SEMINAR :Second meeting in Geometry and Algebra

Université Cheick AntaDiop (UCAD)

Faculté des Sciences et Technique (FST)

Laboratoire d'Algèbre, de Cryptologie, de Géométrie Algébrique et Applications(LACGAA)

Place: Salle master FST

Date : September 1st 2012

Time: 9h-19h

Title and Abstract of Talks

1) **The merit factor of linear recurrent sequences**
ChérifBachir Deme:
Abstract: The aim of this presentation is to show how to calculate the merit factor of linear recurrent sequences.
First we give some definitions and properties of linear recurrent sequences, and finally we calculate the merit factor of these sequences.

2) **Title: A New Characterization of Commutative Strongly Π-Regular Rings**
Anta NianeGueyeToure
Abstract:
Let R be a commutative ring. It is known that any injective endomorphism of finitely generated R-module is an isomorphism if and only if every prime ideal of R is maximal. This result makes possible a characterization of rings on which all finitely generated modules are co-hopfian. The motivation of this paper comes from trying to extend these results to mono-correct modules. In doing so, we show that any finitely generated R-module is mono-correct if and only if every prime ideal of R is maximal and we obtain a characterization of commutative rings on which all finitely generated module are mono-correct. Such rings are exactly commutative strongly PI-regular rings. So we have a new characterization of commutative strongly PI-regular rings.

3) **On I-modules and S_{1}-modules**
Mankagna Albert Diompy
Abstract: Let R be a non necessarely commutative ring and M an unital left R-module.We use the category $\sigma[M]$ the full subcategory of $R-Mod$ whose objects are all M-subgenerated modules. We say that M satisfies property $(I) (resp.(S))$ if every injective $(resp. surjective)$ R-endomorphism of M is an automorphism.\\
It is well know that every artinian $(resp. finite \ length)$ module satisfies the property (I) $(resp. (S)$ but the converse is not true. For example: the $\mathbb{Z}$-module $\mathbb{Q}$ of rational numbers has the properties (I) and (S) but $\mathbb{Q}$ is neither artinian nor noetherian so not finite length.\\
The aim of this presentation is to characterize for a fixed ring the R-modules M for which every object of $\sigma[M]$ satisfying the property $(I) (resp. (S))$ are artinian $(resp. finite \ length)$. Such modules are called I-modules $(resp. S_{1}-modules)$.\\
First we give a characterization of S_{1}-abelians groups for after to give characterization of S_{1}-modules semisimple and serials with $\sigma[M]$ admits a progenerator.\\
Secondly after giving some properties of I-modules we charactirize I-modules faithfully balanced and serials
Key words: Duo-ring; $\sigma[M]$; artinian; finite \ length; I-module; S_{1}-module.

4) **Classification of the absolute valued algebras (AVA) with left unit**

satisfying (x2, x2, x2) = 0.
AllassaneDiouf

Abstract. We show that every absolute valued algebra with left unit satisfying (x2, x2, x2) = 0 is finite dimensional of degree ≤ 4. Next, we determine such an algebras. In addition to the already known algebras IR, C, *C, IH, *IH, *IH(i, 1), O, *O, *O(i, 1) the list is completed by two new algebras not yet specified in the literature.

5) **Caractérisation des anneaux pour lesquels tout module endo noethérien est noethérien.**
Mohameth Alassane Ndiaye

