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

Extrait du rapport de jury

Le jury souhaite proposer une leçon qui offre une ouverture large autour du thème des nombres et des corps de nombres utilisés en algèbre ou en géométrie. L'objectif n'est pas d'en présenter le plus possible, mais plutôt d'en choisir certains, suffisamment variés, en en expliquant la genèse et en soulignant leur intérêt par des applications pertinentes. Les nombres décimaux, dyadiques, etc. fournissent des ensembles de nombres dont l'étude, si elle est accompagnée d'applications pertinentes, a sa place dans cette leçon. Les questions d'approximation diophantienne et leur lien avec les fractions continues, sans toutefois être un attendu de la leçon, entrent dans la suite logique de ce type de considération.
Le corps des nombres algébriques, ainsi que certains de ses sous-corps particuliers, comme celui formé par l'ensemble des nombres constructibles ou des sous-anneaux formés par certains ensembles d'entiers algébriques constituent des pistes d'étude. Les candidates et candidats qui maîtrisent ces notions pourront aussi s'aventurer du côté des nombres de Pisot.
La transcendance de π et celle de e sont des résultats à connaître, et le candidat pourra en donner des applications s'il le désire, mais les démonstrations de ces résultats non triviaux ne sont pas exigibles. L'irrationalité de nombres remarquables ($\sqrt{2}$, nombre d'or, e, π) peut être abordée. Étudier les propriétés algébriques de certains ensembles de nombres (par exemple du type $\mathbb{Z}[\omega]$ où ω est un nombre algébrique) peut être une piste intéressante et mener à des applications en arithmétique. L'utilisation des nombres complexes ou, pour aller plus loin, des quaternions, en géométrie ou en arithmétique constitue aussi une piste exploitable pour cette leçon.

Présentation de la leçon

Je vais vous présenter la leçon 127 intitulée : "Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications". Le but de cette leçon sera d'étudier certains types de nombres remarquables, d'anneaux et de corps usuels au travers de propriétés fondamentales et remarquables.
Dans une première partie on s'intéresse aux nombres remarquables avec en premier lieu les nombres (ir-)rationnels. On commence par rappeler la définition du corps des fractions avant d'en venir au cas spécifique de $\mathbb{R}$ et de $\mathbb{Q}$ en parlant de nombres rationnels et irrationnels et en donnant quelques propriétés sur ces nombres ainsi que la densité de $\mathbb{Q}$ dans $\mathbb{R}$ et l'alternative dense-monogène pour les sous-groupes additifs de $\mathbb{R}$ et quelques corollaires. On parle ensuite de nombres décimaux en introduisant la définition ainsi qu'un résultat de densité puis conclure par la notion de développement décimal illimité propre et impropre. On termine cette première partie avec la notion de nombres algébriques et transcendants : on donne la définition ainsi que quelques exemples puis l'on donne une caractérisation très pratique des éléments algébriques grâce aux polynômes minimaux et la théorie de la dimension avant de finir par le théorème de Liouville qui permet de construire une infinité de nombres transcendants.
Dans une deuxième partie on s'intéresse au corps des nombres algébriques. Pour cela, on commence avec une première sous-partie où l'on donne les définitions ainsi que les premières propriétés. On donne ainsi la définition d'une extension finie et algébrique et l'on montre que toute extension finie est algébrique mais que la réciproque est fausse ! On termine cette première sous-partie avec le cas des extensions quadratiques en en donnant la définition avant de s'intéresser spécifiquement au cas de $\mathbb{Q}\left(\sqrt{d}\right)$ en donnant sa clôture intégrale. On s'intéresse ensuite au cas des corps cyclotomiques en se consacrant à l'étude des polynômes cyclotomiques : on rappelle ainsi la définition du n-ième polynôme cyclotomique avant d'en venir à ses propriétés fondamentales ainsi qu'une application au calcul du degré d'une extension.
On passe ensuite au corps des nombres constructibles et à la constructibilité du n-gone à la règle non graduée et au compas. Pour cela, on commence par donner les règles du jeu ainsi que la définition d'un nombre constructible. On remarque ensuite que l'on peut réaliser la plupart des constructions géométriques et il est donc naturel de se demander si l'on peut réaliser toutes les constructions géométriques (spoiler : c'est non !) et sinon trouver une caractérisation de la constructibilité : c'est ce que l'on va faire par la suite. On commence par montrer que les nombres constructibles forment un sous-corps de $\mathcal{C}$ et que si un nombre α est constructible, alors l'extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est de degré une puissance de 2. Ce critère n'est qu'une condition nécessaire mais très puissante car sa contraposée permet de montrer facilement si un nombre est constructible ou non. On termine ensuite par le théorème 52 qui donne enfin une caractérisation de la constructibilité (mais au pris d'une démonstration complexe...) et qui permet de répondre aux 3 problèmes grecs antiques (trisection de l'angle, duplication du cube et quadrature du cercle). On conclut cette partie avec le théorème de Gauss-Wantzel ainsi que l'interrogation de savoir ce qu'il se passe si l'on modifie les règles du jeu (rmq. 74).

