Rapport du 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 (√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.

Références

- Cours d'Algèbre - Daniel Perrin
- Cours d'algèbre - Demazure
- Théorie de Galois - Escofier
- Modules sur les anneaux commutatifs - Diaz Toca, Lombardi et Quitté
- Mathématiques pour l'Agrégation (Algèbre) - J.E. Rombaldi
- Petit guide du calcul différentiel - Rouvière

Développements

- Test de Solovey Strassen
- Norme d'une extension

Méta-plan

1. Algébricité
    1. Nombres algébriques, nombres transcendants
    2. Norme d'un élément algébrique
    3. Corps de nombres
2. Nombres premiers
    1. L'ensemble des nombres premiers
    2. Résidus quadratiques
3. Anneaux d'entiers
    1. Introduction par un exemple : les entiers de Gauss
    2. Théorie générale

Plan détaillé

I - Algébricité

1 - Nombres algébriques, nombres transcendants [Rombaldi, Escofier, Rouvière]

1. Définition (élément algébrique, élément transcendant) : Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit algébrique sur K s'il est annulé par un polynôme non nul à coefficients dans K. Dans le cas contraire, il est dit transcendant.
2. Exemples :
    1. Si q est un rationnel et p est un entier, $\sqrt[p]{q}$ est algébrique sur $\mathbb{Q}$.
    2. Si K est un corps, l'indéterminée $X \in K(X)$ est transcendante sur K.
    3. Le nombre de Liouville est transcendant sur $\mathbb{Q}$.
    4. π et e sont transcendants sur $\mathbb{Q}$ (admis)
3. Définition : polynôme minimal. Degré d'un élément algébrique.

4. Théorème (caractérisation des nombres alégbriques) : $\alpha \in L$ est algébrique sur K si, et seulement si, $K(\alpha)$ est un K-ev de dimension finie. Dans ce cas, sa dimension est le degré de α et $K(\alpha) \cong K[X]/\langle \pi_\alpha \rangle$.
5. Théorème (caractérisation des nombres transcendants) : $\alpha \in L$ est transcendant sur K si, et seulement si, $K(\alpha)$ est un K-ev de dimension infinie. Dans ce cas, $K[\alpha] \cong K[X]$ et $K(\alpha) \cong K(X)$ en tants que K-algèbres.
6. Application : $\mathbb{C}$ peut être construit comme le corps $\mathbb{R}[X]/\langle X^2+1 \rangle$. L'unité imaginaire i est alors définit comme la classe de X dans le quotient.
7. Théorème : Soit L un corps algébriquement clos et K un sous corps de L. L'ensemble des éléments de L algébriques sur K est une clôture algébrique de K.

2 - Norme d'un élément algébrique [Tauvel]

1. Proposition : Soit L/K une extension finie. Pour tout $\alpha \in L$, l'application $m_\alpha : x \mapsto \alpha x$ est K-linéaire sur L. De plus, l'application $\alpha \mapsto m_\alpha$ est un morphisme de K-algèbres injectif.
2. Définition : on appelle norme de $\alpha \in L$ sur K le déterminant de m_α. C'est un élément de K.
3. Exemples :
    1. Si $\alpha \in K$, $N(\alpha) = \alpha^{[L:K]}$.
    2. Pour tout $z = a + ib \in \mathbb{Q}(i)$, $N_{\mathbb{Q}(i)/\mathbb{Q}}(z) = a^2 + b^2 = |z|^2$
    3. $N(\alpha) = 0 \iff \alpha = 0$.
4. Proposition (DVT 1, partie 1/3):
    1. La norme est multiplicative : $N(\alpha\beta) = N(\alpha)N(\beta)$.
    2. On note $n := [L : K]$ et $d := \deg(\alpha)$. On a $N(\alpha) = [\pi_\alpha(0)]^{n/d}$.
    3. Si M/L est une extension dans laquelle π_α est scindé de racines $\omega_1, \dots, \omega_d$, alors $N_{L/K}(\alpha) = [\prod \omega_i]^{n/d}$

