

Leçon N° 127 : Exemples de nombres remarquables

I) Corps et nombres remarquables

1) Corps, algèbre et transcendance (les corps sont commutatifs)

Définition 1: Soit K un corps. On dit que L est une extension de K lorsque $K \subset L$.

Proposition 2: Soit $K \subset L$ une extension de corps. Alors L est un K -ev et on note $[L:K] = \dim_K L$ le degré de cette extension.

Théorème 3: (base télescopique) Soient $K \subset L \subset M$ des corps.

(e.i.) $\exists$ une base de L sur K , $(\beta_j)_{j \in J}$ une base de M sur L . Alors la famille $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ est une base de M sur K .

Corollaire 4: (multiplicativité des degrés) Avec les mêmes notations et si le degré des extensions sont finis, on a :

$$[M:K] = [M:L] \times [L:K]$$

Remarque 5: $\mathbb{Q}$ est une extension sur $\mathbb{R}$ de degré 2.

Définition 6: Soit $K \subset L$ une extension et $\alpha \in L$.

Soit $P: K[X] \rightarrow K$ le morphisme défini par $P|_K = \text{id}_K$ et $P(X) = \alpha$.

1) Si P est irréductible, on dit que α est transcendant sur K .

2) Sinon, on dit que α est algébrique sur K . Alors il existe un polynôme irréductible unitaire P tel que $P(\alpha) = 0$, qui est appelé polynôme minimal de α sur K .

Exemples 7 $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ le polynôme minimal $X^2 - 2$

1) i est algébrique sur $\mathbb{Q}$ le polynôme minimal $X^2 + 1$

3) $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ le polynôme minimal $X^3 - 2$.

Définition 8: Soit $K \subset L$ une extension et $\alpha \in L$.

1) $K[X]$ est le plus petit sous-anneau de L contenant K et X .

2) $K(\alpha)$ est le plus petit sous-corps de L contenant K et α .

Proposition 9: On a $K[X] \subset K(\alpha)$ et

$$K(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)}, P, Q \in K[X], Q(\alpha) \neq 0 \right\}$$

Théorème 10: Soient $K \subset L$ une extension et $\alpha \in L$. Les propriétés suivantes sont équivalentes :

1) α est algébrique sur K .

2) $K[X] = K(\alpha)$

3) $\dim_K K(\alpha) < +\infty$.

De plus, si P est le polynôme minimal de α , $\dim_K K(\alpha) = \deg(P)$.

Théorème 11: Soient $K \subset L$ une extension et posons $M = \{x \in L \mid x \text{ est algébrique sur } K\}$, alors M est sous-corps de L et M est algébriquement clos lorsque L l'est.

Théorème 12: (Kronecker) $\mathbb{C}$ est transcendant sur $\mathbb{R}$ AD715.

Théorème 13: (Lindemann) π est transcendant sur $\mathbb{Q}$ AD715.

2) Construction de la règle et du compas

Définition 14: Soit P_0 un ensemble de points contenant O et I . On dit qu'un point P est P_0 -élémentaire - constructible lorsque P est obtenu par intersection de deux droites géométriques appartenant aux ensembles suivants :

1) L'ensemble des droites passant par deux points distincts de P_0

2) L'ensemble des cercles centrés en un point de P_0 et dont le rayon est la distance entre deux points de P_0 .

On dit que P est de constructible lorsque $\exists$ existe un nombre fini de points $P_1, \dots, P_n = P$ tels que $\forall C \in \mathbb{R}^2, \mathbb{N}^2, P$ est de élémentaire constructible $\exists$ existe de $P_0 \cup \{P_1, \dots, P_{n-1}\}$.

Dans le suite $P_0 = \{0, 1\}$.

Proposition 15: Soient A, B, C constructibles, $A \neq B$. Alors

1) $\exists$ milieu de $[A, B]$ et sa médiatrice sont constructibles

2) $\exists$ perpendiculaire $\delta(A, B)$ passant par C est constructible

3) $\exists$ parallèle $\delta'(A, B)$ passant par C est constructible.

Corollaire 16: Soit $\odot$ un angle donné par deux demi-cercles Γ par. Alors la bissectrice de $\odot$ est constructible.

Définition 17: Un nombre complexe z est constructible lorsque $(z, \bar{z})$ l'est.

Proposition 18: L'ensemble des nombres complexes constructibles est un sous-espace de $\mathbb{C}$ contenant $\mathbb{Q}$ et stable par racine carrée. (cf Annexe 1)

Proposition 19: Soit P un point constructible élementairement, alors $\mathbb{Q}(\sqrt[n]{P})$ est un extension de $\mathbb{Q}$ de degré au plus n .

Définition 20: On dit que $K \subseteq \mathbb{C}$ est 2-décomposable lorsque $\exists$ existe une tour d'extensions $K = E_1 \subseteq E_2 \subseteq \dots \subseteq E_r = \mathbb{C}$ tel que $\forall C \in \mathbb{R}, \forall D, [E_{i+1} : E_i] \leq 2$.

