

Exercice 6:

- Déterminer tous les sous-groupes finis de $(\mathbb{C}^*, \times)$

(A) Soit G un sous-groupe de $\mathbb{C}^*$ tel que $\text{Card}(G) / n < +\infty$

Soit $x \in G$, alors $x^n = e_{\mathbb{C}^*} = 1$

Donc $x \in U_n$

Donc $G \subset U_n$

Or, $|G| = |U_n| = n$ donc $G = U_n$

(S) Montrons que $(U_n, \times)$ est un sous groupe de $(\mathbb{C}^*, \times)$

- Soit $n \geq 1$, $G = U_n = \{e^{2i\pi k/n} \mid k \in [0, n-1]\}$

- $U_n \subset \mathbb{C}^*$ (1)

- $1^n = 1 \in U$ (2)

- $\forall x, y \in U_n, \left(\frac{x}{y}\right)^n = \frac{x^n}{y^n} = 1$ donc $xy^{-1} \in U_n$ (3)

$\Rightarrow (U_n, \times)$ est un sous groupe de $(\mathbb{C}^*, \times)$

Exercice 14

1) Soient $(a_1, b_1, a_2, b_2) \in \mathbb{Z}^4$ tel que $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$

Ainsi, $a_1 - a_2 = \sqrt{2}(b_2 - b_1)$ (*)

Si $b_1 \neq b_2$, $\sqrt{2} = \frac{a_1 - a_2}{b_2 - b_1} \in \mathbb{Q}$ (or $\sqrt{2} \notin \mathbb{Q}$ car $v_2(2) = 1$ est impair donc absurde)

Alors $b_1 = b_2$ donc $a_1 = a_2$ (*)

CCL: Soit $x \in \mathbb{Z}[\sqrt{2}]$, son écriture sous la forme $a + b\sqrt{2}$
 $(a, b) \in \mathbb{Z}^2$ est unique

2) C'est clair (vérifier $\mathbb{Z}[\sqrt{2}]$ contient $0_{\mathbb{R}}$ et $1_{\mathbb{R}}$ et stable par somme torde et produit torde)

3) Analyse: Soit σ un automorphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$, alors $\sigma(1) = 1$

$$\text{Soit } n \in \mathbb{Z}, \sigma(1 \times n) = n \sigma(1) = n$$

$$\begin{aligned} \text{Soit } a, b \in \mathbb{Z}, \sigma(a + b\sqrt{2}) &= \sigma(a + 0\sqrt{2} + (0 + b\sqrt{2})) \\ &= \sigma(a) + \sigma(b\sqrt{2}) \\ &= \sigma(a) + \sigma(b)\sigma(\sqrt{2}) = a + b\sigma(\sqrt{2}) \end{aligned}$$

$$\text{Alors, } 2 = \sigma(2) = \sigma(\sqrt{2}^2) = \sigma(\sqrt{2})^2$$

$$\text{Donc } \sigma(\sqrt{2}) = \pm\sqrt{2}$$

$$\text{Si } \sigma(\sqrt{2}) = \sqrt{2} \Rightarrow \sigma \text{ est l'id} \Rightarrow \text{impossible}$$

$$\text{Donc } \sigma(\sqrt{2}) = -\sqrt{2}$$

Synthèse: Montrons que $\sigma: \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}[\sqrt{2}]$ est un iso d'anneaux.

