limite. Établir l'inégalité : $|t - t_n| \leq 2.10^{-(n+1)!}$. En déduire que le réel t (nombre de Liouville) est transcendant sur $\mathbb{Q}$.

(a) Soit C_S un dénominateur (positif) commun aux coefficients de S . Ainsi $S(x)$ s'écrit alors $S(x) = \frac{1}{C_S} \sum_{i=0}^n a_i x^i$ avec $a_i \in \mathbb{Z}$, pour $i \in [0, n]$. On a donc $S(r) = \frac{1}{C_S q^n} \sum_{i=0}^n a_i p^i q^{n-i}$, or $\sum_{i=0}^n a_i p^i q^{n-i} \in \mathbb{Z}$ et est non nul car sinon $r \in \mathbb{Q}$ serait racine de S qui ne serait pas irréductible sur $\mathbb{Q}$. On a donc $\left| \sum_{i=0}^n a_i p^i q^{n-i} \right| \geq 1$ et donc

$$|S(r)| \geq \frac{1}{C_S q^n}$$

(b) Soit $M = \sup_{t \in [\alpha-1, \alpha+1]} |S'(t)|$, l'inégalité des accroissements finis (S est continue sur $[\alpha-1, \alpha+1]$ et dérivable sur $] \alpha-1, \alpha+1[$) s'écrit : pour tout $r \in [\alpha-1, \alpha+1]$, $|S(r)| = |S(r) - S(\alpha)| \leq M|\alpha - r| \leq \max(M, 1)|\alpha - r|$ et, pour $r \in \mathbb{Q}$ en particulier, on obtient $\frac{1}{C_S q^n} \leq \max(M, 1)|\alpha - r|$.
Donc, en posant $K = \frac{1}{C_S \max(M, 1)} > 0$,

$$\exists K > 0, \forall r = \frac{p}{q} \in \mathbb{Q} \cap [\alpha-1, \alpha+1], (q > 0) \quad |\alpha - r| \geq \frac{K}{q^n}$$

(c) $\forall k \geq 1, 10^{-k!} \leq 10^{-k}$ et $(\sum 10^{-k})$ converge donc par comparaison de séries à termes positifs,

La suite des sommes partielle (t_n) converge

De plus, $\forall n \in \mathbb{N}, t - t_n = \sum_{k=n+1}^{\infty} 10^{-k!} = 10^{-(n+1)!} \sum_{k=n+1}^{\infty} 10^{(n+1)!-k!}$. Or, pour $k \geq n+2$, $k! - (n+1)! = (n+1)! \left(\prod_{i=n+2}^k i - 1 \right) \geq (n+1)!(k-1) \geq k - n - 1$, inégalité vraie aussi pour $k = n+1$, et donc :
 $0 \leq t - t_n \leq 10^{-(n+1)!} \sum_{k=n+1}^{\infty} 10^{-(k-n-1)} = 10^{-(n+1)!} \frac{1}{1 - 10^{-1}} = \frac{10}{9} 10^{-(n+1)!}$, puis :

$$|t - t_n| \leq 2.10^{-(n+1)!}$$

Supposons t algébrique de degré d , avec $d \geq 1$. Remarquons que les résultats de a. et b. sont valables pour $n = 1$ (et même pour $n = 0$) les démonstrations n'utilisant pas $n \geq 2$. En les appliquant à $S = M_t$, on a : $\exists K \in \mathbb{R}_+^*, \forall r = \frac{p}{q} \in \mathbb{Q} \cap [t-1, t+1], |t - r| \geq \frac{K}{q^d}$.

Or il existe $N \in \mathbb{N}$ tel que : $\forall n \geq N, t_n \in [t-1, t+1]$. D'autre part $t_n = \frac{p}{10^{n!}}$, avec p dans $\mathbb{N}$, donc : $\forall n \geq N, |t - t_n| \geq \frac{K}{10^{dn!}}$. Ce qui précède donne : $\forall n \geq N, 2.10^{-(n+1)!} \geq \frac{K}{10^{dn!}}$, soit $10^{-(n+1-d)n!} \geq \frac{K}{2}$. Mais $\lim_{n \rightarrow +\infty} 10^{-(n+1-d)n!} = 0$, ce qui conduit à une contradiction.

t est transcendant sur $\mathbb{Q}$

9. Soient $\alpha > \beta$ les deux racines de $P = X^2 - X - 1$. On pose $A = \mathbb{Z}[\alpha] = \{x + \alpha y, x, y \in \mathbb{Z}\}$ et $\sigma : x + \alpha y \mapsto x + \beta y$. Soit $N : z \mapsto z\sigma(z)$ défini sur A .

