1. Nombres remarquables

1.1. Nombres rationnels, irrationnels

Définition 1. L'ensemble des nombres **rationnels** est défini par $\mathbf{Q} := \left\{\frac{a}{b} \ : \ (a,b) \in \mathbf{Z} \times \mathbf{N}^*\right\}$: c'est le corps des fractions de $\mathbf{Z}$.

Proposition 2. On dispose de la chaîne d'inclusions $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. En particulier, $\mathbf{Q}$ est un corps et c'est le plus petit corps de caractéristique nulle (à isomorphisme près).

Définition 3. Un nombre **irrationnel** est un élément de $\mathbf{R} \setminus \mathbf{Q}$.

Exemple 4. 4, $4/3$ et $3/5$ sont rationnels. $\sqrt{2}$ et $\mathrm{e} = \exp(1)$ sont irrationnels.

Définition 5. On définit π comme étant le périmètre d'un cercle de rayon $1/2$ dans le plan euclidien. C'est également le double du premier zéro positif de la fonction cosinus.

Proposition 6. π est irrationnel.

Définition 7. Soit $x \in \mathbf{R}$. On appelle **développement décimal** de x toute écriture de $x - \lfloor x \rfloor$ sous la forme $\sum_{n=1}^{+\infty} \frac{a_n}{10^n}$, où $a_n \in [\![0,9]\!]$ pour tout $n \geq 1$.

Remarque 8. Le développement décimal est unique si l'on impose de plus que (a_n) ne stationne pas à 9 à partir d'un certain rang.

Définition 9. Un nombre x est dit **décimal** s'il admet un développement décimal nul à partir d'un certain rang.

Exemple 10. 10 et $3/10$ sont décimaux. $10/9$ n'est pas décimal.

Proposition 11. L'ensemble $\mathbf{D}$ des nombres décimaux est un sous-anneau de $\mathbf{Q}$.

Théorème 12. Un nombre est rationnel si et seulement si son développement décimal est périodique à partir d'un certain rang.

Application 13. Le nombre $\theta := \sum_{n=0}^{\infty} \frac{1}{10^{n^2}}$ est irrationnel.

Proposition 14. Un nombre θ est irrationnel si et seulement si $\mathbf{Z} + \theta\mathbf{Z}$ est dense dans $\mathbf{R}$.

Application 15. Une fonction continue sur $\mathbf{R}$ admettant 1 et $\sqrt{2}$ pour périodes est constante.

1.2. Nombres algébriques, transcendants

Définition 16. Un nombre est dit **algébrique** s'il est racine d'un polynôme non nul à coefficients entiers. En particulier, on parle d'**entier algébrique** lorsque l'on peut choisir ce polynôme unitaire. On dit qu'un nombre est **transcendant** s'il n'est pas algébrique.

Exemple 17. $\sqrt{2}$ et i sont des entiers algébriques. $\frac{1}{\sqrt{2}}$ est un nombre algébrique mais pas un entier algébrique.

Définition 18. Soit ω un nombre algébrique. Son **polynôme minimal** $P_\omega \in \mathbf{Q}[X]$ est le polynôme unitaire de degré minimal annulant ω. Son degré est appelé **degré de** ω.

Proposition 19. Un nombre algébrique est un entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

Théorème 20 : Liouville. Soit α un nombre algébrique de degré $d \geq 2$. Alors il existe un réel $C(\alpha)$ tel que

$$\forall (p,q) \in \mathbf{Z} \times \mathbf{N}^*, \quad \left|\alpha - \frac{p}{q}\right| \geq \frac{C(\alpha)}{q^d}.$$

Application 21. Le nombre $\alpha := \sum_{k=0}^{\infty} \frac{1}{10^{k!}}$ est transcendant.

Théorème 22 : Hermite–Lindemann (admis). Soit a un nombre algébrique. Alors $\exp(a)$ est transcendant.

Corollaire 23. π et $\mathrm{e} = \exp(1)$ sont transcendants.

Application 24. Pour $k \in \mathbf{N}^*$, $\zeta(2k)$ est transcendant car il s'écrit $\pi^{2k}q$, avec $q \in \mathbf{Q}$.

2. Anneaux de nombres algébriques

Théorème 25. Les nombres (resp. entiers) algébriques sont stables par somme, produit et passage à l'inverse (resp. somme et produit).

Corollaire 26. L'ensemble des nombres algébriques $\mathbf{A}$ est une extension de corps de $\mathbf{Q}$: c'est sa clotûre algébrique. L'ensemble des entiers algébriques forme un sous-anneau de $\mathbf{A}$.