3 - Corps de nombres [Escoffier]

a) Théorie générale

1. Définition (corps de nombre) : on appelle corps de nombre toute extension finie de $\mathbb{Q}$.
2. Exemples :

    1. Les corps cyclotomiques $\mathbb{Q}(\omega)$ sont des corps de nombres.
    2. Le corps de nombres algébriques $\bar{\mathbb{Q}}$ n'est pas considéré comme un corps de nombres.
3. Théorème : soit α un nombre algébrique de degré n. Il existe exactement n morphismes d'extensions $\mathbb{Q}(\alpha)/\mathbb{Q} \to \mathbb{C}/\mathbb{Q}$.
4. Corollaire (théorème de l'élément primitif) : soit $K/\mathbb{Q}$ un corps de nombres. Il existe un nombre algébrique $\alpha \in K$ tel que $K = \mathbb{Q}(\alpha)$.
5. Exemple : $\sqrt{2} + i$ est un élément primitif de l'extension $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$.

b) Corps cyclotomiques

1. Définition (racine primitive de l'unité) : un nombre complexe ω est appelé racine primitive n-ième de l'unité lorsqu'il est d'ordre n dans le groupe $\mathbb{C}^*$. On note μ_n^* l'ensemble de ces éléments.
2. Remarque : $e^{\frac{2ik\pi}{n}} \in \mu_n^* \iff k \wedge n = 1$. Il existe donc $\varphi(n)$ racine primitive n-ièmes de l'unité, avec φ l'indicatrice d'Euler.
3. Définition (polynôme cyclotomique) : on note $\phi_n := \prod_{\omega \in \mu_n^*}(X - \omega)$ le n-ième polynôme cyclotomique à coefficients complexes.
4. Lemme : $X^n - 1 = \prod_{d|n} \phi_d$.
5. Corollaire : $\phi_n \in \mathbb{Z}[X]$.
6. Théorème : tous les polynômes cyclotomiques sont irréductibles dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.
7. Application : le corps cyclotomique $\mathbb{Q}(\mu_n)$ obtenu en adjoingnant à $\mathbb{Q}$ l'ensemble des racines n-ièmes de l'unité de $\mathbb{C}$ forme une extension de degré $\varphi(n)$.

II - Nombres premiers

1 - L'ensemble des nombres premiers [Rombaldi]

1. Théorème $\mathbb{Z}$ est un anneau euclidien, donc principal et factoriel. On appelle nombre premier ses éléments irréductibles positifs.
2. Exemples : 2 est l'unique nombre premier pair. $561 = 3 \times 11 \times 17$ n'est pas premier. 1 **n'est pas premier**.
3. Proposition : l'ensemble des nombres premiers est infini.
4. Proposition : les assertions suivantes sont équivalentes
    1. p est un nombre premier.

2. $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.
3. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre.
4. $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$
5. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps.
   Dans ce cas, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

5. Application : Par réduction modulo 7, le système diophantien à coefficients dans $\mathbb{Z}$ suivant n'a pas de solution entières :

$$\begin{cases} 3x - 10y = 78 \\ 4x - 11y = -5 \end{cases}$$

2 - Nombres de Carmichael [Damazure]

1. Définition (nombre de Carmichael) un entier composé n est dit de Carmichael s'il satisfait :

$$\forall a \in \mathbb{Z},\ a \wedge n = 1 \implies a^{n-1} \equiv 1[n]$$

2. Exemple : 561 est le plus petit nombre de Carmichael.
3. Proposition : soit n un entier composé. n est de Carmichael si, et seulement si, pour tout diviseur premier p de n, $\neg(p^2 \mid n)$ et $p - 1 \mid n - 1$. (DVT 2)
4. Théorème (Solovey-Strassen, DVT 2) : soit n un entier impair différent de 1. Alors n est premier si, et seulement si :

$$\forall a \in \mathbb{Z},\ a \wedge n = 1 \implies \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}[n]$$

5. Application (test de primalité probabiliste de Solovey-Strassen) :
   Entrée : n à tester, $k \geq 1$ un entier.
   Sortie : vrai ou faux.
   Répéter k fois :
   Choisir a au hasard dans $[[2, n-1]]$
   Si $a \wedge n \neq 1$, renvoyer faux
   Si $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}[n]$, renvoyer faux
   renvoyer vrai
   Si cet algorithme renvoie faux, n est composé. Sinon, la probabilité pour que n soit composé est inférieure ou égale à $1/2^k$.