(a) Montrer que A est un anneau. On notera U l'ensemble des inversible de cet anneau. Montrons que A est un sous-anneau de $\mathbb{R}$.

Il est clair que A est stable par somme et par passage à l'opposé et contient 0. Donc A est un sous-groupe de $(\mathbb{C}, +)$.

$\alpha + \beta = 1$, donc $\beta = 1 - \alpha$ est dans A , par relation coefficients et racines d'un polynôme.

En outre, pour tous x, y, x', y' dans $\mathbb{Z}$,

$$(x + \alpha y) \times (x' + \alpha y') = xx' + (xy' + x'y) \alpha + yy' \alpha^2 = xx' + (xy' + x'y) \alpha + yy'(1 + \alpha) = xx' + yy' + (xy' + x'y + yy') \alpha \in A.$$

Ainsi, A est un sous-anneau de $\mathbb{R}$, donc un anneau.

- (b) Pour $u \in A$, montrer que l'écriture $u = x + \alpha y$, avec x, y dans $\mathbb{Z}$ est unique.
 Comme $\alpha = \frac{1+\sqrt{5}}{2}$, c'est un irrationnel. Sur $\mathbb{Q}$ le polynôme minimale de α est donc P , puis $\mathbb{Q}[\alpha]$ admet comme $\mathbb{Q}$ -base $(1, \alpha)$ et, de ce fait, l'écriture $u = x + \alpha y$ avec $(x, y) \in \mathbb{Z}^2$ est unique car $\mathbb{Z}[\alpha]$ est inclus dans $\mathbb{Q}[\alpha]$.

On peut donc définir $\sigma : x + \alpha y \mapsto x + \beta y$ sur A et $N : z \mapsto z\sigma(z)$.

- (c) Montrer que Id_A et σ sont les seuls automorphismes d'anneaux de A .

- (d) Soit $z \in A$. Montrer que : $z \in U \Leftrightarrow |N(z)| = 1$.

Soit $x + y\alpha \in A$ avec x et y dans $\mathbb{Z}$. On a (toujours grâce aux relations coefficients/racines) :

$$N(x + y\alpha) = (x + y\alpha)(x + y\beta) = x^2 + xy(\alpha + \beta) + y^2(\alpha\beta) = x^2 + xy - y^2 \in \mathbb{Z}.$$

De plus, pour tous z et z' dans A , $N(z z') = z z' \sigma(z z') = z z' \sigma(z) \sigma(z') = N(z) \times N(z')$.

Soit $z \in U$. Il existe $z' \in A$ tel que $z z' = 1$. On en déduit que $N(z) \times N(z') = 1$ donc $N(z)$ est un entier relatif inversible dans $\mathbb{Z}$ donc égal à 1 ou -1. Inversement si : $\pm 1 = N(z) = z\sigma(z)$ alors $\pm\sigma(z)$ est un inverse de z donc $z \in U$.

- (e) Soit $V = U \cap]1, +\infty[$. Montrer que si $z = x + \alpha y$ est dans V , alors : $x \geq 0$ et $y \geq 1$ en considérant $\{z, 1/z, -z, -1/z\}$.

Soit $z = x + \alpha y \in V$. On a : $-z \in U, z^{-1} \in U$ et $-z^{-1} \in U$ et aussi : $z \in]1, +\infty[, -z \in]-\infty, -1[, z^{-1} \in]0, 1[$ et $-z^{-1} \in]-1, 0[$. Parmi ces quatre nombres, seul le plus grand, qui est z , est dans $]1, +\infty[$. Or on a : $z > z^{-1}$ et $z > -z^{-1}$, donc : $x + \alpha y > x + \beta y = x + y - \alpha y$. Donc $0 < y(2\alpha - 1)$ donc $y > 0$ donc $y \geq 1$ puisque y est un entier.

Dans le cas où $N(z) = 1$ on a $(x + \alpha y)(x + \beta y) = 1$. Puisque $z > 0$ on a $x + \beta y > 0$ d'où $x > (-\beta)y \geq -\beta = \frac{\sqrt{5}-1}{2} > 0$.

Dans le cas où $N(z) = -1$ on a $(x + \alpha y)(x + \beta y) = -1$. Puisque $z > 1$, on a :

$$(x + \alpha y)(x + \beta y) < x + \beta y \text{ (car } x + \beta y < 0) \text{ et donc : } x + \beta y > -1 \text{ donc}$$

$$x > -1 + (-\beta)y \geq -1 - \beta > -1. \text{ Donc } x \geq 0 \text{ puisque } x \text{ est un entier.}$$

- (f) En déduire que $U \cap \mathbb{R}_+^*$ est engendré par α .