Enfin, on conclut par l'étude de 3 anneaux de nombres algébriques de la forme $\mathbb{Z}[\omega]$ avec des structures différentes et qui sont de plus en plus fortes. On commence par un anneau intègre mais non factoriel : $\mathbb{Z}[i\sqrt{n}]$. On étudie cet anneau du point de vue algébrique en montrant qu'il est stable par conjugaison et en déterminant ses inversibles et ses éléments réductibles et on montre finalement qu'il n'est pas factoriel. On passe ensuite au cas de l'anneau $\mathbb{Z}\left[\frac{1}{2}\left(1+i\sqrt{19}\right)\right]$ en montrant qu'il n'est pas euclidien mais qu'il possède néanmoins une pseudo-division euclidienne ainsi qu'une structure d'anneau principal. Finalement, on conclut cette leçon par l'anneau des entiers de Gauss qui possède la structure la plus forte des trois car il est euclidien pour le stathme N. On donne enfin le théorème des deux carrés ainsi que les irréductibles de $\mathbb{Z}[i]$.

Plan général

I - Nombres remarquables
1 - Nombres (ir-)rationnels
2 - Nombres décimaux
3 - Nombres algébriques et transcendants

II - Corps des nombres algébriques
1 - Définitions et premières propriétés
2 - Corps cyclotomiques

III - Corps des nombres constructibles
1 - Nombres constructibles à la règle non graduée et au compas
2 - Application à la constructibilité du n-gone régulier

IV - 3 anneaux de nombres algébriques de la forme $\mathbb{Z}[\omega]$ aux structures différentes
1 - $\mathbb{Z}\left[i\sqrt{n}\right]$: un exemple d'anneau intègre non factoriel
2 - $\mathbb{Z}\left[\frac{1}{2}\left(1+i\sqrt{19}\right)\right]$: un exemple d'anneau principal non euclidien
3 - $\mathbb{Z}[i]$: un exemple d'anneau euclidien

Cours détaillé

I Nombres remarquables

I.1 Nombres (ir-)rationnels

Définition 1 : Corps des fractions d'un anneau [Rombaldi (1), p.214] :
On considère A un anneau.
On note $\mathrm{Frac}(A)$ le **corps des fractions de** A, c'est-à-dire l'ensemble des éléments de la forme $\frac{a}{b}$, avec $a, b \in A$ et b nul.

Exemple 2 : [Rombaldi (1), p.214]
∗ Le corps de fractions de $\mathbb{Z}$ est égal à $\mathbb{Q}$.
∗ Pour $\mathbb{K}$ un corps commutatif, on a $\mathrm{Frac}(\mathbb{K}[X]) = \mathbb{K}(X)$.

Définition 3 : Nombre (ir-)rationnel [Deschamps, p.21] :
On appelle **nombre rationnel** (resp. **irrationnel**) tout nombre qui appartient à $\mathbb{Q}$ (resp. qui n'appartient pas à $\mathbb{Q}$).

Exemple 4 : [Deschamps, p.21]
∗ Tout entier relatif est rationnel. ∗ 0,5 et $\frac{2}{5}$ sont rationnels.
∗ $\sqrt{2}$, $\sqrt{3}$, π et e sont irrationnels.

Proposition 5 : [Deschamps, p.21]
∗ La somme d'un irrationnel et d'un rationnel est un irrationnel.
∗ Le produit d'un rationnel non nul par un irrationnel est un irrationnel.
∗ On ne peut rien dire en général sur la somme et le produit de deux irrationnels.

