École de recherche CIMPA à Oujda en 2015
Théorie des nombres et ses applications

Résumés des cours

Quelques Applications de la théorie algébrique des nombres

Abdelmalek AZIZI (Université Mohammed Premier, Oujda, Maroc)

La théorie des nombres a plusieurs applications en sciences et en industrie. En particulier, elle a plusieurs applications en cryptographie : la méthode de chiffrement RSA se base sur la théorie élémentaire des nombres et la méthode d'échange de clés (Diffie-Helmann) définie à l'aide du logarithme discret sur un groupe cyclique est appliquée sur des groupes de classes de certains corps de nombres et elle trouve son efficacité, jusqu'à présent, lorsqu'on l'applique sur des groupes elliptiques. Dans cette conférence, on va s'intéresser à la méthode d'échange de clés appliquée à un groupe de classes d'un corps de nombres. Plus particulièrement, on traitera le cas d'un corps quadratique imaginaire et le cas d'un corps quadratique réel.

Introduction aux fonctions L

Abdelmejid BAYAD (Université d'Evry Val d'Essonne, Evry, France)

Dans ce cours, nous étudions les **propriétés analytiques et arithmétiques** des fonctions zêtas et fonctions L suivantes

1. Zêta de Riemann
2. Séries et fonctions L de Dirichlet
3. Fonctions zêta de Dedekind.

En particulier, nous verrons le théorème de Klingen-Siegel sur la rationalité des valeurs des zêtas de Dedekind associées aux corps de nombres totalement réels, prises aux entiers négatifs. Dans ce cours, quelques conjectures et questions ouvertes liées aux valeurs spéciales de ses fonctions L, seront précisées. Dans ce qui suit une liste non exhaustive pour une introduction aux fonctions zêtas et séries L de Dirichlet.

Bibliographie :
H.M. Edwards, Harold M. (2001), *Riemann's Zeta Function,* (2001) Dover.
N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions,* (1984) 2nd edition, Graduate, Springer Verlag 1984.
J.P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7. Springer-Verlag, 1973.
E.C. Titchmarsh, *The theory of the Riemann zeta-function,* Oxford University. Press, 1951.

Elliptic Curves and Their Application in Cryptography

Gerhard FREY (University of Duisburg-Essen, Allemagne)

References :
Everything needed about Elliptic Curves can be found in
J. Silverman : The Arithmetic of Elliptic Curves, GTM 106, Springer 1986.
Everything used in the lecture about Public Key Cryptography and Elliptic Curves including the theory of finite fields both from the theoretical and algorithmic point of view can be found in
H. Cohen and G. Frey (eds.) : Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC 2005.
In this book one finds an exhausting list of references (40 pp).

1. Public Key Cryptography. In the first section we shall explain the basic principles of public key cryptography and explain protocols for key exchange and signatures using discrete logarithms (DL). We explain hardness of DL by complexity functions. We introduce finite fields and take first example for DL-groups the multi- plicative group of such fields. We shall motivate why its complexity is only subexponential.

2. Cubics. We look at plane projective cubics and explain geometrically the addition law. We define elliptic curves as nonsingular cubics E and take the group of rational points of such curves over finite fields as candidates for DL-groups. We introduce basic notions like endomorphisms and isogenies of elliptic curves and discuss as example the Frobenius endomorphism for E defined over finite fields Fq.

3. Elliptic Curves over Complex and Finite Fields. We discuss elliptic curves over complex numbers, their torsion points and explain basic properties of curves with complex multiplication. We use these results for elliptic curves over finite fields and prove, by Deur- ing's lifting theorem, properties of the characteristic polynomial of the Frobe- nius endomorphism and in particular, get the so-called Riemann Hypothesis for elliptic curves.

4. Counting Algorithms. To use elliptic curves for DL-groups it is crucial to be able rapidly the number of points on such curves over finite fields. We explain different methods for this including the method with complex multiplication.

5. Security. We discuss strong points for the security of DL-systems based on elliptic curves but stress that there are possible attacks for special curves,in particular attacks by the Tate-pairing that excludes supersingular elliptic curves. In addition there are attacks if elliptic curves over non-prime fields are taken.

6. Pairing-based Cryptography. If there is time I shall explain how pairings can be used not only as means for attacks but in a constructive way, too.