Proposition 27. Soit $\omega \in \mathbf{C}$ un nombre algébrique de degré d. L'ensemble $\mathbf{Q}(\omega) = \left\{a_0 + a_1\omega + \ldots + a_{d-1}\omega^{d-1} \ : \ a_0, \ldots, a_{d-1} \in \mathbf{Q}\right\}$ est une extension de $\mathbf{Q}$ de degré d, appelée **corps de nombres de degré** d.

Définition 28. Soit $\omega \in \mathbf{C}$ un nombre algébrique. Les éléments de $\mathbf{K} = \mathbf{Q}(\omega)$ annulés par un polynôme unitaire à coefficients entiers sont appelés les **entiers de K**.

Proposition 29. Soit $\omega \in \mathbf{C}$ un nombre algébrique. L'ensemble $A_{\mathbf{K}}$ des élements entiers de $\mathbf{K} = \mathbf{Q}(\omega)$ est un sous-anneau de $\mathbf{K}$, appelé **anneau des entiers de K**.

2.1. Corps de nombres quadratiques

Définition 30. Un corps de **nombres quadratiques** est une extension finie de $\mathbf{Q}$ de degré 2.

Proposition 31. Soit $\mathbf{K}$ un corps de nombres quadratiques. Alors il existe $d \in \mathbf{Z}$ sans facteur carré tel que $\mathbf{K} = \mathbf{Q}(\sqrt{d})$. On dit que $\mathbf{K}$ est un corps quadratique **réel** (resp. **imaginaire**) si $d > 0$ (resp $d < 0$).

Définition 32. Pour $x = \alpha + \beta\sqrt{d} \in \mathbf{Q}(\sqrt{d})$, la **norme** de x est définie par $N(x) := \alpha^2 - d\beta^2$. N est à valeurs rationnnelles et stable par produit.
La **trace** de x est définie par $T(x) := 2\alpha$. T est à valeurs rationnelles et stable par somme.

Définition 33. Soit $\mathbf{K} = \mathbf{Q}(\sqrt{d})$. Les éléments entiers de $\mathbf{K}$ sont appelés **entiers quadratiques**.

Exemple 34. Pour $d = -1$, $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\mathrm{i})$ et son anneau des entiers est l'anneau des entiers de Gauss $\mathbf{Z}[\mathrm{i}]$.

Proposition 35. Si $x \in A_{\mathbf{K}}$, alors $N(x) \in \mathbf{Z}$. La réciproque est fausse.

Théorème 36. Soit $x \in \mathbf{K} = \mathbf{Q}(\sqrt{d})$. $x \in A_{\mathbf{K}}$ si et seulement si $N(x) \in \mathbf{Z}$ et $T(x) \in \mathbf{Z}$.

Proposition 37. Si $d \equiv 2$ ou 3 $[4]$, alors $A_{\mathbf{K}} = \mathbf{Z}[\sqrt{d}]$.
Si $d \equiv 1[4]$, alors $A_{\mathbf{K}} = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$.

Théorème 38. $A_{\mathbf{K}}^{\times} = \{x \in A_{\mathbf{K}} \mid N(x) = \pm 1\}$.

Proposition 39. Soit $\mathbf{K} = \mathbf{Q}(\mathrm{i}\sqrt{d})$ avec $d \in \mathbf{N}^*$. Alors

- ⋆ Si $d = 1$, alors $A_{\mathbf{K}} = \mathbf{Z}[\mathrm{i}]$ et $A_{\mathbf{K}}^{\times} = \{\pm 1, \pm \mathrm{i}\}$.
- ⋆ Si $d = 3$, alors $A_{\mathbf{K}} = \mathbf{Z}[\mathrm{j}]$ et $A_{\mathbf{K}}^{\times} = \left\{\pm 1, \pm \mathrm{j}, \pm \mathrm{j}^2\right\}$.
- ⋆ Sinon, $A_{\mathbf{K}}^{\times} = \{\pm 1\}$.

Proposition 40. Soit $\mathbf{K} = \mathbf{Q}(\sqrt{d})$ avec $d \in \mathbf{N}^*$. Alors il existe une unité $\omega > 1$ de $A_{\mathbf{K}}$ (appelée **unité fondamentale**) telle que $A_{\mathbf{K}}^{\times} = \{\pm\omega^n \ : \ n \in \mathbf{Z}\}$.

Exemple 41. Si $d = 5$, alors $A_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\varphi]$, où $\varphi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or. De plus, c'est l'unité fondamentale et l'on a $\mathbf{Z}[\varphi]^{\times} = \{\pm\varphi^n \ : \ n \in \mathbf{Z}\}$.