Proposition 6 : [Rombaldi (2), p.100]
Les ensembles $\mathbb{Q}$ et $\mathbb{R}\backslash\mathbb{Q}$ sont denses dans $\mathbb{R}$.

Théorème 7 : Alternative dense-monogène [Rombaldi (2), p.114] :
Tout sous-groupe additif de $\mathbb{R}$ est dense ou de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}$.

Corollaire 8 : [Rombaldi (2), p.115]
Soient $a, b \in \mathbb{R}^*$.
Le sous-groupe additif $a\mathbb{Z} + b\mathbb{Z}$ est dense (resp. discret) dans $\mathbb{R}$ si, et seulement si, $\frac{a}{b}$ est irrationnel (resp. rationnel).

Corollaire 9 : [Rombaldi (2), p.115]
Soient $a_1, ..., a_n \in \mathbb{R}^*$.
Les assertions suivantes sont équivalentes :
∗ $\sum_{i=1}^{n} a_i\mathbb{Z}$ est discret dans $\mathbb{R}$. ∗ $\sum_{i=1}^{n} a_i\mathbb{Z}$ est fermé dans $\mathbb{R}$.
∗ Pour tous $j \neq k$ compris dans $[\![1; n]\!]$, $\frac{a_j}{a_k}$ est rationnel.

Corollaire 10 : [Rombaldi (2), p.116]
Soit θ un réel. θ est irrationnel si, et seulement si, il existe deux suites $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ d'entiers relatifs telles que pour tout $n \in \mathbb{N}$, $q_n\theta - p_n \neq 0$ et $\lim\limits_{n\to+\infty}(q_n\theta - p_n) = 0$.

Exemple 11 : [Rombaldi (2), p.131]
$\frac{\ln(5)}{\ln(2)} \notin \mathbb{Q}$, donc $\ln(2)\mathbb{Z} + \ln(5)\mathbb{Z}$ est dense dans $\mathbb{R}$.

Proposition 12 : [Rombaldi (2), p.169]
L'ensemble des périodes d'une fonction de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-groupe de $\mathbb{R}$ (et on le note $\mathcal{P}(f)$).

Proposition 13 : [Rombaldi (2), p.169]
Une fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ est constante si, et seulement si, $\mathcal{P}(f) = \mathbb{R}$.

Théorème 14 : [Rombaldi (2), p.169]
Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ continue non constante.
$*$ Le groupe $\mathcal{P}(f)$ est un fermé de $\mathbb{R}$.
$*$ f est périodique si, et seulement si, $\mathcal{P}(f)$ est discret et non réduit à $\{0\}$.

I.2 Nombres décimaux

Définition 15 : Nombre décimal [Rombaldi (2), p.98] :
On appelle **nombre décimal** tout nombre rationnel de la forme $\frac{a}{10^m}$ avec $a \in \mathbb{Z}$ et $m \in \mathbb{N}$ et on note $\mathbb{D}$ l'ensemble des nombres décimaux.

Proposition 16 : [Rombaldi (2), p.100 + 131]
$\mathbb{D}$ et $\mathbb{D}^*$ sont denses dans $\mathbb{R}$.

On note $\mathcal{D}$ l'ensemble des **développements décimaux illimités**, c'est-à-dire :

$$\mathcal{D} = \left\{(\beta_n)_{n\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}} \text{ tq } \forall n \geq 1,\ \beta_n \in [\![1;9]\!]\right\}$$

et $\mathcal{D}_p$ l'ensemble des **développements décimaux illimités propres**, c'est-à-dire des éléments de $\mathcal{D}$ non stationnaires à 9.

Lemme 17 : [Deschamps, p.793]
Soit $(\beta_n)_{n\in\mathbb{N}} \in \mathcal{D}_p$.
Si l'on note $(a_n 10^{-n})_{n\in\mathbb{N}}$ la suite des sommes partielles de la série de terme général $\beta_n 10^{-n}$, alors on a :

$$\forall n \in \mathbb{N},\ \frac{a_n}{10^n} \leq \sum_{p=0}^{+\infty} \frac{\beta_p}{10^p} \leq \frac{1+a_n}{10^n}$$

Proposition 18 : [Deschamps, p.793]
L'application $\delta : (\beta_n)_{n\in\mathbb{N}} \longmapsto \sum_{n=0}^{+\infty} \frac{\beta_n}{10^n}$ est une application de $\mathcal{D}$ dans $\mathbb{R}^+$ dont la restriction à $\mathcal{D}_p$ est injective.