Circular units

Radan KUCERA (Masaryk University, République tchèque)

For an integer $m > 2$, by the mth cyclotomic field we have in mind the field $\mathbf{Q}(\zeta_\mathbf{m})$, where ζ_m is a primitive mth root of unity. The group of circular numbers of $\mathbf{Q}(\zeta_\mathbf{m})$ is the subgroup D_m of the multiplicative group $\mathbf{Q}(\zeta_\mathbf{m})^\times$ generated by the numbers $1-\zeta_m^a$, where $a = 1, 2, \ldots, m-1$. The group of circular units of $\mathbf{Q}(\zeta_\mathbf{m})$ is the intersection $C_m = D_m \cap E_m$, where E_m means the group of all units of the ring of integers of $\mathbf{Q}(\zeta_\mathbf{m})$. The importance of C_m consists in the fact that it is defined by finitely many explicit generators. Circular units were known already to Kummer who, for a special case of m being a prime-power, proved (in contemporary terms speaking) that the index $[E_m : C_m]$ is equal to the class number of $\mathbf{R} \cap \mathbf{Q}(\zeta_\mathbf{m}) = \mathbf{Q}(\cos \frac{\mathbf{2\pi}}{\mathbf{m}})$.

The notion of the group of circular units has been generalized to any abelian field (i.e., a subfield of a cyclotomic field) in different ways (Hasse, Leopoldt, Sinnott, Washington, ...) giving several different groups. The aim of this minicourse is to present circular units and their properties including a few modern applications : for a suitable abelian field one can use a group of circular units to get a divisibility result for the class number or an annihilator of the class group.

La théorie ℓ-adique des corps de classes et quelques applications

Jean-François JAULENT (Université de Bordeaux, France)

Le cours vise à introduire la théorie ℓ-adique du corps de classes et à en développer quelques applications :
- classes logarithmiques des corps de nombres ; valeurs absolues ℓ-adiques et conjecture de Gross. ;
- rationalité et birationalité : descente et propagation ; exemples ;
- approche logarithmique des noyaux sauvages de la K-théorie.

Bibliographie :

G. Gras : Class field theory : from theory to practice, Graduate Texts in Math. Springer-Verlag, 2003.

Introduction aux formes quadratiques binaires et aux groupes de classes des corps quadratiques
Claude LEVESQUE (Université Laval, Canada)

Ce mini-cours se veut une introduction aux formes quadratiques binaires.
En particulier, les formes quadratiques binaires sont utilisées pour déterminer le nombre de classes des corps quadratiques. Le cours est basé sur le volume "Introduction to number theory" de Daniel Flath.

- Formes quadratiques binaires : définies positives, définies négatives, indéfinies ;
- Equivalence de formes quadratiques et classes d'équivalence ;
- Formes quadratiques réduites ;
- Structure de groupe sur ces classes : composition des formes ;
- Liste des formes quadratiques indéfinies réduites via les fractions continues (méthode de Gauss) ;
- Lien avec le groupe de classes des corps quadratiques (imaginaires et réels).

Computational number theory
Daniel C. MAYER (Graz, Autriche)

The four lectures on computational number theory begin with regulators and class groups of quadratic fields determined with continued fractions and quadratic forms using techniques of Shanks and Buchmann. The theory is then extended to general number fields and their Galois groups, unit groups and class groups. Finally, primality tests and factoring methods are presented, based on elliptic curves and number fields.

La théorie d'Iwasawa des $\mathbf{Z_p}$-extensions d'un corps de nombres
A. MOVAHHEDI (Université de Limoges, France)

Ce cours introductif s'adresse aux jeunes chercheurs doctorants ou post-doctorants intéressés par la théorie algébrique des nombres. Les chercheurs marocains travaillent beaucoup sur les groupes des classes d'idéaux des corps de nombres et ce cours sera l'occasion de donner l'un des célèbres théorèmes d'Iwasawa concernant la croissance des p-parties des nombres des classes d'idéaux dans une $\mathbf{Z_p}$-extension où p est un nombre premier. Une $\mathbf{Z_p}$-extension d'un corps de nombres F est une extension infinie qui peut être concrétisée par la donnée d'une tour infinie $F \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots$ où pour tout entier naturel n, l'extension F_n/F est cyclique de degré p^n. L'idée de la preuve du théorème d'Iwasawa en question est de considérer la limite projective des p-groupes des classes d'idéaux le long de la tour en la regardant comme un module sur l'anneau des séries formelles $\mathbf{Z_p}[[\mathbf{T}]]$ en une indéterminée T.

L'introduction des $\mathbf{Z_p}$-extensions permet aussi de donner une interprétation algébrique naturelle de la conjecture de Leopoldt - a priori de nature transcendante - sur la non nullité du régulateur p-adique d'un corps de nombres. À travers ce cours, nous donnerons l'interprétation de cette conjecture par le nombre des $\mathbf{Z_p}$-extensions indépendantes du corps de nombres en question.