6. Remarque : avec $k = 30$, la probabilité qu'un entier composé soit déclaré premier par l'algorithme de Solovey-Strassen est inférieure à un milliardième !

III - Anneaux d'entiers

1 - Introduction par un exemple : les entiers de Gauss [Perrin]

> Bien que plusieurs résultats présentés ici se déduisent de la théorie générale présentée ensuite, ils admettent une démonstration élémentaire qui justifie qu'on traite cet exemple à titre introductif.

1. Définition (entiers de Gauss)
2. Remarque : $\mathbb{Z}[i] \cong \mathbb{Z}[X]/\langle X^2 + 1\rangle$
3. Théorème : c'est un anneau euclidien dont le stathme est donné par la norme. Ses inversibles sont exactement ses éléments de norme 1, c'est-à-dire ± 1 et $\pm i$.
4. Proposition : Soit p un nombre premier. Les assertions suivantes sont équivalentes :
    1. p est somme de deux carrés d'entiers
    2. p est réductible dans $\mathbb{Z}[i]$.
    3. $p \equiv 1[4]$ ou $p = 2$.
5. Théorème : soit n un entier admettant la décomposition $\prod p^{\nu_p(n)}$. Alors n est somme de deux carrés si, et seulement si, pour tout facteur premier p de n, $\nu_p(n)$ est pair ou $p = 2$ ou $p \equiv 1[4]$

2 - Théorie générale [Diaz-Toca, Lombardi et Quitté]

1. Définition (entier d'un corps de nombres) : soit K un corps de nombres. Un élément $\alpha \in K$ est dit entier s'il existe un polynôme unitaire à coefficients entiers qui annule α. On note $\mathfrak{O}_K$ l'ensemble des éléments entiers de K.
2. Exemples :
    1. Les entiers de $\mathbb{Q}$ sont exactement les éléments de $\mathbb{Z}$.
    2. Les racines de l'unité sont toutes entières.
    3. Pour $q \in \mathbb{Q}_+ \setminus \mathbb{Z}$, $\sqrt{q}$ n'est pas entier.
3. Proposition : soit A un sous anneau factoriel de $\mathbb{C}$. Si $\alpha \in Frac(A)$ est un entier algébrique, alors $\alpha \in A$.

4. Exemple / Contre-exemple :
    1. Les entiers de Gauss sont bien les entiers de $\mathbb{Q}[i]$!
    2. L'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas l'anneau des entiers de $\mathbb{Q}(\sqrt{5})$, car le nombre d'or est entier et appartient à $\mathbb{Q}(\sqrt{5})$.
5. Proposition (caractérisation des entiers) : soit $\alpha \in K$. Les assertions suivantes sont équivalentes :
    1. $\alpha \in \mathfrak{O}_K$
    2. $\mathbb{Z}[\alpha]$ est un groupe abélien de type fini.
    3. $\pi_\alpha \in \mathbb{Z}[X]$ (DVT 1, partie 2/3)
6. Remarque : si $q \in \mathbb{Q}_+ \setminus \mathbb{Z}$, $\mathbb{Q}(\sqrt{q})$ est un $\mathbb{Q}$-espace vectoriel de dimension 2. Pourtant, $\mathbb{Z}[\sqrt{q}]$ est un $\mathbb{Z}$-module qui n'est pas de type fini.
7. Théorème : $\mathfrak{O}_K$ est un sous-anneau de K.
8. Théorème : Un élément $\alpha \in \mathfrak{O}_K$ est inversible dans $\mathfrak{O}_K$ si, et seulement si, sa norme est ± 1. (DVT 1, 3/3)
9. Exemple : soit α une racine complexe de $X^3 + 4X^2 - 8X + 2$. α n'est pas inversible dans l'anneau des entiers de $\mathbb{Q}(\alpha)$.