Théorème 19 : [Deschamps, p.794]
Tout réel positif x s'écrit de manière unique sous la forme $x = \sum_{n=0}^{+\infty} \frac{\beta_n}{10^n}$, avec $(\beta_n)_{n\in\mathbb{N}}$ une suite d'entiers naturels telle que pour tout $n \in \mathbb{N}^*$ on ait $\beta_n \in [\![0;9]\!]$ et qui n'est pas constamment égale à 9 à partir d'un certain rang (cette écriture est le **développement décimal illimité propre de** x).
Pour tout $n \in \mathbb{N}$, si l'on note a_n la partie entière de $10^n x$, la suite $(\beta_n)_{n\in\mathbb{N}}$ est définie par :

$$\beta_0 = a_0 \text{ et } \forall n \in \mathbb{N},\ \beta_{n+1} = a_{n+1} - 10a_n$$

Remarque 20 : [Deschamps, p.794]
La restriction à $\mathcal{D}_p$ de la fonction δ est donc une bijection.

Corollaire 21 : [Rombaldi (2), p.103]
$\mathbb{R}$ est non dénombrable.

I.3 Nombres algébriques et transcendants

Définition 22 : Élément algébrique/transcendant [Perrin, p.66] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$, $\alpha \in \mathbb{L}$ ainsi que le morphisme de corps $\varphi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ tel que $\varphi|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$ et $\varphi(T) = \alpha$.
$*$ Lorsque φ est injectif, il n'y a que le polynôme nul qui s'annule en α. On dit alors que α est **transcendant sur** $\mathbb{K}$.
$*$ Lorsque φ n'est pas injectif, il existe $\mu_\alpha \in \mathbb{K}[T]$ non nul unitaire tel que $\mathrm{Ker}(\varphi) = (\mu_\alpha)$. On dit alors que α est **algébrique sur** $\mathbb{K}$ et que μ_α est le **polynôme minimal de** α **sur** $\mathbb{K}$.

Exemple 23 : [Perrin, p.66]
$*$ Les nombres $\sqrt{2}$, i et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 1$ et $X^3 - 2$.
$*$ Les nombres π et e sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$) [ADMIS].

Proposition 24 : Caractérisation des éléments algébriques [Perrin, p.66] :
Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$.
Les assertions suivantes sont équivalentes :
$*$ α est algébrique sur $\mathbb{K}$. $*$ On a $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
$*$ On a $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$ (plus précisément, $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(\mu_\alpha)$).
$*$ Il existe un unique polynôme $\mu_\alpha \in \mathbb{K}[X]$ unitaire et irréductible dans $\mathbb{K}[X]$ tel que $\mu_\alpha(\alpha) = 0_{\mathbb{K}}$.
$*$ $\mathbb{K}(\alpha) = \mathrm{Vect}_{\mathbb{K}}(1_{\mathbb{K}}, \alpha, \alpha^2, ..., \alpha^{\deg(\mu_\alpha)-1})$.

Théorème 25 : [Rombaldi (2), p.104]
L'ensemble des nombres algébriques est dénombrable et il existe une infinité de nombres transcendants.

Théorème 26 : Théorème de Liouville [Rombaldi (2), p.278]
Soit α un nombre algébrique de degré $d \geq 1$.
$*$ Pour $d = 1$, α est rationnel et il existe une constante $C_\alpha > 0$ telle que pour tout nombre rationnel $r = \frac{p}{q}$ distinct de α on ait $\left|\alpha - \frac{p}{q}\right| \geq \frac{C_\alpha}{q}$.
$*$ Pour $d \geq 2$, α est irrationnel et il existe une constante $C_\alpha > 0$ telle que pour tout nombre rationnel $r = \frac{p}{q}$ distinct de α on ait $\left|\alpha - \frac{p}{q}\right| \geq \frac{C_\alpha}{q^d}$.

