NOM : TOUVENET

Prénom : Jules

Rouge entourez l'épreuve Bleu

entourez le Jury A B C D E F

Sujet choisi : 127 - Exemples de nombres remarquables. Exemples d'irrationnels et de nombres remarquables. Applications.

Autre sujet :

I. Irrationnalité & Transcendance

I.1. Nombres rationnels & Nombres irrationnels

Déf 1 : On définit l'ensemble des rationnels par : $\mathbb{Q} = \{\frac{a}{b} \mid (a,b) \in \mathbb{Z} \times \mathbb{N}^*\}$
$\mathbb{Q}$ est le corps des fractions de l'anneau des entiers $\mathbb{Z}$.

Prop 2 : $\mathbb{Q}$ est le plus petit corps de caractéristique nulle à isomorphisme près.

Déf 3 : On définit l'ensemble des réels comme le complété de $\mathbb{Q}$ pour la distance induite par la norme $|\cdot|$.
On définit l'ensemble des irrationnels comme l'ensemble $\mathbb{R} \setminus \mathbb{Q}$

Prop 4 : Soit $d \in \mathbb{N}$. $\sqrt{d}$ est rationnel ssi d est un carré parfait.

Prop 5 : Soit $d \in \mathbb{N}$. $\log_2(d)$ est rationnel ssi d est une puissance de 2.

Prop 6 : e et π sont irrationnels.

Thm 7 : Soit $p \in \mathbb{N}_{\geq 2}$. Soit $x \in \mathbb{R}_+$. Il existe une unique suite $(c_n) \in \mathbb{R}^{\mathbb{N}}$ telle que :
- $c_0 = \lfloor x \rfloor$
- $\forall n \in \mathbb{N}$, $c_n \in \{0, 1, \dots, p-1\}$
- (c_n) ne stationne pas à $p-1$
- $\sum_{n=0}^{+\infty} \frac{c_n}{p^n} = x$.

Déf 8 : (c_n) est appelé développement p-adique de x.

Rem 9 : Si $p = 10$, on retrouve le développement décimal.

Prop 10 : Le développement p-adique de $x \in \mathbb{R}_+$ est donné algorithmiquement par $(\lfloor \gamma_n \rfloor)_{n \in \mathbb{N}}$ où (γ_n) est définie par : $\gamma_0 = x$ et $\forall n \in \mathbb{N}$, $\gamma_{n+1} = p\gamma_n - \lfloor \gamma_n \rfloor$.

Ex 11 : Soit $p \geq 2$. $\frac{1}{p+1}$ a pour développement p-adique la suite : $(0, p-1, 0, p-1, 0, p-1, \dots)$

Ex 12 : Un nombre décimal est un nombre dont le développement décimal est fini (ie stationne à 0).

Thm 13 : Soit $x \in \mathbb{R}_+$. Les assertions suivantes sont équivalentes :
- $x \in \mathbb{Q}$
- $\exists p \geq 2$, le développement p-adique de x est périodique à partir d'un certain rang.
- $\forall p \geq 2$, le développement p-adique de x est périodique à partir d'un certain rang.

App 14 : $\sum_{n=0}^{+\infty} \frac{1}{10^{n^2}}$ est irrationnel.

I.2. Nombres algébriques & Nombres transcendants

Déf 15 : Soit $\alpha \in \mathbb{C}$. Soit $ev_\alpha : \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & \mathbb{Q}[\alpha] \\ P(X) & \longmapsto & P(\alpha) \end{array}$
Si ev_α n'est pas injective, α est dit algébrique.
Si ev_α est injective, α est dit transcendant.

Déf 16 : On note $\overline{\mathbb{Q}}$ l'ensemble des complexes algébriques.

Prop 17 : $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.

Déf 18 : On appelle polynôme minimal de $\alpha \in \overline{\mathbb{Q}}$ l'unique polynôme unitaire générateur de l'idéal $\ker(ev_\alpha)$.
On le note π_α. π_α est irréductible dans $\mathbb{Q}[X]$.

Ex 19 : Soit p premier. $\sqrt{2}$, i et $e^{\frac{2i\pi}{p}}$ sont algébriques.
Leurs polynômes minimaux sont $X^2 - 2$, $X^2 + 1$ et $X^{p-1} + \dots + X + 1$.

Prop 20 : Soit $\alpha \in \mathbb{C}$. Les assertions suivantes sont équivalentes :
- $\alpha \in \overline{\mathbb{Q}}$
- $\mathbb{Q}(\alpha) / \mathbb{Q}$ est algébrique
- $[\mathbb{Q}(\alpha) : \mathbb{Q}] < +\infty$

Prop 21 : $\overline{\mathbb{Q}}$ est dénombrable.

