Algebraic Geometry, Number Theory and Applications in Cryptography and Robot kinematics

AIMS-Cameroon, Limbé

July 2 - 13, 2019

Organizing Committee

Christian Maire, University of Franche-Comté, France, christian.maire@univ-fcomte.fr
Aminatou Pecha, University of Maroua, Cameroon, aminap2001@yahoo.fr

Scientific Committee

Michel Coste, University Rennes 1, France
Marco Garuti, Universita Degli Studi Di Padova, Italy
Christian Maire, University of Franche-Comté, France
Marie-Françoise Roy, University Rennes 1, France

http://www.prema-a.org/cimpa-school-limbe/

The CIMPA-School "Algebraic Geometry, Number Theory and Applications in Cryptography and Robot kinematics" took place at AIMS-Cameroon, Limbé, from july 2 to july 13, 2019.
This mathematical meeting brought together

- 50 participants: 7 lecturers, one participant from CIMPA staff, 18 participants from Cameroon, 22 participants from other African regions (outside of Cameroon), a french and a USA participant.
- 20 nationalities namely participants coming from: Algeria, Burkina Faso, Cameroon, République du Congo, République Démocratique du Congo, Gabon, Ghana, Kenya, Madagascar, Mali, Niger, Nigeria, Rwanda, Senegal, Sudan, Tanzania, but also, France, Italy, Spain and USA.
- 11 females and 39 males.

The *Congress of African Women in Mathematics Association* (AWMA) is an associated Regional Workshop of this School for Central Africa; indeed African Women Mathematicians met at AIMS-Cameroon two days after, with the opportunity to attend the School.

Scientific content
This School has offered an intensive teaching session to graduate students and young researchers from Africa. The topics developed were in Algebraic Geometry and Number Theory. The following six courses have been selected:

- *Advanced topics in semi-algebraic geometry and modelization in robot kinematics*, by Michel Coste,
- *Counting points on algebraic varieties*, by Tony Ezome,
- *Basic algebraic number theory and class field theory*, by Elisa Lorenzo Garcia,
- *Fundamental groups in Algebraic and Arithmetic Geometry*, by Marco Garuti.
- *Tate module and Abelian varieties*, by Christian Maire,
- *Quantitative and algorithmic recent results in real algebraic geometry*, by Marie-Françoise Roy,

These fundamental courses describe all theoretical elements needed for the applications in cryptography and robot kinematics which have been developed at the end of the School. Beyond lectures, we have also planned:

- sessions devoted to solving exercises,
- sessions with computers with Sage, by Samuel Lelievre,
- a list of mini-projects has been proposed at the beginning of the School, in relation with some courses; at the end of the meeting, students have made short presentations of their work,
- lectures given by young researchers on their works.

Files of the exercices and mini-projects topics are attached at the end of the report.

Host institution and local context in mathematics
African Institute for Mathematical Science (AIMS, https://aims-cameroon.org) is an innovative, pan-African centre for Post Graduate education, research and outreach

which has achieved global recognition since opening in South Africa in 2003. AIMS-Cameroon is part of the network of AIMS centers and offers a one year Master's degree in mathematical science to African graduates every year since 2013. It is located in Limbé, in the South West Region of Cameroon. Professor Mama Foupouagnigni is the President of AIMS-Cameroon and Professor Marco Garuti, from Universita Degli Studi Di Padova in Italy, is the Academic Director.

On the other hand, Algebraic Geometry and Number Theory in sub-Saharan Africa got a fresh start in 2011, when some African young researchers went back in their native countries after their PhD defenses. Since then between 2011 and 2013 there have been PhD defenses from students working locally in Africa.
This is in this context that, on January 16th 2012, the *Pole of Research in Mathematics and their Applications in Information Security* (PRMAIS, HTTPS://WWW.PREMA-A.ORG/) was created. It is hosted in *Université des Sciences et Techniques de Masuku in Franceville (Gabon)*, and it is funded by Simons Foundation. PRMAIS consists of three components: PRMAIS-Senegal, PRMAIS-Cameroon, PRMAIS-Madagascar; and since 1st May 2018, a new network PREMA with researchers from Tunisia, Nigeria, Niger, Burkina Faso and Mali. PRMAIS aims to develop fundamental mathematical topics from Algebraic Geometry and Number Theory in African universities. Applications of these theoretical studies in cryptography, coding theory and robot kinematics are also developed. PREMA members have important collaborations with researchers all over the world.