II Corps des nombres algébriques

II.1 Définitions et premières propriétés

Définition 27 : Extension finie/algébrique [Perrin, p.67] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$.
On dit que $\mathbb{L}/\mathbb{K}$ est une extension :
$*$ **finie** lorsque $[\mathbb{L} : \mathbb{K}] < +\infty$.
$*$ **algébrique** lorsque tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Théorème 28 : [Perrin, p.67]
Si $\mathbb{L}/\mathbb{K}$ une extension de corps, alors $M = \{x \in \mathbb{L} \text{ tq } x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps de $\mathbb{L}$.

Remarque 29 : [Perrin, p.67]
La proposition 24 montre donc que toute extension finie est algébrique, cependant la réciproque est fausse comme le montre l'extension $A/\mathbb{Q}$ avec A le sous-corps de $\mathbb{C}$ égal à $\{\alpha \in \mathbb{C} \text{ tq } \alpha \text{ est algébrique sur } \mathbb{Q}\}$!

Définition 30 : Extension quadratique [Escofier, p.45] :
On appelle **extension quadratique** toute extension de corps de degré 2.

Proposition 31 : [Escofier, p.60]
Toute extension quadratique de $\mathbb{Q}$ est de la forme $\mathbb{Q}(\sqrt{a})$ avec a un entier relatif sans facteur carré.

Jusqu'à la fin de cette sous-partie, on considère $d \in \mathbb{Z}$ sans facteur carré, $\sqrt{d} \in \mathbb{C}$ une racine carrée de d et $\mathbb{K} = \mathbb{Q}\left(\sqrt{d}\right) = \{a + b\sqrt{d},\ (a,b) \in \mathbb{Q}\}$.

Proposition 32 : [Perrin, p.90]
Soit $x = a + b\sqrt{d} \in \mathbb{K}$.
En notant $A = \{z \in \mathbb{K} \text{ tq } z \text{ est entier sur } \mathbb{K}\}$, on a l'équivalence :

$$(x \in A) \iff (2a \in \mathbb{Z} \text{ et } a^2 - db^2 \in \mathbb{Z})$$

Proposition 33 : [Perrin, p.90]
$*$ Si $d \equiv 2, 3\ [4]$, alors $A = \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d},\ (a,b) \in \mathbb{Z}^2\right\}$.
$*$ Si $d \equiv 1\ [4]$, alors $A = \mathbb{Z}\left[\frac{1}{2}\left(1 + \sqrt{d}\right)\right]$.

II.2 Corps cyclotomiques

Dans toute cette sous-partie, on considère $\mathbb{K}$ un corps commutatif de caractéristique p, on note $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \text{ tq } \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{K}$ et on suppose que $\text{PGCD}(p, n) = 1$.

Définition 34 : Racine primitive n-ième de l'unité [Perrin, p.80] :
On considère $P(X) = X^n - 1$ et $\mathbb{K}_n$ un corps de décomposition de P.
On appelle **racine primitive n-ième de l'unité**, tout élément $\zeta \in \mathbb{K}_n$ tel que $\zeta^n = 1$ et pour tout $d \in [\![1; n-1]\!]$, $\zeta^d \neq 1$ (et on note $\mu_n^*(\mathbb{K})$ l'ensemble composé de ces éléments).

Définition 35 : n-ième polynôme cyclotomique [Perrin, p.80] :
On appelle **n-ième polynôme cyclotomique sur** $\mathbb{K}$ le polynôme :

$$\Phi_{n,\mathbb{K}}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$$

Remarque 36 : [Perrin, p.80]
$\Phi_{n,\mathbb{K}}(X)$ est un polynôme unitaire et de degré $\varphi(n)$.

Exemple 37 : [Perrin, p.81]
Sur $\mathbb{Q}$, on a :
$\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Proposition 38 : [Perrin, p.80]
On a la formule :

$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}}(X)$$

Remarque 39 : [Perrin, p.81]
La formule de la proposition précédente permet de calculer les polynômes cyclotomiques par récurrence en écrivant :

$$\Phi_{n,\mathbb{K}}(X) = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d\neq n}} \Phi_{d,\mathbb{K}}(X)}$$

Proposition 40 : [Perrin, p.81]
On a $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Théorème 41 : [Perrin, p.82]
Le polynôme $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$.