Cor 22 : Il existe des nombres transcendants. (Et beaucoup...)

Thm 23 : (Liouville)
Soit $\alpha \notin \mathbb{Q}$ algébrique et $d := \deg(\pi_\alpha)$.
$\exists C > 0$, $\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*$, $|\alpha - \frac{p}{q}| \geq \frac{C}{q^d}$.

Déf 24 : On dit que $\alpha \notin \mathbb{Q}$ est un nombre de Liouville si pour tout entier n assez grand il existe $\frac{p}{q} \in \mathbb{Q}$ avec $q \geq 2$ tel que $|\alpha - \frac{p}{q}| < \frac{1}{q^n}$.

Thm 25 : Tout nombre de Liouville est transcendant.

App 26 : $\sum_{k=0}^{+\infty} \frac{1}{10^{k!}}$ est transcendant.

Thm 27 : (Hermite-Lindemann, admis)
Si $\alpha \neq 0$ est algébrique, alors e^α est transcendant.

Cor 28 : e et π sont transcendants.

II. Corps de nombres

II.1. Définition

Déf 29 : Un corps de nombres est une extension finie de $\mathbb{Q}$.

Ex 30 : Soit $\alpha \in \mathbb{C}$ algébrique de degré d. $\mathbb{Q}(\alpha)$ est un corps de nombres et $\{1, \alpha, \dots, \alpha^{d-1}\}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$.

Déf 31 : Si $d \in \mathbb{Z}$ est sans facteur carré, alors on dit que $\mathbb{Q}(\sqrt{d})$ est un corps de nombres quadratique dont $\{1, \sqrt{d}\}$ est une $\mathbb{Q}$-base.

Thm 32 : Si $\mathbb{K}$ est un corps de nombres, alors il existe $\alpha \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{Q}(\alpha)$.

Ex 33 : $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{3} + \sqrt[3]{2})$.

II.2. Extensions cyclotomiques

Déf 34 : Une extension cyclotomique est un corps de nombres de la forme $\mathbb{Q}(\zeta_n)$ où $\zeta_n = e^{\frac{2i\pi}{n}}$ et $n \in \mathbb{N}^*$.

Déf 35 : On note $\mathbb{U}_n = \{\omega \in \mathbb{C} \mid \omega^n = 1\}$ l'ensemble des racines $n^{ème}$ de l'unité.
On note $\mathbb{U}_n^\times = \{\omega \in \mathbb{U}_n \mid \langle \omega \rangle = \mathbb{U}_n\}$ l'ensemble des racines primitives $n^{ème}$ de l'unité.

Prop 36 : $\mathbb{U}_n = \{e^{\frac{2i\pi k}{n}} \mid k \in [\![1, n]\!]\}$, $\mathbb{U}_n^\times = \{e^{\frac{2i\pi k}{n}} \mid k \in [\![1, n]\!], k \wedge n = 1\}$

Prop 37 : $\#\mathbb{U}_n^\times = \varphi(n) := \#\{k \in [\![1, n]\!], k \wedge n = 1\}$

Déf 38 : $\Phi_n(X) := \prod_{\omega \in \mathbb{U}_n^\times} (X - \omega)$ est appelé $n^{ème}$ polynôme cyclotomique.

Prop 39 : $X^n - 1 = \prod_{d \mid n} \Phi_d$ et si p est premier, $\Phi_p = X^{p-1} + \dots + X + 1$.

Cor 40 : $\Phi_n(X) \in \mathbb{Z}[X]$.

Thm 41 : Φ_n est irréductible dans $\mathbb{Q}[X]$.

App 42 : (Théorème de progression arithmétique de Dirichlet, version faible)
Il existe une infinité de premiers congrus à 1 modulo n.

Cor 43 : $\mu_{\zeta_n} = \Phi_n$ et $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Prop 44 : Si p est premier, alors $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$ est cyclique d'ordre $p-1$.

II.3. Applications aux constructions à la règle et au compas

Déf 45 : Soit E une partie de $\mathbb{C}$. On dit que $\alpha \in \mathbb{C}$ est constructible à partir de E si α est une intersection entre une droite passant par deux points de E et un cercle de centre un point de E et de rayon une distance entre deux points de E ou une intersection de deux droites ou de deux cercles.

