

127 Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

I – Nombres remarquables

1. Deux exemples fondamentaux : e et π

DÉFINITION 1

On définit la fonction **exponentielle complexe** pour tout $z \in \mathbb{C}$ par

$$\sum_{n=0}^{+\infty} \frac{z^n}{n!}$$

on note cette somme e^z ou parfois $\exp(z)$.

[QUE]
p. 4

REMARQUE 2

Cette somme est bien définie pour tout $z \in \mathbb{C}$ d'après le critère de d'Alembert.

PROPOSITION 3

- (i) $\forall z, z' \in \mathbb{C}, e^{z+z'} = e^z e^{z'}$.
- (ii) $\exp$ est holomorphe sur $\mathbb{C}$, de dérivée elle-même.
- (iii) $\exp$ ne s'annule jamais.

DÉFINITION 4

On définit e le **nombre d'Euler** par $e = e^1 > 0$.

p. 383

PROPOSITION 5

La fonction $\varphi : t \mapsto e^{it}$ est un morphisme surjectif de $\mathbb{R}$ sur $\mathbb{U}$, le groupe des nombres complexes de module 1.

p. 7

PROPOSITION 6

En reprenant les notations précédentes, $\text{Ker}(\varphi)$ est un sous-groupe fermé de $\mathbb{R}$, de la forme $\text{Ker}(\varphi) = a\mathbb{Z}$. On note $a = 2\pi$.

2. Nombres algébriques, transcendants

DÉFINITION 7

Un nombre complexe (resp. réel) z est dit **nombre algébrique complexe** (resp. **nombre algébrique réel**) s'il existe $P \in \mathbb{Z}[X] \setminus \{0\}$ tel que $P(z) = 0$.

[GOZ]
p. 40

EXEMPLE 8

$\pm\sqrt{2}$ et $\pm i$ sont des nombres algébriques.

p. 40

THÉORÈME 9

Théorème de Liouville.

Soit α un nombre algébrique réel, racine d'un polynôme $P \in \mathbb{Z}[X]$ de degré supérieur ou égal à 2. Alors,

$$\exists C_\alpha > 0 \text{ tel que } \forall \frac{p}{q} \in \mathbb{Q}, \left\| x - \frac{p}{q} \right\| \geq \frac{C}{q^d}$$

[QUE]
p. 391

APPLICATION 10

Le nombre de Liouville,

$$\sum_{n=1}^{+\infty} \frac{1}{10^{n!}}$$

est transcendant.

THÉORÈME 11

Théorème d'Hermite.

e est transcendant.

[GOZ]
p. 41

THÉORÈME 12

Théorème de Lindemann.

π est transcendant.

APPLICATION 13

Les nombres $\zeta(2k)$ sont transcendants pour $k \in \mathbb{N}^*$.

[QUE]
p. 385

II – Anneaux de nombres algébriques

NOTATION 14

On note $\mathbb{A}$ l'ensemble des nombres algébriques complexes. $\mathbb{A} \cap \mathbb{R}$ est alors l'ensemble des nombres algébriques réels.

[GOZ]
p. 40

THÉORÈME 15

- (i) $\mathbb{A}$ est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$.
- (ii) $\mathbb{A} \cap \mathbb{R}$ est un sous-corps de $\mathbb{R}$ qui contient $\mathbb{Q}$.

COROLLAIRE 16

$\mathbb{A}$ est la clôture algébrique de $\mathbb{Q}$.

p. 63

REMARQUE 17

Toute extension de $\mathbb{Q}$ de degré fini est alors un sous-corps de $\mathbb{A}$.

1. Corps de nombres quadratiques

PROPOSITION 18

Soit $d \in \mathbb{N}$ tel que $d \geq 2$. Les assertions suivantes sont équivalentes.

- (i) $\sqrt{d} \notin \mathbb{Q}$.
- (ii) $\sqrt{d} \notin \mathbb{N}$.
- (iii) Il existe p premier tel que $v_p(d)$ (la valuation p -adique de d) est impaire.
- (iv) $\mathbb{Q}[\sqrt{d}]$ est une extension de $\mathbb{Q}$ de degré 2.

p. 33

DÉFINITION 19

On appelle **corps quadratique** toute extension de degré 2 de $\mathbb{Q}$ dans $\mathbb{C}$.