Abstract: La théorie des modules est une généralisation du concept d'espaces vectoriels. En effet, au sein des structures algébriques, un module est pour un anneau ce qu'un espace vectoriel est pour un corps. Or, nous avons une classe intéressante de modules appelée modules n\oe thériens dont les prémices reposent essentiellement sur la condition de chaîne ascendante qui est une propriété mathématique sur les ordres, identifiée initialement par Emmy Noether en 1921 dans le contexte de l'algèbre commutative. La condition de finitude relative aux chaînes descendantes d'idéaux a été introduite par Artin. Les anneaux fortement co-Hopfiens ont été introduits par Kaplansky \cite{hmai49}, Azumaya les appelle anneaux fortement π-réguliers. Mon mémoire de master 2 était consacré à l'étude des modules endo noethériens respectivement endo artiniens initiés par A. Kaidi dans son exposé du 15 octobre 2009 sur les "Modules avec conditions de chaîne sur les Endoimages et les Endonoyaux". On dit qu'un A-module M est endo n\oe thérien, s'il vérifie la condition de chaîne ascendante, pour les sous modules de la forme $Ker f$ où f est un endomorphisme de M. Autrement dit toute chaîne de la forme:$$Ker f_1 \subset Ker f_2 \subset \cdots \subset Ker f_n \subset \cdots \ \textit{avec} \ f_i \in End(M)$$ est stationnaire. Nous pouvons rappeler que la classe des modules endo n\oe thériens englobe toutes les propriétés initialement connues des modules n\oe thériens. En effet tout module n\oe thérien est endo n\oe thérien, mais la réciproque est fausse. Dès lors nous voudrons caractériser les anneaux pour lesquels, tout module endo n\oe thérien est n\oe thérien. De tels anneaux seront nommés dans notre étude $EKFN$-anneau. Dans un premier temps, nous avons remarqué que dans un anneau semi simple A, tout A-module endo n\oe thérien est n\oe thérien, d'où l'idée de caractériser les $EKFN$-anneaux n'est pas vide. De plus nous avons même montré que tout anneau artinien à idéaux principaux est un $EKFN$-anneau.

6) **Pairing on Huff curves:**
Abdoul Aziz Ciss

Abstract: Recently two kinds of Huff curves were introduced as elliptic curves models and their arithmetic was studied. It was also shown that they are suitable for cryptographic use such as Montgomery curves or Koblitz curves (in Weierstrass form) and Edwards's curves.
In this work, we introduce the new generalized Huff curves $ax(y^{2} -c) = by(x^{2}-d)$ with $abcd(a^{2}c-b^{2}d)\neq 0$, which contains the generalized Huff's model $ax(y^{2}- d) = by(x^{2}-d)$ with $abd(a^{2}-b^{2})\neq 0$ of Joye-Tibouchi-Vergnaud and the generalized Huff curves $x(ay^{2} -1) =y(bx^{2}-1)$ with $ab(a-b)\neq 0$ of Wu-Feng as a special case.
The addition law in projective coordinates is as fast as in the previous particular cases. More generally all good properties of the previous particular Huff curves, including completeness and independence of two of the four curve parameters, extend to the new generalized Huff curves. We verified that the method of Joye-Tibouchi-Vergnaud for computing of pairings can be generalized over the new curve.
Keywords: Huff curves, pairing, Divisor, jacobian, Miller algorithm, elliptic curve models, Edwards curves, Koblitz Curves,}

7) **On a new binary elliptic curve**
Ahmed Khalifa

Abstract: Since their introduction in cryptography by Koblitz, Miller and MenezesMenezes, elliptic curves have been extensively used because they allows to use a more small key size and discrete logarithm is much more difficult in elliptic curve that in $(\mathbb{Z}/p\mathbb{Z})^{*}$ where p is a prime. Furthermore, pairings on elliptic curve have received major interest, due to their using to design cryptography's tools such as cryptanalyse technics or protocols.
It is known that Elliptic curves can be represented in different forms. These different forms induce different arithmetic properties, to obtain faster scalar multiplications, various forms of elliptic curves have been extensively studied in the last two decades. In this work we propose a new binary elliptic curve.

8) -Scalar multiplication on elliptic curve by Fröbenius map.

Ahmed Youssef

Abstract
Koblitz has suggested to use “anomalous" elliptic curves defined over F2, which are non-supersingular and allow for efficient multiplication of points by an integer. For these curves, Meier and Staffelbach gave a method to find a polynomial of the Frobenius map corresponding to a given multiplier. Muller generalized their method to arbitrary non-supersingular elliptic curves defined over a small field of characteristic 2.
In this paper, we propose an algorithm to speed up scalar multiplication on an elliptic curve defined over a small field. The proposed algorithm uses the same technique as Muller's to get an expansion by the Frobenius map, but its expansion length is half of Muller's due to the reduction step Also, it uses a more efficient algorithm to perform multiplication using the Frobenius expansion.
Consequently, the proposed algorithm is 2 times faster than Muller's. Moreover, it can be applied to an elliptic curve defined over finite fields with odd characteristic and does not require any precomputation or additional memory.
Keywords: Scalar Multiplications, Frobenius Map, Frobenius Expansion, Elliptic Curves, Public Key Cryptography, addition-subtraction chain.

