Licence de Mathématiques - L3

Université de Toulon

2017/2018

Présentation de l'option **Algèbre**

Yves Aubry

Septembre 2017

Vers l'an 280 après J.-C, le père de l'Algèbre, Diophante d'Alexandrie, disparaît...

Vers l'an 280 après J.-C, le père de l'Algèbre, Diophante d'Alexandrie, disparaît...

La légende raconte que sur sa tombe, on pouvait lire un problème, dû à Métrodore, permettant de calculer son âge à son décès.

Voici une version de cette épitaphe en alexandrins :

Passant, sous ce tombeau repose Diophante.
Ces quelques vers tracés par une main savante
Vont te faire connaître à quel âge il est mort.
Des jours assez nombreux que lui compta le sort
Le sixième marqua le temps de son enfance ;
Le douzième fut pris par son adolescence.
Des sept parts de sa vie, une encore s'écoula,
Puis s'étant marié, sa femme lui donna
Cinq ans après un fils qui, du destin sévère
Reçut de jours hélas ! deux fois moins que son père.
De quatre ans, dans les pleurs, celui-ci survécut.
Dis, si tu sais compter, à quel âge il mourut.

En 1621 est publiée la traduction du Grec au Latin des Arithmetica, principal ouvrage de Diophante.

En 1621 est publiée la traduction du Grec au Latin des Arithmetica, principal ouvrage de Diophante.

Arithmeticorum Lib. II. 85

teruallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 – 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quot continet latus ipsius 16. esto à 2 N. – 4. ipse igitur quadratus erit 4 Q. + 16. – 16 N. hæc æquabuntur vnitatibus 16 – 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$. & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16. diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. – 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. – 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. – 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit ergo primi latus $\frac{16}{5}$.

Autour de 1660 quelque part en France...

Autour de 1660 quelque part en France...

Autour de 1660 quelque part en France...

"J'ai trouvé une merveilleuse démonstration de cette proposition. Mais la marge est trop étroite pour la contenir."

Autour de 1660 quelque part en France...

"J'ai trouvé une merveilleuse démonstration de cette proposition. Mais la marge est trop étroite pour la contenir." Pierre de Fermat

Conjecture de Fermat

Pour $n \geq 3$ et $x, y, z \in \mathbb{Z}$:

$$x^n + y^n = z^n \implies xyz = 0$$

Conjecture de Fermat

Pour $n \geq 3$ et $x, y, z \in \mathbb{Z}$:

$$x^n + y^n = z^n \implies xyz = 0$$

Exo : Il suffit de le montrer pour les exposants premiers impairs ℓ.

Conjecture de Fermat

Pour $n \geq 3$ et $x, y, z \in \mathbb{Z}$:

$$x^n + y^n = z^n \implies xyz = 0$$

Exo : Il suffit de le montrer pour les exposants premiers impairs ℓ.

Théorème

Soit ζ une racine primitive ℓ-ième de l'unité dans $\mathbb{C}$. Si l'anneau $\mathbb{Z}[\zeta]$ est principal, l'équation n'a pas de solutions entières non triviales.

C'est quoi ?

Mais d'où vient cet anneau $\mathbb{Z}[\zeta]$?

Corps de nombres, Anneau des entiers, Groupes de Galois

Soit K un **corps** de nombres, i.e. une extension algébrique de degré fini de $\mathbb{Q}$.

Les éléments de K entiers sur $\mathbb{Z}$ forment un **anneau** $\mathcal{O}_K$ appelé l'anneau des entiers de K.

Proposition

$\mathbb{Z}[\zeta]$ *est l'anneau des entiers du corps cyclotomique* $\mathbb{Q}(\zeta)$.
L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ *est galoisienne, de degré* $\varphi(n)$ *où* φ *est la fonction indicatrice d'Euler, de* **groupe** *de Galois isomorphe à* $(\mathbb{Z}/\ell\mathbb{Z})^*$.

Les trois chapitres du cours

On étudiera :

I. La théorie des **groupes**

II. La théorie des **anneaux**

III. La théorie des **corps**.

Durée des chapitres

Le chapitre

I. La théorie des **groupes**
durera la moitié du semestre.

Durée des chapitres

Le chapitre

I. La théorie des **groupes**
durera la moitié du semestre.

Les chapitres

II. La théorie des **anneaux**

et

III. La théorie des **corps**.

s'étaleront sur la 2ème moitié du semestre.

Théorie des Groupes

On passera en revue les notions de :

- Groupes cycliques

- Groupes abéliens

- Groupes simples

- Groupes quotients, sous-groupes distingués, sous-groupes de Sylow, actions de groupes sur un ensemble...

- Groupe symétrique, groupe diédral, groupe quaternonien...

- Groupes résolubles

Théorie des groupes : le sommaire (7 chapitres)

1. Structures

- Groupes, anneaux et corps
- Morphismes
- Générateurs et relations d'équivalences

2. Exemple des entiers modulo n

- Le groupe $\mathbb{Z}$, ses sous-groupes et ses quotients
- Morphismes de groupes de $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$ dans un groupe
- Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

3. Quotients et produits de groupes

- Sous-groupes distingués
- Produits directs et indirects

Théorie des groupes (suite)

4. Groupes agissant sur un ensemble
- Action d'un groupe sur un ensemble
- Formule des classes

5. Le groupe symétrique

6. Théorie de Sylow

7. Groupes abéliens finis
- Groupes abéliens finis
- Partie sans torsion, partie de torsion
- Le théorème de structure des groupes abéliens de type fini

Théorie des Anneaux

On passera en revue les notions de :

- Anneau factoriel

- Anneau Noethérien

- Anneau principal

- Anneau euclidien

- Anneau intégralement clos

Théorie des corps

On passera en revue les notions de :

- Caractéristique d'un corps, corps de décomposition

- Extension de corps, algébrique, transcendante, galoisienne...

Théorie des corps : le sommaire

1. Les techniques vectorielles

- Degré d'une extension, éléments algébriques

- Corps de rupture, corps de décomposition

2. Les corps finis

- Caractéristique, cardinal, Frobenius

- Existence et unicité des corps finis

- Le groupe multiplicatif $\mathbf{F}_q^*$

- Construction de $\mathbf{F}_4$

- Inclusions de corps finis

Théorie des corps : le sommaire (suite)

3. La théorie de Galois

- Extension normale

- Groupe de Galois

- Corps des invariants

- La correspondance de Galois

Cours conseillé pour qui ?

Cours conseillé pour qui ?

Ce cours est vivement conseillé à tout étudiant souhaitant s'orienter vers les métiers de l'enseignement de Mathématiques (**CAPES** et **Agrégation**).

Il est aussi conseillé à tout étudiant souhaitant s'orienter vers la **Recherche** en Mathématiques.

Partiel

Un partiel se tiendra à la moitié du semestre
(Note de Contrôle Continu).

T.D. : Polycopié d'exercices

Un polycopié d'exercices est disponible sur ma page web (taper "Yves Aubry" sur Google).

Fin

Algébriquement vôtre