Définition 42. Soit A un anneau commutatif unitaire et intègre. On dit que $p \in A$ est :

- ⋆ **irréductible** si $\forall a, b \in A$, $p = ab$ implique $a \in A^{\times}$ ou $b \in A^{\times}$.
- ⋆ **premier** si $\forall a, b \in A$, $p|ab$ implique $p|a$ ou $p|b$.

Remarque 43. Un élément premier est irréductible. La réciproque est fausse dès lors que A n'est pas factoriel. Par exemple, 2 est irréductible mais non premier dans $\mathbf{Z}[\mathrm{i}\sqrt{5}]$.

Théorème 44. Soit $\mathbf{K} = \mathbf{Q}(\sqrt{d})$. Alors tout élément de $A_{\mathbf{K}}$ se décompose en produit d'éléments irréductibles. De plus cette décomposition est unique (ie $A_{\mathbf{K}}$ est factoriel) si et seulement si tout élément irréductible de $A_{\mathbf{K}}$ est premier.

Exemple 45. Dans $\mathbf{Z}[\mathrm{i}\sqrt{5}] = A_{\mathbf{Q}(\mathrm{i}\sqrt{5})}$, $6 = 2 \times 3 = (1 + \mathrm{i}\sqrt{5})(1 - \mathrm{i}\sqrt{5})$. Il n'y a donc pas unicité de la décomposition : on retrouve que $\mathbf{Z}[\mathrm{i}\sqrt{5}]$ n'est pas factoriel.

Théorème 46. Les anneaux $\mathbf{Z}[\mathrm{i}]$ et $\mathbf{Z}[\mathrm{j}]$ des entiers de $\mathbf{Q}(\mathrm{i})$ et $\mathbf{Q}(\mathrm{i}\sqrt{3})$ sont euclidiens.

Application 47. Résolution explicite de l'équation $x^2 + y^2 = z^2$ dans $\mathbf{Z}^3$.

Application 48. L'équation de Fermat $x^3 + y^3 = z^3$ n'a pas de solution dans $(\mathbf{Z}^*)^3$.

Application 49 : Théorème des deux carrés [DEV 1]. Soit $S := \{n \geq 2 \mid \exists (a,b) \in \mathbf{N}^2, a^2 + b^2 = n\}$. Alors $n \in S$ si et seulement si pour tout nombre premier p congru à 3 modulo 4, $v_p(n)$ est pair.

Exemple 50. $585 = 3^2 \cdot 5 \cdot 13$ est donc une somme de deux carrés. En effet, $585 = 21^2 + 12^2 = 24^2 + 3^2$.

2.2. Corps cyclotomiques

Soit $n \in \mathbf{N}^*$. On fixe $\omega := \mathrm{e}^{2\mathrm{i}\pi/n}$ une racine primitive n-ième de l'unité.

Définition 51. Le n-ième **polynôme cyclotomique** est défini par $\Phi_n(X) = \prod_{k=1, k\wedge n=1}^{n} (X - \omega^k)$.

Théorème 52. On a l'égalité $X^n - 1 = \prod_{d|n} \Phi_d$. De plus, Φ_n est à coefficients entiers et irréductible dans $\mathbf{Q}[X]$.

Corollaire 53. Φ_n est le polynôme minimal de ω. Notons φ l'indicatrice d'Euler. $\mathbf{Q}(\omega)$ est une extension algébrique finie de $\mathbf{Q}$ de degré $\varphi(n)$: on l'appelle **corps cyclotomique** de degré $\varphi(n)$.

Théorème 54. Soit p un nombre premier impair et α une racine primitive p-ième de l'unité. Alors l'anneau des entiers du corps cyclotomique $\mathbf{Q}(\alpha)$ est égal à $\mathbf{Z}[\alpha]$.

3. Nombres constructibles

On se place dans un repère cartésien sur lequel on peut marquer les points (1,0) et (0,1). On peut alors tracer à l'aide d'une règle (non graduée) et d'un compas les droites passant par deux points déjà construits ainsi que les cercles ayant leur centre en un point construit et dont le rayon est la distance entre deux points déjà construits.

De plus, les intersections de deux droites déjà construites, de deux cercles déjà construits et d'une droite et d'un cercle déjà construits définissent de nouveaux points du plan obtenus par construction élémentaire.

Définition 55. Un point du plan est **constructible** s'il est obtenu par une suite finie de constructions élémentaires.

Définition 56. Un réel a est **constructible** si le point $(a, 0)$ est constructible.