Déf 46 : On définit par récurrence $(E_n) \in \mathcal{P}(\mathbb{C})^{\mathbb{N}}$ par $E_0 = \{0, 1\}$ et $\forall n \in \mathbb{N}$ E_{n+1} est l'ensemble des nombres constructibles à partir de E_n.
On note $\mathbb{E} := \bigcup_{n \geq 0} E_n$ l'ensemble des nombres constructibles.

Prop 47 : $\mathbb{E}$ est un corps contenant $\mathbb{Q}$ et stable par racines carrées.

Prop 48 : Soient $a, b \in \mathbb{R}$. $a + ib \in \mathbb{E} \iff a, ib \in \mathbb{E}$

Thm 49 : (Wantzel) $\alpha \in \mathbb{C}$ est constructible ssi il existe $\mathbb{K}_0 \subset \dots \subset \mathbb{K}_m$ une tour d'extensions telle que : • $\mathbb{K}_0 = \mathbb{Q}$ • $\alpha \in \mathbb{K}_m$
• $\forall i \in [\![0, m-1]\!]$, $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$

Cor 50 : Si $\alpha \in \mathbb{C}$ est constructible, alors $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est une puissance de 2.

App 51 : (Quadrature du cercle)
Un carré dont l'aire vaudrait celle d'un cercle de rayon constructible n'est pas constructible. (Car π n'est pas algébrique.)

App 52 : (Duplication du cube)
Un cube dont le volume vaudrait celui d'un cube de côté constructible n'est pas constructible. (Car $\sqrt[3]{2}$ est de degré 3.)

Ex 53 : La réciproque du corollaire du théorème de Wantzel est fausse.
L'une des deux (au moins) racines réelles de $X^4 - X - 1$ n'est pas constructible alors qu'elle a degré $4 = 2^2$.

Thm 54 : Soit p premier impair et $\alpha \in \mathbb{N}^*$. $\zeta_p \alpha \in \mathbb{E} \iff \begin{cases} \exists m \in \mathbb{N}, p = 1 + 2^m \\ \alpha = 1 \end{cases}$

Cor 55 : (Gauss-Wantzel) Soit $n \geq 3$.
Le n-gone régulier est constructible ssi n est de la forme $n = 2^\alpha p_1 \dots p_r$ avec $\alpha \in \mathbb{N}^*$ et $\forall i \in [\![1, r]\!]$, $p_i = 1 + 2^{m_i}$ premier.

DEV 1

III. Anneau des entiers d'un corps de nombres

III.1. Entiers algébriques

Déf 56 : $\alpha \in \mathbb{C}$ est appelé entier algébrique s'il est annulé par un polynôme unitaire à coefficients entiers. On note $\mathbb{A}$ l'ensemble des entiers algébriques.

Prop 57 : $\mathbb{A}$ est un anneau inclus dans $\overline{\mathbb{Q}}$.

Prop 58 : Soit $\alpha \in \mathbb{C}$. $\alpha \in \mathbb{A} \iff (\alpha \in \overline{\mathbb{Q}}$ et $\mu_\alpha \in \mathbb{Z}[X])$

Ex 59 : $i \in \mathbb{A}$, $\sqrt{2} \in \mathbb{A}$, $\frac{2}{\sqrt{2}} \notin \mathbb{A}$, $\frac{1+i\sqrt{5}}{2} \in \mathbb{A}$, $\frac{1+i\sqrt{3}}{2} \notin \mathbb{A}$.

Déf 60 : Soit $\mathbb{K}$ un corps de nombres. On définit $\mathcal{O}_\mathbb{K}$ l'anneau des entiers de $\mathbb{K}$ par : $\mathcal{O}_\mathbb{K} := \mathbb{K} \cap \mathbb{A}$.

Prop 61 : Soit $\mathbb{K}$ un corps de nombres. $\mathcal{O}_\mathbb{K}$ est un sous-anneau de $\mathbb{A}$.

Ex 62 : • $\mathcal{O}_{\overline{\mathbb{Q}}} = \mathbb{A}$ • $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$

III.2. Anneau des entiers d'un corps de nombres quadratique

Déf 63 : On dit qu'un corps de nombres quadratique $\mathbb{Q}(\sqrt{d})$ est réel si $d > 0$ et imaginaire si $d < 0$.

Déf 64 : L'application $N : \begin{array}{ccc} \mathbb{Q}(\sqrt{d}) & \longrightarrow & \mathbb{Z} \\ a+b\sqrt{d} & \longmapsto & a^2 - db^2 \end{array}$ est appelée norme de $\mathbb{Q}(\sqrt{d})$.