THÉORÈME 20

Soit $\mathbb{L}$ un corps quadratique. Alors, il existe un entier relatif $d \notin \{0, 1\}$, sans facteur carré tel que

$$\mathbb{L} = \mathbb{Q}[\sqrt{d}]$$

où $\sqrt{d}$ désigne un complexe dont le carré est égal à d .

DÉFINITION 21

Soit d un entier non nul qui n'est pas un carré dans $\mathbb{Z}$ et $z = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ avec $x, y \in \mathbb{Q}$. La **norme** de z est

$$N(z) = x^2 - y^2 d$$

PROPOSITION 22

Soit d un entier non nul qui n'est pas un carré dans $\mathbb{Z}$. Pour $z = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ avec $x, y \in \mathbb{Q}$. Posons $\tilde{z} = x - y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$.

- (i) L'application $z \mapsto \tilde{z}$ est un automorphisme des anneaux $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$. Pour tout $z \in \mathbb{Q}[\sqrt{d}]$, nous avons $\tilde{\tilde{z}} = z$ et $N(z) = z\tilde{z}$. Si $z \in \mathbb{Z}[\sqrt{d}]$, alors $N(z) \in \mathbb{Z}$.
- (ii) $\mathbb{Q}[\sqrt{d}] \cong \mathbb{Q}[X]/(X^2 - d)$ est un corps.
- (iii) Dans $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$, nous avons $N(z_1 z_2) = N(z_1)N(z_2)$ et $N(z) = 0 \iff z = 0$.

PROPOSITION 23

Soit d un entier non nul qui n'est pas un carré dans $\mathbb{Z}$.

- (i) Les inversibles de $\mathbb{Z}[\sqrt{d}]$ sont exactement les éléments z tels que $N(z) = \pm 1$.
- (ii) Tout élément non nul et non inversible de $\mathbb{Z}[\sqrt{d}]$ possède une décomposition en produit d'irréductibles.

[ULM18]
p. 67

2. Anneau des entiers de Gauss

DÉFINITION 24

L'anneau $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ est l'**anneau des entiers de Gauss**.

EXEMPLE 25

Pour $z = x + iy \in \mathbb{Z}[i]$, nous avons $N(z) = x^2 + y^2$ et donc les inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$.

NOTATION 26

On note Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P]
p. 137**REMARQUE 27**

$n \in \Sigma \iff \exists z \in \mathbb{Z}[i] \text{ tel que } N(z) = n$.

LEMME 28

$\mathbb{Z}[i]$ est euclidien de stathme N .

LEMME 29

Soit p un nombre premier. Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p \in \Sigma$.

THÉORÈME 30**Deux carrés de Fermat.**

Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \pmod{4}$ (où $v_p(n)$ désigne la valuation p -adique de n).

3. Corps cyclotomiques

Soit m un entier supérieur ou égal à 1.

DÉFINITION 31

On définit

$$\mu_m = \{z \in \mathbb{C}^* \mid z^m = 1\}$$

l'ensemble des **racines m -ièmes de l'unité**. C'est un groupe (cyclique) pour la multiplication dont l'ensemble des générateurs, noté μ_m^* , est formé des **racines primitives m -ièmes de l'unité**.

[GOZ]
p. 67

PROPOSITION 32

- (i) $\mu_m^* = \{e^{\frac{2ik\pi}{m}} \mid k \in \llbracket 0, m-1 \rrbracket, \text{pgcd}(k, m) = 1\}$.
- (ii) $|\mu_m^*| = \varphi(m)$, où φ désigne l'indicatrice d'Euler.

PROPOSITION 33

Le sous-corps $\mathbb{Q}(\xi)$ de $\mathbb{C}$ ne dépend pas de la racine m -ième primitive ξ de l'unité considérée.

DÉFINITION 34

On appelle **corps cyclotomique**, un corps de la forme de la Proposition 33 (ie. engendré par une racine primitive de l'unité).