Prior work related to the School

Since 2015, PRMAIS has organized or supported many mathematical meetings in Africa, at least two events every year. Let us just mention the events of the last two years.

- On 13 January 2017, *Les Journées Algébriques du Gabon*, in Ecole Normale Supérieure, Libreville (Gabon).
- From 10 to 23 May 2017 in Thiès (Senegal), an African Mathematical School in *Mathematics for Post-Quantum Cryptography and Signal Processing.*
- From 2 to 14 April 2018 in Franceville (Gabon), an African Mathematical School in the theme *Mathematics for asymmetric cryptography and robot kinematics.*
- From 18 to 22 February 2019, *Les Journées Algébriques du Gabon*, in Ecole Normale Supérieure, Libreville.

The stay

The participants from abroad arrived in Douala airport the week-end before the School. Some of them had to stay one night or two nights in Douala, in order to take some shuttle organized by AIMS-Cameroon (Limbé is at two-hours drive from Douala).

The School officialy started on tuesday 2nd of july with the presentation of AIMS-Cameroon by Marco Garuti, of PREMA by Tony Ezome and of CIMPA by Vlady Ravelomanana.

The lectures of the School have been given in the main classroom of AIMS-Cameroon since the dates chosen correspond to a vacation period in AIMS-Cameroon. The classroom was equipped with a video projector and large green board.

During the School, AIMS-Cameroon provided with its facilities to all participants (internet connection, financial staff, cleaning services, etc.), including accomodation for about 48 students and for the lecturers. Meals have been taken in the main building.
At the end of the School, participants have been the possibility to fill up a questionnaire concerning the School. The evaluaton show that the atmosphere, scientific content and activities proposed during the School (courses, exercises, mini-projects, lectures by young researchers) have been very appreciated. However the participants suggested that the totality of lecturers give documents on line for their courses. The lack of water in rooms during several days was reported and criticized.

Funding
The School has received financial support from

CIMPA	https://www.cimpa.info/
AIMS-Cameroon	https://aims-cameroon.org
PREMA	http://www.prema-a.org/
IRMAR Univ. Rennes 1	https://irmar.univ-rennes1.fr
IMU	https://www.mathunion.org/
OpenDreamKit Horizon 2020	https://opendreamkit.org/
ANR FLAIR Project	http://anrflair.math.cnrs.fr/
RNTA	http://www.rnta.eu/

Schedule

day	9-10:15am	10:45-12am	2-3:15pm	3:45-5	5:15-6
july 2			MFR	ELG	discussion
july 3	TE	ELG	MFR	exercices (MFR)	YR lectures
july 4	TE	CM	ELG	exercices (ELG)	YR lectures
july 5	MC	CM	MFR	exercices (ELG)	YR lectures
july 6	TE	CM			
july 7					
july 8	MFR	CM	SL	exercices (TE)	YR lectures
july 9	MC	MG	ELG	SL	YR lectures
july 10	TE	MG	SL	exercices	YR lectures
july 11	MC	MG	exercices (TE)	projects	projects
july 12	MC	MG			

MFR: Marie-Françoise Roy
Quantitative and algorithmic recent results in real algebraic geometry

MC: Michel Coste
Advanced topics in semi-algebraic geometry and modelization in Robot Kinematics

ELG: Elisa Lorenzo Garcia
Basic algebraic number theory and class field theory

SL: Samuel Lelievre
Introduction to SAGE

CM: Christian Maire
Tate Module and Abelian Varieties

TE: Tony Ezome
Point counting on algebraic varieties and applications in cryptography

MG: Marco Garuti
Fundamental groups in Algebraic and Arithmetic Geometry

YR: young researchers

Abstracts of courses

Michel Coste, University Rennes 1, France, michel.coste@univ-rennes1.fr

Advanced topics in semi-algebraic geometry and modelization in Robot Kinematics

The course will give a short introduction to Robot Kinematics and show examples of applications of algebraic and semialgebraic geometry in this field. I shall discuss direct and inverse kinematics and singularities, especially for parallel robots. I shall also discuss mechanisms having several operating modes, with possibly different degrees of freedom. I shall explain methods to translate problems of robot kinematics into systems of polynomial equations, including the model of the group of rigid motions given by the Study quadric, using dual quaternions. The effective methods of algebraic and semialgebraic geometry can then be applied (elimination, decomposition into primary components, cylindrical algebraic decomposition...). Problems to study with the help of computer algebra systems will be given to the students.