9) On $\mathfrak{R}$-SemisimplesSemimodules Over semirings

Landing Fall

Abstract: The notion of "simple module" in the theory of rings and modules is a fundamental tool and was generalized in different ways in the theory of semirings and semimodules. By our definition, a semimodule M over a semiring R, is a $\mathfrak{R}$-simple semimodule if any congruence relation defined over M is trivial or universal. This definition of "simple semimodule" is most the strong definition because they induces all the other known definitions. In this paper, we study and characterizes the subclass of $\mathfrak{R}$-simple and $\mathfrak{R}$-semisimplesemimodules in the class of subtractive and cancellativesemimodules.
Keywords: semirings, semimodules, subtractive subsemimodules, cancellativesemimodules, strongly independent semimodules, $\mathfrak{R}$-simple semimodules, $\mathfrak{R}$-semisimplesemimodules.

10) Computation of syzygies module over a field.

André Saint EudesMialébamaBouesso

Abstract: Syzygies module are some applications of Gröbner bases, in this work we will answer to **what is the syzygies module about?**
Let $A=K[x_1,…,x_n]$ be a polynomial ring over a field K and $I=< f_1,…,f_s>$ be a finitely generated ideal of A. Consider the following map $$H: A^s\longrightarrow I$$
$$(h_1,…,h_s)\longmapsto \displaystyle\sum_{i=1}^{s}h_if_i$$.
Our main goal in this talk is to give a practice method for determining a finite generator system of kerH
Keywords: Syzygies module, Commutative Gröbner bases, S-polynomial ,Buchberger algorithm, Termination theorem.

11) Gröbner bases Cryptosystem over Valuation ring and Dedekind ring

Jean Marie Preira

Abstract: Polly Cracker system is a public key cryptosystem in which the private key is a Gr\"obner basis. Many attacks show that this system based on Gr\"obner bases over a field are not secure.

The analysis of all known attacks shows that they use in some step, the solution of a linear system in the underlying field. Hence to avoid all known attacks on Polly Cracker, it will suffice to work into a ring for which linear systems are difficult to solve such that rings with enough non invertible and zeros-divisors elements provided that a concept of Gr\"obner basis exists.

In this work, we introduce two particular cases of Polly Cracker System. The first over principal valuation rings such as $\mathbb{Z}_{p^{\alpha}}$ and the second over a Dedekind ring with zeros divisors such as $Z(t)/\langle p^{\alpha}, t^{2}-t\rangle $ where p is prime and $\alpha\geq 2$ an integer.

Keywords: Public key cryptosystem, Polly Cracker, Linear algebra attack; Valuation rings, Noetherian rings, Dedekind rings, zero-divisors, Gr\"obner basis, Dynamical Gr\"obner basis, Buchberger's algorithm.

12) ATTACKS ON "Strong Diffie-Hellman-DSA KE" and Improvements

Demba Sow

Abstract: In this work, we propose a cryptanalyseof the so called "Strong Diffie-Hellman-DSA Key Exchange (briefly: SDH-DSA-KE)" and after we propose "Strong Diffie-Hellman-Exponential-Schnnor Key Exchange (briefly: SDH-XS-KE) » which is an improvement for efficiency and security. SDH-XS-KE protocol is secure against Session State Reveal attacks, Key independency attacks, Unknown-key share (UKS) attacks and Key-Compromise Impersonation (KCI) attacks. Furthermore, SDH-XS-KE has Perfect Forward Secrecy (PFS) property and is not vulnerable to Disclosure to ephemeral or long-term Diffie-Hellman exponents. We design our protocol in finite groups therefore this protocol can be implemented in elliptic curves.