Corollaire 42 : [Perrin, p.83]
Si ζ est une racine primitive n-ième de l'unité dans un corps commutatif de caractéristique nulle, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_{n,\mathbb{Q}}$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

III Corps des nombres constructibles

Ici, chaque construction commencera de 0 et 1. Durant la construction, nous utiliserons seulement les règles suivantes :
$C1(\alpha, \beta)$: De $\alpha \neq \beta$, on peut tracer la ligne l qui passe par α et β.
$C2(\gamma, \alpha, \beta)$: De $\alpha \neq \beta$ et γ, on peut dessiner le cercle C de centre γ dont le rayon est la distance entre α et β.
$P1$: Le(s) point(s) d'intersection de deux lignes distinctes ℓ_1 et ℓ_2 construites comme ci-dessus.
$P2$: Le(s) point(s) d'intersection d'une ligne ℓ et d'un cercle C construits comme ci-dessus.
$P3$: Le(s) point(s) d'intersection de deux cercles distincts C_1 et C_2 construits comme ci-dessus.

III.1 Nombres constructibles à la règle non graduée et au compas

Définition 43 : Nombre constructible [Berhuy, p.762] :
Un nombre complexe α est un **nombre constructible** lorsqu'il existe une suite finie de constructions à la règle non graduée et au compas utilisant $C1$, $C2$, $P1$, $P2$ et $P3$ qui commence avec 0 et 1 et fini avec α.

Exemple 44 : [Berhuy, p.763]
Il est possible de construire une médiatrice d'un segment, le milieu d'un segment, une bissectrice d'un angle, la symétrie centrale et axiale d'un point, une perpendiculaire et une parallèle à une droite donnée.

Dans toute la suite de cette sous-partie, on note $\mathcal{C} := \{\alpha \in \mathbb{C} \text{ tq } \alpha \text{ est constructible}\}$.

Théorème 45 : [Berhuy, p.764 + 765]
L'ensemble $\mathcal{C}$ est un sous-corps de $\mathbb{C}$.
De plus, on a :
* $\alpha := a + ib \in \mathcal{C}$ si, et seulement si, $a, b \in \mathcal{C} \cap \mathbb{R}$.
* Si $\alpha \in \mathcal{C}$, alors chaque racine carrée de α appartient à $\mathcal{C}$.

Remarque 46 :
$\mathbb{Q}$ est constructible étant donné que $\mathbb{Z}$ est constructible et que $\mathcal{C}$ est un sous-corps de $\mathcal{C}$.

Exemple 47 :
* $2 + \sqrt{4\sqrt{5} - 3\sqrt{7}}$ est constructible.
* $\sqrt[3]{2}$ n'est pas un nombre constructible (cf. plus loin).

Théorème 48 : [Berhuy, p.775]
Soit $\alpha \in \mathbb{C}$.
$\alpha \in \mathcal{C}$ si, et seulement si, il existe des sous-corps de $\mathbb{C}$ tels que :

$$\mathbb{Q} := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}, \forall i \in [\![0; n-1]\!],\ [F_{i+1} : F_i] = 2 \text{ et } \alpha \in F_n$$

Corollaire 49 : [Berhuy, p.776]
Si $\alpha \in \mathcal{C}$, alors il existe $m \in \mathbb{N}$ tel que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$.

Remarque 50 :
* Le corollaire précédent implique que tout $\alpha \in \mathcal{C}$ est algébrique sur $\mathbb{Q}$ et que le degré de son polynôme minimal est une puissance de 2. On a alors $\mathbb{Q} \subsetneq \mathcal{C} \subsetneq \mathcal{A}$ avec $\mathcal{A}$ l'ensemble des nombres algébriques sur $\mathbb{Q}$.
* La contraposée du corollaire précédent est très utile car elle permet de voir que pour qu'un nombre n'est pas constructible, il suffit de déterminer le degré de son polynôme minimal sur $\mathbb{Q}$.

Corollaire 51 :
$\mathcal{C}$ est le plus petit sous-corps de $\mathbb{C}$ qui est fermé pour l'opération d'extraction de racine carrée.

III.2 Application à la constructibilité du n-gone régulier

Théorème 52 : [Berhuy, p.929]
Soient $\alpha \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et $\mathbb{L}$ le corps de décomposition du polynôme minimal de α sur $\mathbb{Q}$.
α est constructible si, et seulement si, $[\mathbb{L} : \mathbb{Q}]$ est une puissance de 2.