Tony Ezome, University of Masuku Franceville, Gabon, latonyo2000@yahoo.fr

Point counting on algebraic varieties and applications in cryptography.

Given an algebraic variety V over a finite field $\mathbb{F}_q$, we know that the $\mathbb{F}_{q^k}$-rational points on V form a finite set. What arises naturally in our mind is the construction of a process which computes the number of $\mathbb{F}_{q^k}$-rational points in V. This is one of the most important and very recurrent questions in cryptography, particularly when V is a (hyper-)elliptic curve C or a Jacobian variety J_C. That led to many points counting algorithms. This course aims to describe the more important methods. We will start with the naive algorithm (enumeration of points) which is a quite general method, and then we will describe the Baby Step Giant Step algorithm for elliptic curves. We will explain how are related the Frobenius endomorphism of a curve C, the number of rational points on C, the number of rational points on the Jacobian J_C, and Weil conjectures. We will also describe the Schoof ℓ-adic algorithm and the main steps in SEA algorithm. We will end by giving a technique for selecting a hyperelliptic curve C (and the underlying finite field) suitable for implementing a discrete logarithm cryptosystem in the Jacobian variety J_C.

Elisa Lorenzo Garcia, University Rennes 1, France, elisa.lorenzogarcia@univ-rennes1.fr

Basic algebraic number theory and class field theory

We will start by studying the structure of the decomposition of prime ideals in number fields and by discussing the definitions of norm, trace and discriminant. From there we will move to the basics of Class Field Theory: we will define the Artin symbol and we will state the Reciprocity Law. We will end by showing the applications of the Class Field Theory to the Theory of the Complex Multiplication. All the course will be illustrated with several examples which will help to the understanding of these deep theories.

Marco Garuti, Universita Degli Studi Di Padova, Italy, and AIMS-Cameroon, marco@aims-cameroon.org

Fundamental groups in Algebraic and Arithmetic Geometry

The course is a survey on the theory of Fundamental Groups in Algebraic and Arithmetic Geometry. Starting from Grothendieck's theory developed in SGA 1, we will review his Anabelian philosophy and its applications to the search for points on varieties.

Christian Maire, University of Franche-Comté, France, christian.maire@univ-fcomte.fr

Tate modules and abelian varieties

In this course, we will introduce the key concepts (and some basic tools) of Galois representations of Tate modules of Abelian varieties (elliptic curves and more generally Jacobian varieties). We will first spend time on elliptic curves to introduce in detail some notions in order to well understand their Tate module: locus of ramification, Frobenius and characteristic polynomial, mod p representation, L-function, image of the representation, modularity, etc. After that, we will explain how these properties extend to the case of genus > 1.

Marie-Françoise Roy, University Rennes 1, France, marie-francoise.roy@univ-rennes1.fr

Quantitative and algorithmic recent results in real algebraic geometry

Important theoretical results in real algebraic geometry such as the algebraic proofs of the fundamental theorem of algebra (valid for a real closed field), the curve selection lemma, the finiteness theorem (i.e a closed semi-algebraic set has closed description) have been recently studied from a quantitative and algorithmic point of view. Several methods are used: the cylindrical decomposition and the critical point method. In both cases, algebraic results about sub-resultants play a role. Important theoretical results in real algebraic geometry have been recently studied from a quantitative and algorithmic point of view. Several methods are used: the cylindrical decomposition and the critical point method. In both cases, algebraic results about sub-resultants play a role. The course treated the following topics

- *real root counting,*
- *quantifier elimination,*
- *semi-algebraic sets and cylindrical decomposition,*
- *connected components and critical point method.*

Lectures given by young researchers

ADEYEMO Hammed Praise, University of Ibadan, Nigeria

Stanley Symmetric Functions of Springer Permutations.

Abstract. In this talk, I will give a construction of Stanley symmetric functions indexed by Springer permutations and establish their connection with that of Grassmannian permutations. This will be done in type A.