Théorème 21: (Wantzel) Un nombre est constructible si et seulement s'il est contenu dans une extension 2-décomposable de $\mathbb{Q}$.

Corollaire 22: Un nombre $z \in \mathbb{C}$ est constructible si et seulement si son degré est une puissance de deux.

Application 23: La quadrature du cercle (i.e. construire $\sqrt[n]{n}$) est impossible.

Application 24: La duplication du cube (i.e. construire $\sqrt[3]{2}$) est impossible.

Théorème 25: Soit $\odot \in \mathbb{R}^2, \pi^1$. L'angle si même $\odot$ est inscriptible. On le polygone $4X^3 - 3X - \cos \odot$ admet une racine dans $\mathbb{Q}(\cos \odot)$.

Exemple 26: π_3 n'est pas constructible mais $\frac{\pi}{4}$ l'est.

II) Annexe de nombres remarquables.

1) Arithmétique principale

Dans cette partie, A est un anneau intègre.

Définition 27: Soit $a \in A$. On dit que a est unitaire lorsque $\exists b \in A$ tel que $ab = 1$. On note $A^\times$ l'ensemble des inversibles de A .

Définition 28: Soit $p \in A$. On dit que p est irréductible lorsque $p \neq 0, p \nmid A^\times$ et $p = ab \Rightarrow a$ ou b est inversible.

Exemple 29: Dans $\mathbb{Z}$, les inversibles sont ± 1 , les irréductibles, $\mathbb{P}$ ou p est un nombre premier.

Théorème 30: Dans $\mathbb{N}$, il existe une infinité de nombres premiers.

Définition 31: On dit que P est principal lorsque $\exists$ existe un $a \in A$ tel que $P = (a)$.

Proposition 32: Dans un anneau principal, p est irréductible si et seulement si p est un idéal premier.

Définition 33: Un anneau commutatif intègre est dit euclidien lorsque $\exists$ existe une application $\varphi: A^\times \rightarrow \mathbb{N}$ telle que $\forall (a, b) \in A^2, b \neq 0, \exists (q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Exemples 34: 1) $\mathbb{Z}$ est euclidien pour le standard $u \mapsto |u|$

2) $\mathbb{K}[X]$ est euclidien pour le standard $P \mapsto \deg(P)$

3) $\mathbb{D}$ est euclidien.

Théorème 35: Un anneau euclidien est principal.

Lemme 36: Soit A un anneau euclidien, $f \in A$ tel $x \nmid f$ et b la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur A/fA , soit surjective.

Lemme 37: $A := \mathbb{Z} \left[\frac{1+i\sqrt{5}}{2} \right] = \mathbb{Z}[\alpha]$, $N(\beta) = \alpha\bar{\beta} \mapsto \alpha^2 + b\alpha -$
 Soient a et $b \in A \setminus \{0\}$, $\exists q, r \in A$ avec 1) $r = 0$ ou $N(r) < N(b)$
 2) $a = bq + r$ avec $2a = bq + r$

Application 38: $\mathbb{Z} \left[\frac{1+i\sqrt{5}}{2} \right]$ est principal pour l'euclidien.

Théorème 39: On munit $A \times A \setminus \{0\}$ des deux distances par :

$(a, b) + (c, d) = (ad + bc, bd)$ et $(a, b) \times (c, d) = (ac, bd)$
 et de la relation $((a, b), R(a', b'))$ si $(a, b) \leq (a', b')$.

Alors $(A \times A \setminus \{0\}) / R$ est un corps, appelé corps de fractions de A et noté $\text{Frac}(A)$.

Exemple 40: Pour $A = \mathbb{Z}$, $\text{Frac}(A) = \mathbb{Q}$.

2) Théorème des deux carrés

Notations 41: On introduit $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2, (a, b) \in \mathbb{N}^2\}$

$\mathbb{Z}[\sqrt{-1}] = \{a + ib \mid a, b \in \mathbb{Z}\}$ sous anneau de $\mathbb{C}$ (intégrale)

$N : \mathbb{Z}[\sqrt{-1}] \rightarrow \mathbb{N}$

$z = a + ib \mapsto N(z) = a^2 + b^2$

Lemme 42: $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm i\}$

Lemme 43: $\mathbb{Z}$ est stable par $\times$

Lemme 44: $\mathbb{Z}[\sqrt{-1}]$ est euclidien pour le standard.

Lemme 45: $(p \in \mathbb{Z})$ si p n'est divisible par 4, $p \in \Sigma$

Théorème 46: (des deux carrés) Soit $p \in \mathbb{Z}$.

$(p \in \mathbb{Z})$ si $p = 2$ ou $p \equiv 1 \pmod{4}$

des
2