Exemple 57. $\sqrt{2}$ et le nombre d'or sont constructibles.

Proposition 58. L'ensemble $\mathcal{C}$ des nombres réels constructibles est un sous-corps de $\mathbf{R}$ contenant $\mathbf{Q}$ et stable par extraction de racine carrée.

Proposition 59. Soit $P \subseteq \mathbf{R}^2$ et K le sous-corps de $\mathbf{R}$ engendré sur $\mathbf{Q}$ par les coordonnées des points de P. Si (a, b) est un point du plan obtenu par une construction élémentaire à partir des points de P, alors $[K(a,b) : K] \in \{1, 2\}$.

Théorème 60 : Wantzel [DEV 2]. Un nombre réel a est constructible si et seulement s'il existe une tour d'extensions $\mathbf{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbf{R}$ telle que $a \in K_m$ et $[K_{i+1} : K_i] = 2$ pour tout $0 \leq i < m$.

Corollaire 61. Un nombre constructible est algébrique, de degré une puissance de 2.

Exemple 62. $\sqrt[3]{2}$ n'est pas constructible.

Application 63. Impossibilité de la quadrature du cercle : pour un cercle de rayon constructible, il est impossible de construire un carré dont l'aire est égale à celle du disque bordé par le cercle.

Application 64. Soit p un nombre premier impair. Si une racine primitive p-ième de l'unité est constructible, alors p est un nombre premier de Fermat, ie $p = 2^{2^m} + 1$ avec $m \in \mathbf{N}$.

Théorème 65 : Gauss–Wantzel. Le polygône régulier à n côtés P_n est constructible à la règle et au compas si et seulement si $n = 2^a p_1 \cdots p_r$, avec $a \in \mathbf{N}$ et $p_1, \ldots, p_r$ des nombres premiers de Fermat distincts.

Défense du plan :

Je décris ici la progression logique que j'ai suivi en construisant ce plan. Evidemment qu'il est impossible d'en faire un exposé aussi détaillé en 6 minutes, il suffit de garder les points-clés et de bien les relier entre eux.

Je commence par présenter les exemples « classiques » d'ensembles de nombres remarquables $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ puis on étudie plus en détail les nombres rationnels qui forment le plus petit corps de caractéristique nulle.
Je donne ensuite des exemples et des caractérisations des nombres rationnels et irrationnels. Cela permet de citer dès le départ des nombres remarquables irrationnels comme $\sqrt{2}$, e ou π.
Les rationnels formant un corps, ils sont stables par les 4 opérations élémentaires. Cependant, l'exemple de $\sqrt{2}$ montre qu'ils ne sont pas stables par extractions de racines. On est donc naturellement amené à étudier l'ensemble des nombres qui sont racines de polynômes à coefficients rationnels, autrement dit l'ensemble des nombres algébriques.
Je présente donc la définition des nombres algébriques puis le cas particulier des entiers algébriques avec une première caractérisation liée à leur polynôme minimal, j'y reviendrai dans le II.
Cependant, tous les nombres ne sont pas algébriques (l'ensemble des nombres algébriques étant dénombrable), il existe donc théoriquement des nombres non algébriques : les nombres transcendants. Il est cependant relativement difficile de prouver qu'un nombre est transcendant. Je donne plusieurs résultats à ce sujet : d'abord le théorème de Liouville qui donne une condition nécessaire pour qu'un nombre soit algébrique. Sa contraposée donne donc une condition suffisante de transcendance, ce qui permet de construire les nombres de Liouville qui ont été historiquement les premiers nombres dont la transcendance a été prouvée. Puis j'énonce en l'admettant le théorème de Hermite-Lindemann, bien plus difficile à prouver, qui donne la transcendance de nombreux autres nombres et en particulier e et π.

Revenons aux nombres algébriques. Ils ont une propriété algébrique fondamentale : ils sont stables par opérations algébriques, autrement dit ils forment un corps, et même un corps algébriquement clos. De même, les entiers algébriques sont stables par somme et produit donc forment un anneau.
On peut alors, pour α un nombre algébrique, donner à l'anneau de polynômes $\mathbf{Q}[\alpha]$ une structure de corps. On définit ainsi des extensions finies de $\mathbf{Q}$: les corps de nombres. La stabilité des nombres algébriques par somme et produit assure alors que ces extensions sont elles-mêmes algébriques.
De plus, les entiers algébriques d'un corps de nombres $\mathbf{K}$ en forment un sous-anneau : l'anneau des entiers de $\mathbf{K}$.