Thm 65 : Soit $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ un corps quadratique. Alors,

$$\mathcal{O}_\mathbb{K} = \begin{cases} \mathbb{Z}[\sqrt{d}] \text{ si } d \equiv 2, 3 \ [4] \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{\alpha+\beta\sqrt{d}}{2} \mid \alpha, \beta \in \mathbb{Z} \text{ de même parité}\right\} \text{ si } d \equiv 1 \ [4] \end{cases}$$

Ex 66 : • $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$ • $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ • $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ • $\mathcal{O}_{\mathbb{Q}(i\sqrt{3})} = \mathbb{Z}[j]$

Déf 67 : Soit $\mathbb{K}$ quadratique. $\mathcal{O}_\mathbb{K}^\times$ est le groupe des unités de $\mathcal{O}_\mathbb{K}$.

Prop 68 : Soit $\mathbb{K}$ quadratique. $\mathcal{O}_\mathbb{K}^\times = \{z \in \mathcal{O}_\mathbb{K} \mid N(z) = \pm 1\}$.

Prop 69 : Soit $\mathbb{K} = \mathbb{Q}(i\sqrt{d})$ avec $d > 0$ un corps quadratique imaginaire.
Si $d = 1$, $\mathcal{O}_\mathbb{K}^\times = \{\pm 1, \pm i\}$. Si $d = 3$, $\mathcal{O}_\mathbb{K}^\times = U_6$. Sinon, $\mathcal{O}_\mathbb{K}^\times = \{\pm 1\}$.

Lemme 70 : Soit $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ avec $d > 0$ un corps quadratique réel.
$\forall \varepsilon \in \mathcal{O}_\mathbb{K}^\times$, $\varepsilon > 1 \Rightarrow \varepsilon \geq \frac{1+\sqrt{d}}{2}$.

Thm 71 : $\exists \omega > 1$, $\mathcal{O}_\mathbb{K}^\times = \{\pm \omega^n \mid n \in \mathbb{Z}\}$ ω est appelée unité fondamentale.

Ex 72 : $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}^\times = \left\{\left(\frac{1+\sqrt{5}}{2}\right)^n \mid n \in \mathbb{Z}\right\}$

Thm 73 : Soit $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ quadratique. $\mathcal{O}_\mathbb{K}$ est euclidien (et donc factoriel) pour $d = -11, -7, -3, -2, -1, 2, 3, 5$ et 13.

Prop 74 : Soit $\mathbb{K}$ quadratique et $z \in \mathbb{K}$. Si $N(z)$ est premier dans $\mathbb{Z}$, alors z est irréductible dans $\mathcal{O}_\mathbb{K}$.

Ex 75 : Pour $d = -5$, $\mathcal{O}_\mathbb{K} = \mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

App 76 : $1, -1, i$ et $-i$ sont les seuls complexes de partie réelle et imaginaire rationnelles dont l'argument est commensurable à π.

III.3. Application à la résolution d'équations diophantiennes

App 77 : (de la factorialité de $\mathbb{Z}[i\sqrt{2}]$)
26 est l'unique entier $n \in \mathbb{Z}$ tel que $n-1$ est un carré et $n+1$ est un cube. C'est-à-dire que l'équation diophantienne $x^2 + 2 = y^3$ admet pour solutions $(5, 3)$ et $(-5, 3)$.

Rem 78 : 0 est l'unique entier encadré par un cube et un carré. Mais c'est plus dur à montrer...

Prop 79 : $\mathbb{Z}[i]$ est factoriel.

App 80 : Soit p premier. $p \in \Sigma := \{a^2 + b^2 \mid a, b \in \mathbb{Z}\} \iff p = 2$ ou $p \equiv 1 \ [4]$

Thm 81 : (Théorème des deux carrés) Soit $n \in \mathbb{N}$.
$n \in \Sigma \iff (\forall p$ premier tel que $p \mid n$, $p \equiv 3 \ [4] \Rightarrow v_p(n)$ est pair$)$

DEV2

Déf 82 : Soit $d > 0$ sans facteur carré. On appelle l'équation diophantienne $x^2 - dy^2 = -1$ est appelée équation de Pell-Fermat.