DÉFINITION 35

On appelle **m -ième polynôme cyclotomique** le polynôme

$$\Phi_m = \prod_{\xi \in \mu_m^*} (X - \xi)$$

THÉORÈME 36

- (i) $X^m - 1 = \prod_{d|m} \Phi_d$.
- (ii) $\Phi_m \in \mathbb{Z}[X]$.
- (iii) Φ_m est irréductible sur $\mathbb{Q}$.

COROLLAIRE 37

Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_m^* est Φ_m . En particulier, le degré de $\mathbb{Q}(\xi)$ sur $\mathbb{Q}$ est $\varphi(m)$.

APPLICATION 38**Théorème de Wedderburn.**

Tout corps fini est commutatif.

APPLICATION 39**Dirichlet faible.**

Pour tout entier n , il existe une infinité de nombres premiers congrus à 1 modulo n .

[GOU21]
p. 99

III – Application à la constructibilité à la règle et au compas

On note $\mathcal{P}$ un plan affine euclidien muni d'un repère orthonormé direct $\mathcal{R} = (O, \vec{i}, \vec{j})$. On s'autorise à identifier chaque point $M \in \mathcal{P}$ avec ses coordonnées $(x, y) \in \mathbb{R}^2$ dans $\mathcal{R}$.

[GOZ]
p. 47

DÉFINITION 40

On dit qu'un point $M \in \mathcal{P}$ est **constructible** (sous-entendu *à la règle et au compas*) si on peut le construire en utilisant uniquement la règle et le compas, en supposant O et $I = (1, 0)$ déjà construits.

PROPOSITION 41

Soient A, B deux points constructibles distincts.

- (i) Si A est constructible, son symétrique par rapport à O l'est aussi.
- (ii) $J = (0, 1)$ est constructible.
- (iii) Si C est un point constructible, on peut construire à la règle et au compas la perpendiculaire à (AB) passant par C .
- (iv) Si C est un point constructible, on peut construire à la règle et au compas la parallèle à (AB) passant par C .

PROPOSITION 42

Soit $x \in \mathbb{R}$.

$$(x, 0) \text{ est constructible} \iff (0, x) \text{ est constructible}$$

DÉFINITION 43

Un nombre vérifiant la proposition précédente est dit **nombre constructible**.

PROPOSITION 44

- (i) Tout élément de $\mathbb{Q}$ est constructible.
- (ii) (x, y) est constructible si et seulement si x et y le sont.

THÉORÈME 45

L'ensemble $\mathbb{E}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

DEV

THÉORÈME 46**Théorème de Wantzel.**

Soit $t \in \mathbb{R}$. t est constructible si et seulement s'il existe une suite finie $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :

- (i) $L_0 = \mathbb{Q}$.
- (ii) $\forall i \in \llbracket 1, p \rrbracket$, L_i est une extension quadratique de L_{i-1} .
- (iii) $t \in L_p$.

COROLLAIRE 47

- (i) Si x est constructible, le degré de l'extension $\mathbb{Q}[x]$ sur $\mathbb{Q}$ est de la forme 2^s pour $s \in \mathbb{N}$.
- (ii) Tout nombre constructible est algébrique.

CONTRE-EXEMPLE 48

- $\sqrt[3]{2}$ est algébrique, non constructible.
- $\sqrt{\pi}$ est transcendant et n'est donc pas constructible.

APPLICATION 49**Quadrature du cercle.**

Il est impossible de construire, à la règle et au compas, un carré ayant même aire qu'un disque donné.

APPLICATION 50**Duplication du cube.**

Il est impossible de construire, à la règle et au compas, l'arête d'un cube ayant un volume double de celui d'un cube donné.

Bibliographie

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.

<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

Théorie de Galois

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2^e éd. Ellipses, 1^{er} avr. 2009.

<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

L'oral à l'agrégation de mathématiques

[I-P]

LUCAS ISENMANN et TIMOTHÉE PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2^e éd. Ellipses, 26 mars 2024.

<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

Analyse complexe et applications

[QUE]

Martine QUEFFÉLLEC et Hervé QUEFFÉLEC. *Analyse complexe et applications. Nouveau tirage*. Calvage & Mounet, 13 mai 2017.

<http://www.calvage-et-mounet.fr/2022/05/09/analyse-complexe-et-applications/>.

Anneaux, corps, résultants

[ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.

<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html>.