- $\sigma(1) = 1 \rightarrow$ clair
- $\sigma(x+y) = \sigma(x) + \sigma(y)$ clair
- $\forall x, y \in \mathbb{Z}[\sqrt{2}]^2, x = a_1 + b_1\sqrt{2}, y = a_2 + b_2\sqrt{2} \quad (a_1, a_2, b_1, b_2) \in \mathbb{Z}^4$

$$\text{Alors } \sigma(xy) = (a_1a_2 + 2b_1b_2 - \sqrt{2}(a_1b_2 + a_2b_1))$$

$$\begin{aligned} \text{Et } \sigma(x)\sigma(y) &= (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 \\ &\quad - \sqrt{2}(a_1b_2 + a_2b_1) \end{aligned}$$

4) j'ai passé de bonnes vacances globalement, j'ai passé du temps avec Bingo mon chat (10 Kg) et il a mangé une grenouille car il avait un peu faim. (un peu gourmand)

5) Soit $x \in \mathbb{Z}[\sqrt{2}]$, montrons que $x \in \mathbb{Z}[\sqrt{2}]^* \Leftrightarrow N(x) = 1$

$$\boxed{\Rightarrow} \text{ Si } x \text{ est inversible, alors } N(xx^{-1}) = N(1) = 1$$

$$\text{Or } N(xx^{-1}) = N(x)N(x^{-1}) \quad (1.1 \text{ mult et } \sigma \text{ morphisme})$$

$$\text{Donc } N(x)N(x^{-1}) = 1$$

$$\text{Or, } N(x) \text{ et } N(x^{-1}) \in \mathbb{N}. \text{ Donc } \boxed{N(x) = 1}$$

☐ Si $N(x) = 1$, alors $x \sigma(x) = \pm 1$

Si $x \sigma(x) = 1 = \sigma(x) x$, alors x est inversible d'inverse $\sigma(x)$

Si $x \sigma(x) = -1 = \sigma(x) x$, alors x est inversible d'inverse $-\sigma(x)$

6) Soit $x \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$, $y \in \mathbb{Z}[\sqrt{2}]$

$\exists (q, r) \in \mathbb{Z}[\sqrt{2}]^2$ tq $y = qx + r$ et $N(r) < N(x)$

• Posons $(y_1, y_2, x_1, x_2) \in \mathbb{Z}^4$, $x = x_1 + x_2\sqrt{2} \neq 0$ et $y = y_1 + y_2\sqrt{2}$

$$\text{Alors } \frac{y}{x} = \frac{y_1 + y_2\sqrt{2}}{x_1 + x_2\sqrt{2}} = \underbrace{\frac{y_1 x_1 - 2 y_2 x_2}{x_1^2 - 2 x_2^2}}_{\in \mathbb{Q}} + \underbrace{\frac{\sqrt{2}(y_1 y_2 - x_2 y_1)}{x_1^2 - 2 x_2^2}}_{\in \mathbb{Q}} \quad q_2$$

• Soit $(a_1, a_2) \in \mathbb{Z}^2$ tels que $|q_1 - a_1| \leq \frac{1}{2}$ et $|q_2 - a_2| \leq \frac{1}{2}$

Posons $q = a_1 + \sqrt{2} a_2$

$$\begin{aligned} \text{• Alors, } N\left(\frac{y}{x}\right) &= N\left(\frac{y - qx}{x}\right) = N\left(\frac{y}{x} - q\right) \\ &= N(q_1 + \sqrt{2} q_2 - (a_1 + \sqrt{2} a_2)) \\ &= N(q_1 - a_1 + \sqrt{2}(q_2 - a_2)) \\ &= |(q_1 - a_1)^2 - 2(q_2 - a_2)^2| \leq \frac{3}{4} \end{aligned}$$

(on choisit a_1 entre q_1 et $q_1 + 1$ le plus proche de q_1)

$$\text{Ainsi, } \frac{N(y)}{N(x)} \leq \frac{3}{4} \text{ donc } N(y) \leq \frac{3}{4} N(x) < N(x)$$

7) Supposons I un idéal de $\mathbb{Z}[\sqrt{2}] \neq \{0\}$

Posons $m = \min \{N(x) : x \in I \setminus \{0\}\}$ existe par bon ordre, donc, il existe $a \in I$ $\in \mathbb{N}^*$ $N(a) = m$