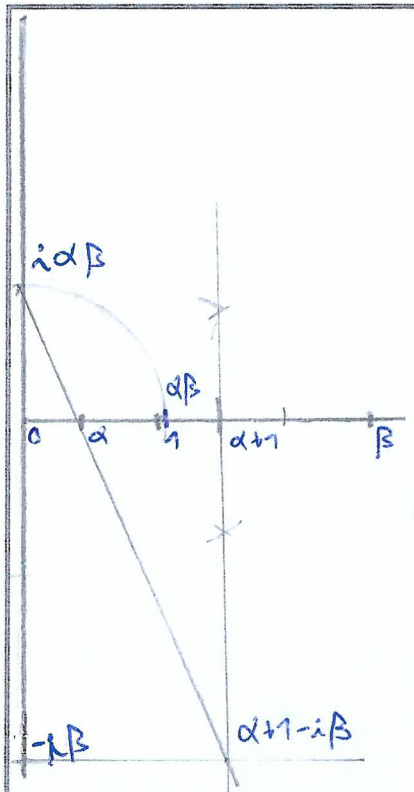
Thm 83 : Les solutions $(x_n, y_n)_{n \in \mathbb{N}}$ telles que $\forall n \in \mathbb{N}$, $x_n, y_n \geq 0$ de l'équation de Pell-Fermat sont données par la relation de récurrence :

$$\begin{cases} x_{n+2} = 2x_{n+1} x_{n+1} - x_n \\ y_{n+2} = 2x_{n+1} y_{n+1} - y_n \end{cases}$$

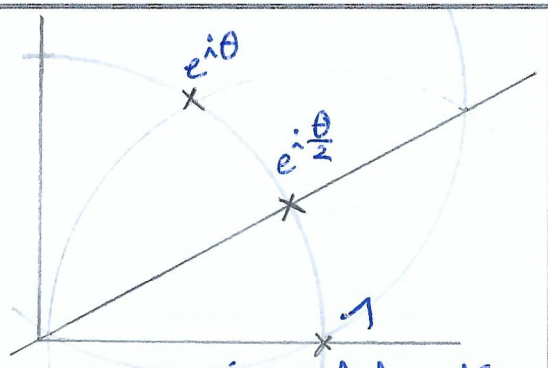
avec $(x_0, y_0) = (1, 0)$ et (x_1, y_1) tel que $x_1 + y_1\sqrt{d}$ est une unité fondamentale de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

App 84 : Une formation triangulaire de canons se divise en deux formations triangulaires de taille égal. Il y a $\frac{n(n+1)}{2}$ canons ou $n = \sum_{i=0}^{k} 2^{i-1}\binom{2k+1}{2i}$ avec $k \in \mathbb{N}$.

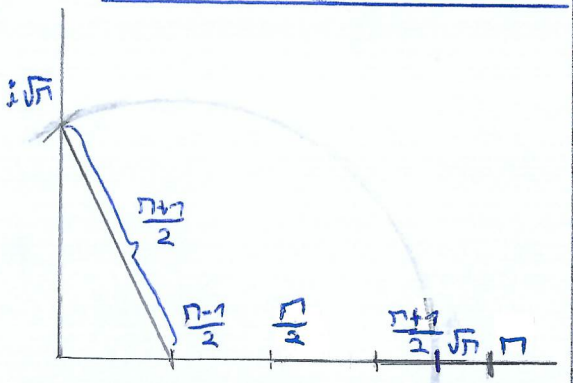
App 85 : 4900 est l'unique carré à être un nombre pyramidal.