À la fin du cours nous exposerons (cette fois évidemment sans démonstration) le lien extraordinaire qui existe entre les groupes des classes d'idéaux et les fonctions L au moyen de la conjecture principale d'Iwasawa (théorème de Mazur-Wiles pour $\mathbf{Q}$, Wiles pour un corps totalement réel).

Nous suivrons essentiellement le livre "Topics in Iwasawa Theory" qui est en train d'être rédigé par Ralph Greenberg. Il est téléchargeable sur sa page personnelle :
http ://www.math.washington.edu/ greenber/book.pdf

La conjecture de Bloch-Kato pour les fonctions L de Dedekind
Thong NGUYEN QUANG DO (Université Franche-Comté, France),
Ramdorai SUJATHA (University of British Columbia, Canada)

L'un des thèmes les plus fascinants de la théorie des nombres concerne les propriétés arithmétiques attachées aux valeurs spéciales des fonctions L des motifs. Quelques exemples archétypiques : les congruences de Kummer, la formule analytique du nombre de classes, la conjecture de Birch & Swinnerton-Dyer... , tous englobés maintenant dans la conjecture de Bloch-Kato, également appelée « conjecture des nombres de Tamagawa » (et ses versions équivariantes). La théorie d'Iwasawa fournit à l'heure actuelle la seule méthode générale permettant d'attaquer ce problème. Dans le prolongement des cours de A. Bayad sur les fonctions L complexes et de A. Movahhedi sur la théorie des $\mathbf{Z_p}$-extensions, on se propose d'étudier le cas des motifs de Tate : les fonctions L associées sont les fonctions L de Dedekind, dont la conjecture de Bloch-Kato donne pour les valeurs spéciales aux entiers rationnels une expression remarquable, généralisant la formule analytique du nombre de classes. Une démonstration complète (du moins dans son principe) sera donnée pour le corps des rationnels $\mathbf{Q}$, et plus généralement pour un corps abélien totalement réel.

Les équations diophantiennes et leurs applications
Michel WALDSCHMIDT (Université Pierre et Marie Curie-Paris 6, France)

De nombreuses questions mathématiques se ramènent à résoudre des équations diophantiennes. L'arithmétique des corps de nombres est un des principaux exemples. Les équations dites de Fermat–Pell (considérées antérieurement par Ramanujan) interviennent aussi dans l'étude topologique des variétés riemanniennes et dans des questions de combinatoire symbolique avec les mots de Christoffel. Le problème du nombre de classes de Gauss fait intervenir des équations diophantiennes. Plusieurs questions de logique se ramènent également à des équations diophantiennes.

Plusieurs méthodes permettent de résoudre des équations diophantiennes. Historiquement, les plus anciennes (remontant principalement à Pierre de Fermat) utilisent des arguments d'arithmétique spécifiques à l'exemple traité. Il a fallu attendre les travaux de Lagrange au XVIIIème siècle pour savoir résoudre complètement les équations quadratiques en deux variables. Ce n'est qu'à la fin du XIXème siècle, et surtout au XXème siècle, que des méthodes un peu générales ont été développées. La solution négative du 10ème problème de Hilbert conduit à restreindre l'étude à des équations en un petit nombre de variables - nous nous concentrerons sur le cas de deux variables qui prennent des valeurs entières (points entiers sur des courbes). De nos jours, les méthodes de géométrie arithmétique sont les plus puissantes, elles permettent dans de nombreux cas de décider si une équation diophantienne en deux variables a une infinité de solutions. Les méthodes d'approximation diophantienne fournissent les outils les mieux adaptés, le théorème du sous–espace de Schmidt est un résultat fondamental dont le domaine d'applications n'a pas fini d'être exploré. Mais cela ne suffit pas quand on veut donner la liste des solutions d'équations spécifiques : les méthodes effectives issues de la théorie des nombres transcendants sont les mieux adaptés pour parvenir à ce but.

Le résultat central de ce cours sera le théorème du sous–espace de Wolgang Schmidt. Nous en donnerons un premier énoncé simplifié, qui a déjà beaucoup d'applications profondes. Pour comprendre l'énoncé le plus général, il faut disposer de certaines bases qui seront enseignées dans ce cours. Des applications de ce théorème seront ensuite données, un choix sera fait parmi les nombreuses conséquences, nous privilégierons celles qui ne demandent pas de langage trop sophistiqué.

La démonstration du théorème du sous-espace ne sera pas donnée : quelques indications seront fournies sur la preuve, mais les détails demanderaient trop de développement techniques. Cet énoncé peut être utilisé et appliqué à de multiples questions sans qu'il soit utile de savoir comment on le démontre.

Le cours se poursuivra par une introduction aux méthodes effectives utilisant des outils de la théorie des nombres transcendants, dont l'origine se trouve dans les travaux de Gel'fond et Baker au XXème siècle.