Procédons par double inclusion pour montrer $I = a\mathbb{Z}[\sqrt{2}]$

☐ Claire car I est absorbant

☐ Soit $x \in I$, d'après 6), $\exists (q, r) \in \mathbb{Z}[\sqrt{2}]^2$ tels que $x = qa + r$ et $N(r) < N(a)$

Donc, $x \in I$; donc $qa \in I$; donc $r \in I$, $N(r) < N(a)$

Nécessairement, par min de $N(a)$, $r = 0$, donc $x \in a\mathbb{Z}[\sqrt{2}]$

8) $N(1+\sqrt{2}) = |1-2| = |-1| = 1$

D'après qs), $1+\sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$

9) Soit $u \in |U(\mathbb{Z}[\sqrt{2}])|$, $u > 1$

Montrons que $u \geq 1+\sqrt{2}$. Posons $u = a+b\sqrt{2}$ ($a, b \in \mathbb{Z}$)

Exercice 12:

1) Posons $\Psi \mid \begin{array}{l} \mathbb{Q}[X] \rightarrow \mathbb{C} \\ P \mapsto P(\alpha) \end{array}$. Il s'agit d'un isomorphisme d'anneaux

car:

$$\hookrightarrow \Psi(1) = 1$$

$$\hookrightarrow \forall (P, Q) \in \mathbb{Q}[X]^2, \Psi(P+Q) = (P+Q)(\alpha) = P(\alpha) + Q(\alpha)$$

$$\Psi(P \times Q) = (PQ)(\alpha) = P(\alpha)Q(\alpha)$$

Où, $\text{Ann}(\alpha) = \text{Ker}(\Psi)$ donc $\text{Ann}(\alpha)$ est un idéal de $\mathbb{Q}[X]$

2) Ψ est linéaire et $\mathbb{Q}[\alpha] = \text{Im}(\Psi)$

Donc, $\mathbb{Q}[\alpha]$ est un sev de $\mathbb{C}$ (car l'image d'un ^{est un sev} id. d'anneaux

Posons $n_p = \min(\{n \in \mathbb{N} \mid P \in \text{Ann}(\alpha), \deg(P) = n\})$ bien défini par bon ordre

Soit $P_0 \in \text{Ann}(\alpha)$ tel que $\deg(P_0) = n_p$. Montrons que

$$\mathbb{Q}[\alpha] = \text{Vect}((\alpha^k)_{k \in [0, n_p-1]})$$

[2] Évident

[3] Soit $x \in \mathbb{Q}[\alpha]$, $\exists A \in \mathbb{Q}[X]$ tel que $x = A(\alpha)$

$\exists (Q, R) \in \mathbb{Q}[X]$ tel que $A = QP_0 + R$ et $\deg(R) < \deg(P_0)$

$$A(\alpha) = Q(\alpha)P_0(\alpha) + R(\alpha) = R(\alpha)$$

$$\text{Soit } (x_0, \dots, x_{n_p-1}) \in \mathbb{Q}^{n_p} \text{ tq } R = \sum_{i=0}^{n_p-1} x_i X^i$$

$$\text{Donc } R(\alpha) = \sum_{i=0}^{n_p-1} x_i \alpha^i$$

• Posons $\Psi \mid \begin{array}{l} \mathbb{Q}[X] \rightarrow \mathbb{C} \\ P \mapsto P(\alpha) \end{array}$ un morphisme d'anneaux et $\text{Im}(\Psi)$
= $\mathbb{Q}[\alpha]$ dont sous anneau

• Inversibilité: Soit $x \in \mathbb{Q}[\alpha] \setminus \{0\}$. Posons $\Psi_x \mid \begin{array}{l} \mathbb{Q}[\alpha] \rightarrow \mathbb{Q}[\alpha] \\ y \mapsto xy \end{array}$
linéaire et deux ev de même dimension

• Injectivité: Intégrité de $\mathbb{C}$

$\hookrightarrow \Psi_x$ est bijective: $\exists! y \in \mathbb{Q}[\alpha], xy = 1$