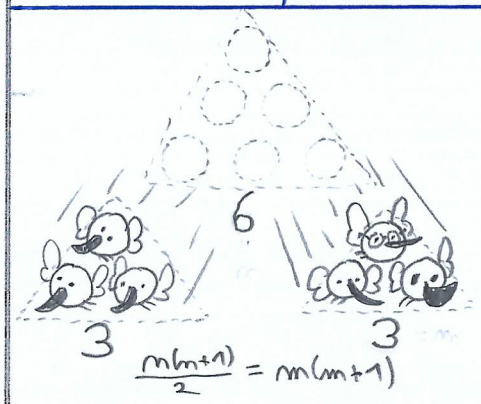
Construction du produit



Construction de la bissectrice

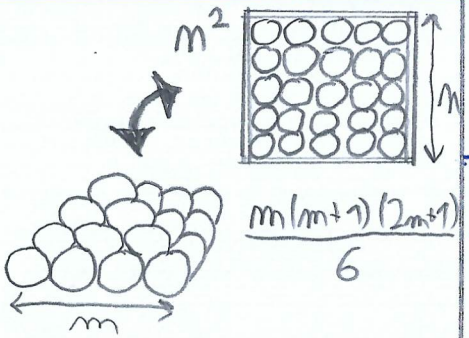


Construction de la racine



$\frac{n(n+1)}{2} = n(n+1)$

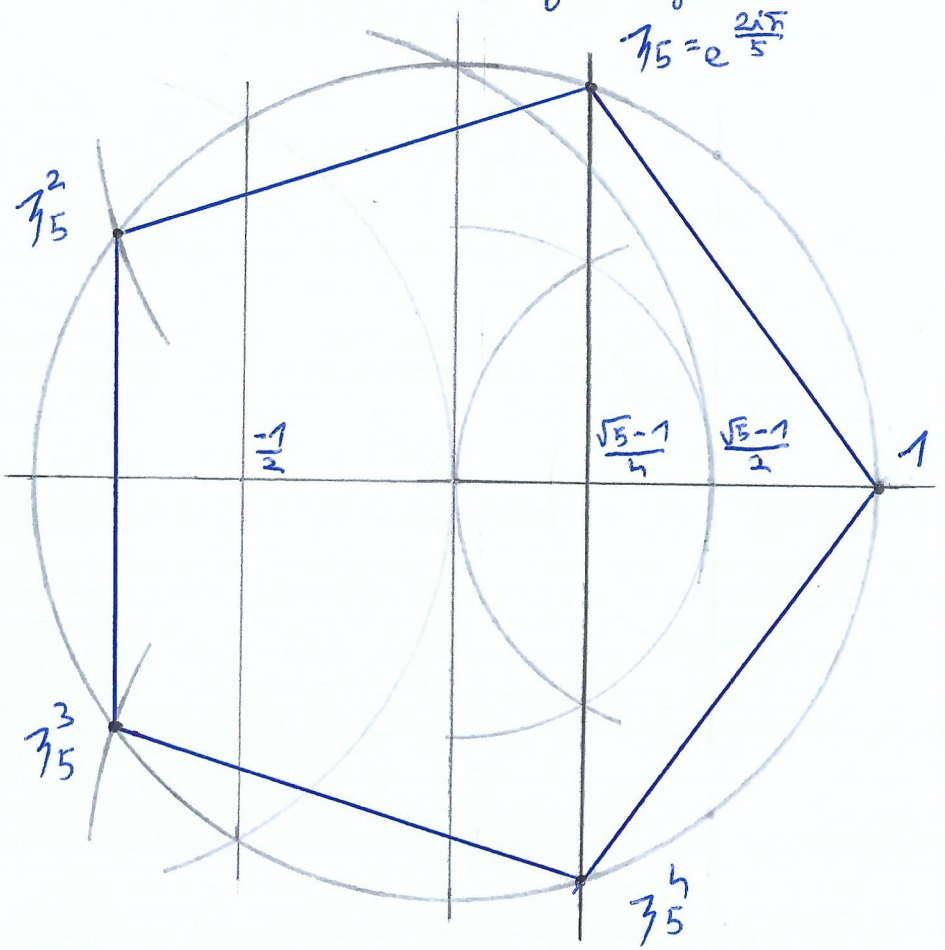
Illustration de l'application 84



$\frac{n(n+1)(2n+1)}{6}$

Illustration de l'application 85

Construction du pentagone régulier



Références :

- ✱ Théorie des nombres (Duverney)
  → I, II.1, III.1, III.2
- ✱ Algèbre, le grand combat (Berhuy)
  → II.2, II.3
- ✱ Carnets de voyage en algèbre (Caldero)
  → III.3

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

1 Commentaires généraux

Comme tout ce qui se trouve sur Agreg-Maths, ne prenez rien pour argent comptant. Des erreurs sèment sans doute le document. Il n'y a pas de bon ou de mauvais choix pour rédiger un plan, seulement des choix bien ou mal motivés. Une décision devient pertinente au moment où l'on peut s'en convaincre soi-même et en convaincre les autres.

Le plan a été écrit pour être présenté en classe, en temps illimité. Le plan est donc strictement plus long que ce que j'aurais pu faire en conditions réelles.

Cette leçon est assez mal aimée car elle demande des connaissances exclusives. Etant fan de théorie des nombres, je me suis fait plaisir. Notez que quasiment rien de ce que j'ai abordé n'est un impératif pour cette leçon.

Le piège principal de cette leçon selon moi est de penser que « nombre remarquable » puisse signifier ce qu'on veut et s'autoriser à faire n'importe quoi. Avec un peu de répartie et de mauvaise fois, tout nombre peut être « remarquable ». Il s'agit bien d'une leçon de théorie des nombres. La façon dont j'ai construit mon plan est explicitée par ma défense détaillée ci-dessous.

2 Défense de plan

Il ne s'agit pas de ma défense mot pour mot mais juste des idées clefs.