Comme le demande le rapport de jury : « *L'objectif n'est pas [de] présenter le plus possible [d'exemples de nombres et de corps de nombres utilisés en algèbre ou en géométrie], mais plutôt d'en choisir certains, suffisamment variés, en en expliquant la genèse et en soulignant leur intérêt par des applications pertinentes.* », je choisis d'étudier plus en détails certains corps de nombres : les corps quadratiques et les corps cyclotomiques car ils sont relativement aisés à construire et à décrire.
Le cadre des corps quadratiques permet de décrire en détail la structure de leurs anneaux d'entiers et leur propriétés algébriques. La factorialité de l'anneau des entiers d'un corps quadratique dans certains cas permet de nombreuses applications, en particulier le théorème des deux carrés qui fait l'objet du premier développement.
Les corps cyclotomiques offrent une perspective plus large avec des extensions de degrés plus élevés et dont l'anneau des entiers se décrit aisément dans certains cas, ce qui permet également de nombreuses application comme la factorisation de l'équation de Fermat, ou l'étude de la constructibilité de certains nombres.

En effet, en prenant un point de vue plus géométrique, on est amené à se demander, parmi les nombres étudiés jusqu'à maintenant, lesquels sont constructibles à la règle et au compas. On montre que les rationnels le sont puis que l'ensemble des nombres constructibles est stable par addition, mulitiplication, passage à l'inverse et extraction de racine carrée, ce qui conduit au deuxième développement : le théorème de Wantzel qui établit une équivalence entre un critère géométrique (la constructibilité d'un nombre) et un critère algébrique (son appartenance à une tour d'extensions quadratiques).
Les applications de ce théorème sont nombreuses : il permet de résoudre certains problèmes de géométrie connus depuis l'Antiquité (quadature du cercle, duplication du cube) ou, combiné aux propriétés des corps cyclotomiques, de déterminer la constructibilité de certaines figures (théorème de Gauss-Wantzel sur la constructibilité des polygônes réguliers).

Exemples de questions posées (ou qui pourraient être posées) :

- ⋆ Vous définissez **Q** comme étant le corps des fractions de **Z**, pourriez-vous préciser cette construction ?
- ⋆ Vous définissez π comme étant égal au demi-périmètre d'un cercle de rayon unité. Peut-on en déduire une expression de π à l'aide d'une intégrale ?
- ⋆ Pourquoi l'ensemble des nombres décimaux forme-t-il un sous-anneau de **Q** ? Sauriez-vous décrire tous les sous-anneaux de **Q** ?
- ⋆ Comment peut-on savoir, sans en exhiber un, qu'il existe forcément des nombres transcendants ?
- ⋆ Quels sont les entiers algébriques contenus dans **Q** ?
- ⋆ Pourriez-vous montrer la proposition 19 ?
- ⋆ Pourquoi les nombres algébriques sont-ils stables par somme et produit ?
- ⋆ Pourriez-vous définir un corps de nombres en général ? Quel est le lien avec la proposition 27 ?
- ⋆ Comment peut-on résoudre l'équation de Pell $x^2 + dy^2 = 1$ à l'aide de la proposition 40 ?
- ⋆ Peut-on trouver un élément strictement positif arbitrairement proche de 0 dans $\mathbf{Z}[\sqrt{2}]$ l'anneau des entiers du corps $\mathbf{Q}(\sqrt{2})$?
- ⋆ Déterminer les solutions de l'équation de Fermat dans le cas $n = 2$ en utilisant les propriétés de l'anneau $\mathbf{Z}[i]$.
- ⋆ Montrer que $\mathbf{Z}[i]$ et $\mathbf{Z}[j]$ sont euclidiens.
- ⋆ Quel est l'intéret des polynômes cyclotomiques au regard de cette leçon ?
- ⋆ Pourquoi les nombres constructibles sont-ils stables par les 4 opérations élémentaires ainsi que par l'extraction de racine carrée ?
- ⋆ Pourquoi l'équation d'une droite passant par deux points à coordonnées dans K est à coefficients dans K ? Pourquoi l'équation d'un cercle de centre un point à coordonnées dans K et de rayon égal à la distance entre 2 points à coordonnées dans K est à coefficients dans K ?

Références :

- ⋆ Pour une grande partie du **1.** et le **2.** : Daniel DUVERNEY, *Théorie des nombres*
- ⋆ Pour le **3.** : Alain JEANNERET, Daniel LINES, *Invitation à l'algèbre*
- ⋆ Pour le développement 1 : Daniel PERRIN, *Cours d'algbère*
- ⋆ Pour le devéloppement 2 : Jean-Claude CARREGA, *Théorie des corps*