Corollaire 53 : [Berhuy, p.787 - 788]
La trisection de l'angle, la duplication du cube et la quadrature du cercle sont impossibles à la règle non graduée et au compas.

Développement 1 : [cf. BERHUY]

Théorème 54 : Théorème de Gauss-Wantzel [Berhuy, p.795] :
Soit n un entier naturel supérieur ou égal à 2.
Le n-gone régulier est constructible à la règle non graduée et au compas si, et seulement si, $n := 2^s \prod_{i=1}^{r} p_i$ (avec $s, r \in \mathbb{N}$ et $p_1, ..., p_r$ qui sont r nombres de Fermat distincts).

Exemple 55 : [Berhuy, p.805]
Il est possible de construire le pentagone régulier avec la règle non graduée et le compas.

Remarque 56 :
Certaines constructions à la règle non graduée et au compas ne sont donc pas possibles (construction de l'heptagone régulier, trisection de l'angle, etc.) Mais que se passe-t-il si l'on modifie les règles du jeu (théorème de Mohr-Mascheroni, théorème de Poncelet-Steiner, règle avec deux graduations, allumettes, origamis, etc.) ?

IV 3 anneaux de nombres algébriques de la forme $\mathbb{Z}[\omega]$ aux structures différentes

IV.1 $\mathbb{Z}[i\sqrt{n}]$: un exemple d'anneau intègre non factoriel

Dans toute cette sous-partie, on considère $n \in \mathbb{N}^*$.

Définition 57 : $\mathbb{Z}[i\sqrt{n}]$ [Rombaldi (1), p.227] :
On note $\mathbb{Z}[i\sqrt{n}]$ **l'ensemble** : $\mathbb{Z}[i\sqrt{n}] = \mathbb{Z} + i\sqrt{n}\mathbb{Z} = \{a + ib\sqrt{n},\ (a,b) \in \mathbb{Z}^2\}$.

Proposition 58 : [Rombaldi (1), p.227]
$\mathbb{Z}[i\sqrt{n}]$ est un sous-anneau de $\mathbb{C}$ stable par conjugaison complexe et isomorphe à $\mathbb{Z}[X]/(X^2 + n)$.

Proposition 59 : [Rombaldi (1), p.227]
On a $\mathbb{Z}[i\sqrt{n}]^\times = \{u \in \mathbb{Z}[i\sqrt{n}] \text{ tq } |u| = 1\}$.
$*$ Pour $n = 1$, on a $\mathbb{Z}[i]^\times = \{-1; 1; -i; i\}$.
$*$ Pour $n \geq 2$, on a $\mathbb{Z}[i\sqrt{n}]^\times = \{-1; 1\}$.

Proposition 60 : [Rombaldi (1), p.227]
Les nombres premiers $p \geq 2$ dans $\mathbb{N}$ et réductibles dans $\mathbb{Z}[i\sqrt{n}]$ sont exactement les nombres p de la forme $p = a^2 + nb^2$.

Proposition 61 : [Rombaldi (1), p.227]
Pour $n \geq 3$, 2 est irréductible et non premier dans $\mathbb{Z}[i\sqrt{n}]$.

Corollaire 62 : [Rombaldi (1), p.226]
Pour $n \geq 3$, l'anneau $\mathbb{Z}[i\sqrt{n}]$ est intègre mais non factoriel.

IV.2 $\mathbb{Z}\left[\frac{1}{2}\left(1 + i\sqrt{19}\right)\right]$: un exemple d'anneau principal non euclidien

Proposition 63 : [Perrin, p.54]
Soit A un anneau euclidien.
Il existe un élément $x \in A$ non inversible tel que la restriction à $A^\times \cup \{0_A\}$ de la projection canonique de A sur $A/(x)$ soit surjective.

Remarque 64 : [Perrin, p.54]
Comme l'image d'un inversible est un inversible, $A/(x)$ est un corps et donc (x) est maximal.

Exemple 65 : [Perrin, p.54]
Pour $A = \mathbb{Z}[i]$, on a $A^\times = \{-1; 1; -i; i\}$ et on peut alors prendre $x = 1 - i$ (car $A/(1-i) \cong \mathbb{Z}/2\mathbb{Z}$).

Proposition 66 : [Perrin, p.54]
L'anneau $\mathbb{Z}\left[\frac{1}{2}\left(1 + i\sqrt{19}\right)\right]$ n'est pas euclidien.