Mon accroche était sur l'idée qu'en mathématiques, on peut attaquer un problème en le considérant dans un espace plus grand. On pense au passage de $\mathbb{R}$ à $\mathbb{C}$ qui simplifie, par exemple, l'étude des rotations du plan ou des polynômes. Comment cela s'applique en algèbre (étude de $\mathbb{Q}$) et en arithmétique (étude de $\mathbb{Z}$) ?

L'idée naïve de passer dans $\mathbb{R}$ pour étudier $\mathbb{Q}$ est mauvaise car l'élargissement est trop grossier. En effet, si on connaît plein de choses sur les réels algébriques grâce à l'existence d'un polynôme minimal, on ne sait pas grand chose des transcendants. Or ces derniers constituent l'essentiel des nombres réels au sens où l'ensemble des nombres algébriques est dénombrable. A ce moment là on peut toucher un mot sur les nombres transcendants. Par exemple en parlant du théorème de Liouville, ou bien du théorème de Hermite-Lindemann (en insistant sur la difficulté à le prouver bien que la transcendance de e et de π soit un résultat de culture général mathématique).

Donc pour appliquer cette stratégie d'élargissement de l'ensemble à $\mathbb{Q}$ on doit étudier des extensions de $\mathbb{Q}$ finies, c'est-à-dire des corps de nombres. Un cas particulier intéressant est celui des extensions cyclotomiques desquelles découle une belle application géométrique via les constructions à la règle et au compas. Je mentionne alors mon premier développement.

Pour appliquer notre stratégie en arithmétique, c'est encore plus subtil. Déjà, le passage de $\mathbb{Z}$ à $\mathbb{Q}$ est trop brutal. $\mathbb{Q}$ étant un corps, on ne peut plus y faire d'arithmétique. La seule façon d'élargir un espace que l'on utilise depuis le début, c'est les extensions de corps. La question qu'on peut se poser est : Est-il possible de trouver une description de $\mathbb{Z}$ à partir de $\mathbb{Q}$ qui une fois appliquée à un corps de nombres $\mathbb{K}$ nous fournissent $\mathcal{O}_{\mathbb{K}}$, un élargissement de $\mathbb{Z}$? Oui : $\mathbb{Z}$ est l'ensemble des des éléments de $\mathbb{Q}$ ayant un polynôme minimal à coefficients entiers. On étudie l'exemple des corps quadratiques $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ dont l'anneau des entiers $\mathcal{O}_{\mathbb{K}}$ est $\mathbb{Z}[\sqrt{d}]$ ou $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ en fonction de la congruence modulo 4 de d. (Pour conclure cette discussion qui motive la définition de l'anneau des entiers, il faudrait un résultat choc qui assure qu'on peut toujours faire de l'arithmétique dans $\mathcal{O}_{\mathbb{K}}$. Idéalement, on voudrait que $\mathcal{O}_{\mathbb{K}}$ soit toujours factoriel. Cependant c'est faux. Ce qui est vrai, c'est que c'est un anneau de Dedekind. Et on en est très content en théorie des nombres car on à un équivalent du théorème fondamental de l'arithmétique dans les anneaux de Dedekind qui dit qu'on a une écriture unique d'un idéal en produit d'idéaux premiers (aux inversibles près). Ca justifie pourquoi il ne suffit pas d'étudier $\mathbb{Z}[\sqrt{d}]$ dès qu'on veut manipuler $\sqrt{d}$. Pour $d \equiv 1[4]$ on ne tombe pas forcément sur un anneau de Dedekind ! Evidemment tout ça dépasse de loin le cadre de la leçon mais c'est intéressant et c'est surtout la fin de la justification propre de la définition des anneaux d'entiers.) On mentionne ensuite les applications aux équations diophantiennes dont notamment mon deuxième développement.

3 Développements

Mon premier développement est le théorème de Gauss-Wantzel. Il se motive comme application des corps de nombres. (Et surtout pas en disant qu'être constructible est une propriété remarquable ! Sinon on retombe dans le piège d'interpréter la notion de « nombre remarquable » comme bon nous semble.) Il est d'un bon niveau et nécessite de faire des choix sur quels points on détaille et quels points on omet. Personnellement je justifiais le calcul du groupe de Galois à l'oral. (Ca n'a jamais vraiment plu aux différents jury auquels j'ai pu montrer ça. Donc faut être béton sur la justification.) Evidemment il faut savoir faire la construction du pentagone. Elle est à apprendre par coeur et fait toujours joli en annexe.

Mon deuxième développement est le théorème des deux carrés. Il n'est pas très dur et pas très original mais est très pertinent dans la leçon et se recase bien. Je fais la preuve de la factorialité de $\mathbb{Z}[i]$, le théorème dans le cas d'un nombre premier, puis le théorème dans le cas général. Faire moins serait un peu léger. Mais du coup ça fait beaucoup. Pas le droit de bégayer !