13) Dtru1: First generalization of NTRU using dual integers

Mamadou G Camara

Abstract: NTRU is the first public key Cryptosystem based on the polynomial ring $\frac{\mathbb{Z}[X]}{\big(X^{N}-1\big)}$. The hard problem underlying this cryptosystem is related to finding short vectors in a lattice.

Several generalizations of NTRU was designed over various integral ring such as $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[w]$ and $\mathbb{H}$.

In this paper, we use the ring with zeros divisors $\mathbb{D}=\mathbb{Z}+\epsilon \mathbb{Z}, \ \epsilon^{2}=0$ (called the ring of Dual Integers) in order to design a new version of NTRU.

To achieve this objective, we have studied the elementary arithmetic properties of the ring of Dual integers in a previous paper.

The main difficulty is to be able to perform a division algorithm with a unique remainder and to invert polynomials with coefficients in quotient ring of the ring of Dual integers.

Nevertheless, we have successfully design NTRU over Dual integers (called DTRU) in a particular quotient ring of the ring of Dual integers. Our scheme has the same level security than NTRU, but is not more efficient. This work shows also that NTRU can be designed even if the ring has zeros divisors!

We have also design over the ring of Dual Integer the cryptosystem NTRU with Non-invertible polynomial proposed by Banks and Shparlinski. This version is more secure than NTRU but is less efficient too.

Keywords: Public key Cryptography, Dual integer, pseudo-norm, pseudo-division, Cryptosystem, NTRU.

14) Introduction to fuzzy algebras

Jean raoulTsiba

Abstract: The notion of fuzzy subset of a set is due to LotfiZadeh. His seminal paper in 1965 has opened up new insights and applications in a wide range of scientific fields.Azriel Rosenfeld used the notion of a fuzzy subset to set downcornerstone papers in several areas of mathematics, among other disciplines. Rosenfeld is the father of fuzzy abstract algebra.The aim of this talk is to introduce the theory of fuzzy algebras in our research group.

Keywords: fuzzy set, lattice, fuzzy group, fuzzy ring, fuzzy module, fuzzy homomorphism .

15) **Dénombrement des codes cycliques irréductibles**

Mohamed SALL

Abstract :

Dans ces travaux nous abordons les **codes cycliques irréductibles**, sous l'angle de leur nombre, relativement à leur poids et selon qu'ils soient projectifs ou pas. Le cas particulier des codes simplexes et non simplexes est aussi traité.

16) New Encryption Scheme based on Reed Muller code modified

El.HadjiModou MBOUP

Abstract:

It is devised a new cryptosystem based on modi_edReedMuller codes RM(r;m). The new cryptosystem is a modi_ed version of Sidel'nikov's one. This allows to increase the security of the public key, and to reconsider Reed Muller codes as good candidates for using in secure encryption scheme. An e_cient decoding with the Reed Muller decoding algorithm RM(r,m) and an increased level of security against attacks of the Sidel'nikov's cryptosystem due to Minder and Shokrolahi are the main advantages of the modi_ed version. Adding new columns implies longer codes, but this would not be a problem for decoding or deciphering because in decode one has only to deal with the words of the secret code belonging to the Reed Muller code RM(r,m). So the decoding phase would not su_er from this modi_cation.

Keywords: McEliece cryptosystem, Minder and Shokrolahi attack,
Reed Muller code.

17) **Les dérivations d'une algèbre réelles de division de dimension finie.**

André DIABANG

Abstract:

Nous allons donner toutes les possibilités de l'algèbre de Lie des dérivations d'une algèbre réelle de division de dimension finie (A.R.D.F) et de préciser un résultat partiel du groupe d'automorphisme des quaternions modifiés.

We will giveall possibilities toLie algebraof derivationsof an algebraofrealfinite dimensionaldivision(ARDF)andthen a resultofpartialautomorphism groupof quaternionsmodified.

18) Etude des objets Hopfiens , objets co-Hopfiens dans la catégorie Com.

OusseynouDiallo

Abstract ::

19) ……..

Amadou Tall