Proposition 67 : [Perrin, p.55]
Soient $a, b \in \mathbb{Z}\left[\frac{1}{2}\left(1 + i\sqrt{19}\right)\right]$ non nuls.
Il existe $q, r \in \mathbb{Z}\left[\frac{1}{2}\left(1 + i\sqrt{19}\right)\right]$ tels que :
$*$ $r = 0$ ou $N(r) < N(b)$. $*$ $a = bq + r$ ou $2a = bq + r$.

Proposition 68 : [Perrin, p.55]
L'anneau $\mathbb{Z}\left[\frac{1}{2}\left(1 + i\sqrt{19}\right)\right]$ est principal.

IV.3 $\mathbb{Z}[i]$: un exemple d'anneau euclidien

Dans toute cette sous-partie, on pose $\Sigma = \{n \in \mathbb{N} \text{ tq } n = a^2 + b^2,\ a, b \in \mathbb{N}\}$, $\mathcal{P}$ l'ensemble des nombres premiers (au sens usuel) et une application (qui est multiplicative) $N : a + ib \longmapsto a^2 + b^2$ définie de $\mathbb{Z}[i]$ dans $\mathbb{N}$.

Définition 69 : L'anneau $\mathbb{Z}[i]$ [Perrin, p.56] :
On appelle **anneau** $\mathbb{Z}[i]$ l'anneau $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$ muni de l'addition et de la multiplication usuelles.

Remarque 70 :
$\mathbb{Z}[i]$ reste un anneau intègre car inclus dans $\mathbb{C}$, cependant les nombres premiers (au sens usuel) qui sont somme de deux carrés ne sont plus irréductibles dans $\mathbb{Z}[i]$ (par exemple $5 = (2 + i)(2 - i)$).

Proposition 71 : [Perrin, p.56]
$\mathbb{Z}[i]^\times = \{-1; 1; -i; i\}$.

Proposition 72 : [Perrin, p.56]
L'ensemble Σ est stable par multiplication.

Proposition 73 : [Perrin, p.57]
L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N.

Développement 2 : [cf. PERRIN]

Lemme 74 : [Perrin, p.57]
Soit $p \in \mathcal{P}$.
Les assertions suivantes sont équivalentes :
$*$ $p \in \Sigma$. $*$ L'élément p n'est pas irréductible dans $\mathbb{Z}[i]$.
$*$ On a $p = 2$ ou $p \equiv 1$ [4]

Théorème 75 : Théorème des deux carrés [Perrin, p.58] :
Soit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{N}$.
$n \in \Sigma$ si, et seulement si, pour tout $p \in \mathcal{P}$ vérifiant $p \equiv 3$ [4], l'entier $v_p(n)$ est pair.

Proposition 76 : [Perrin, p.58]
Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :
$*$ Les entiers premiers $p \in \mathbb{N}$ tels que $p \equiv 3$ [4].
$*$ Les entiers de Gauss $a + ib$ dont la norme est un nombre premier.

Proposition 77 : [Berhuy, p.530]
L'anneau $\mathbb{Z}[j] = \{a + bj,\ (a, b) \in \mathbb{Z}^2\}$ est un anneau euclidien qui possède 6 éléments inversibles.

Remarques sur le plan

— On peut s'intéresser d'avantage aux nombres transcendants en donnant d'autres exemples (nombres de Liouville, $\zeta(2k)$, etc.) ou bien résoudre l'équation de Fermat dans des cas particuliers grâce aux propriétés des anneaux $\mathbb{Z}[i\sqrt{n}]$.

— Il est également possible de s'intéresser aux nombres complexes (construction de $\mathbb{C}$, utilité en arithmétique et en géométrie, etc.) ou bien encore d'approximation diophantienne et de fractions continues.

Liste des développements possibles

— Théorème de Gauss-Wantzel.

— Théorème des deux carrés.

Bibliographie

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.

— Claude Deschamps, *Tout-en-un MPSI*.

— Jean-Étienne Rombaldi, *Éléments d'analyse réelle*.

— Daniel Perrin, *Cours d'algèbre*.

— Jean-Pierre Escofier, *Théorie de Galois*.

— Grégory Berhuy, *Algèbre : le grand combat*.