4 Détails de quelques items

Définition 3

C'est un peu maladroit parce que d'habitude la norme $|\cdot|$ est définie sur $\mathbb{R}$ et la notion de complétée écrite comme ça est vague. Le point sur lequel je voulais insister est que la construction de $\mathbb{R}$ est analytique. Mieux vaudrait retirer cet item et faire passer cette idée pendant la défense.

Proposition 5

C'est issu du théorème fondamental de l'arithmétique.

Items 7 à 14

Parler de développement p-adique est pertinent dans la leçon et s'ancre dans ma sous-partie grâce au théorème 13 qui en fait un test d'irrationnalité illustré dans l'exemple 14. Cependant ça n'a pas trop sa place dans l'angle avec lequel j'attaque la leçon. D'ailleurs je ne parle pas de cette première sous-partie dans ma défense. Mais ça ferait un peu bizarre de ne pas en parler et rendrait mon I. assez vide. Donc puisque ce n'est pas bien dur ça ne coûte rien de le mettre.

Corollaire 28

La transcendance de π est bien un corollaire de Hermite-Lindemann. On applique la contraposée avec $\alpha = i\,\pi$.

Théorème 41

Résultat non-trivial. Attention, on en a besoin si on fait Gauss-Wantzel ! En effet, on a besoin de connaître le polynôme minimal des extensions cyclotomiques… Donc il faut avoir conscience qu'on l'utilise et avoir en tête une idée de la preuve. (Gauss-Wantzel nous force donc à parler de cyclotomie dans toutes les leçons où on le recase…)

Application 42

C'est un résultat connu et ça fait donc une belle application de l'irréductiblité des polynômes cyclotomiques. Par contre ce n'est pas immédiat. Mais ça vaut le coup d'y passer un peu de temps. (Ca serait trop court pour un développement par contre.) C'est très bien fait dans le Berhuy.

Proposition 44

Je l'écris proprement là pour pouvoir m'y référer pendant mon développement sur Gauss-Wantzel. (Attention, je donne quand même l'idée de la preuve à l'oral parce que c'est quand même central dans le développement.)

Définitions 45 & 46

C'est la façon la plus économique que j'ai trouvé pour introduire l'ensemble des nombres constructibles. Je faisais toute cette section III. de tête car je n'ai jamais trouvé de bouquin qui faisait correctement les constructions à la règle et au compas. (C'est-à-dire dans le plan complexe. Pourquoi tout le monde fait ça dans $\mathbb{R}^2$?? Quelle horreur…) Le moins pire est le Berhuy parce qu'il y a pas mal de dessins.

Exemple 53

Contre-exemple au théorème de Wantzel indispensable. Il y a des vidéos de Caldero dessus pour les détails.

Exemple 62

Attention, écrit tel quel $\mathcal{O}_{\bar{\mathbb{Q}}}$ n'a pas de sens car $\bar{\mathbb{Q}}$ n'est pas un corps de nombres…

Lemme 70 et théorème 71

Le théorème se déduit du lemme + l'existence d'un $\varepsilon > 1$ dans $\mathcal{O}_{\mathbb{K}}^{\times}$. Or ce dernier point n'est pas trivial et ne se déduit pas de quoi que ce soit de mon plan ! On peut trouver un tel ε via les fractions continues. On peut aborder les fractions continues dans cette leçon et ça peut faire un beau lien avec les unités fondamentales. Je voulais parler de ça pour traiter les équations de Pell-Fermat. A posteriori, vu la densité de mon plan, j'aurais pu laisser tomber ça. Bref. Il faut avoir conscience de tout ça si vous en parlez.

Application 77 et remarque 78

Il y a une vidéo de Caldero là-dessus pour les curieux.

Proposition 79

Cet énoncé est strictement inclus dans le théorème 73 mais je l'énonce à nouveau pour bien montrer ce que je vais démontrer pendant mon développement.

Théorème 85

Je me moque un peu du monde. Cet item est issu d'une discussion que j'ai eu avec Philippe Caldero (je me la pète). C'est connu sous le nom du problème des boulets de canon. On peut commencer à attaquer le problème par des disjonctions de cas pour se ramener à plusieurs équations de Pell-Fermat. Mais je n'ai pas trouvé de références où c'est rédigé en entier. Pour les intéressés : https://en.wikipedia.org/wiki/Cannonball_problem

5 Références

cf. l'annexe