BA Boumanga Abdoulaye, University of Thiès, Senegal

Cryptographie et sécurité de l'information sur le Web

Abstract. Dans cet exposé nous allons d'abord pouvoir appréhender le fonctionnement de l'infrastructure Web et ensuite comprendre comment la cryptographie est mise en oeuvre sur le Web pour assurer la sécurité de l'information, tout en précisant leurs enjeux majeurs pour un gouvernement ou une organisation.

BANG Narcisse, University of Daschang, Cameroon

Efficient computation of the Miller Loop and the Final exponentiation in Pairing-Based Cryptography

Abstract. In this talk, we show how one can efficiently computes pairings which are very useful in Cryptography.

DJINTELBE Nestor, University Assane SECK, Ziguinchor, Senegal

Compactifications of the space of rigid motions.

Abstract. We present different compactifications of the space of rigid motions and their applications in some problems of robot kinematics.

FOTUE-TABUE Alexandre,

MacWilliams' identity

Abstract. In this talk, we revisit the MacWilliams' identity, which is a relation between the weight enumerator of a linear code and the weight enumerator of its dual code.

FOUAZOU LONTOUO Perez, University of Dschang, Cameroon

Analogues Vélu's formulas for Hessian curve

Abstract. We give an analog of the Vélu's formulas for the Hessian model of an elliptic curve.

KOUMLA KANG-RANG Keth, Abdou Moumouni University of Niamey, Niger.

Généralisation de la théorie des bases de Gröbner dynamiques aux polynômes de Laurent à coefficients sur des anneaux de Dedekind

Abstract. Si R *est un anneau de Dedekind et* $f_i \in \mathrm{R}[X_n^{\pm}]$*, nous déterminons de manière dynamique une base de Gröbner pour* $I = \langle f_i \rangle_{i=1,\cdots,s} \in \mathrm{R}[X_n^{\pm}]$ *et ses syzygies modules.*

MOUSSA Seydou, University Dan Dicko Dankoulodo de Maradi, Niger

Rationalité de l'ensemble des configurations singulières d'une plate-forme de Gough-Stewart

Abstract. Dans cet exposé, nous montrons que l'ensemble des configurations singulières d'une plate-forme de Gough-Stewart admet une paramétrisation rationnelle.

NZAGANYA Nzaganya Edilson, University of Dar es salaam, Tanzania

Topology of a Projective hypersurfaces

Abstract. We compute the Euler characteristics of projective hypersurfaces by using the Griffiths residues and by using Chern classes.

NDONG'A OWINO Julia, Jaramogi University of Science and technology, Bondo, Kenya

Completeness of compact operators whose norms are eigenvalues

PONCHO-KOTEY Ephraim Nii Amon, AIMS Rwanda, Kigali, Rwanda

Counting of Rational Points On an Elliptic Curve

SALISSOU DANGO Mamane Djamilou, University Abdou Moumouni, Niamey, Niger

Factorisation des matrices 2×2 de déterminant égal a 1.

Abstract. Il s'agit, étant donnée une matrice 2×2*, de déterminant* 1*, de pouvoir l'écrire sous la forme d'un produit de matrices élémentaires. Nous regarderons le cas des matrices constantes, polynômiales multivariées et à coefficients dans un anneau de polynômes de Laurent.*

YOUEGO Jocelyne, University of Ngaoundere, Cameroon

Isogeny of supersingular elliptic curves in cryptography.

Abstract. In this talk, we present isogeny of elliptic curves and how they can be used to construct cryptographic primitives.

Participants

ADEYEMO Hammed Praise, University of Ibadan, Nigeria
AMANI FARAJA Deborah, AIMS-Cameroon
ANDRIAMANDRATOMANANA Njaka Harilala, University of Padova, Italy
AZEBAZE GUIMAGANG Laurian, University Yaoundé 1, Cameroon
BA Boumanga Abdoulaye, University of Thiès, Senegal
BANG MBIANG Narcisse, University of Dschang, Cameroon
COSTE Michel, University Rennes 1, France
DJINTELBE Nestor, University Assane SECK, Ziguinchor, Senegal
EZOME Tony, University of Masuku, Franceville, Gabon
FOBASSO TCHINDA Arnaud Girès, University of Yaounde 1, Cameroon
FOMBOH Mary, University of Buea, Cameroon
FOTUE TABUE Alexandre, University Yaoundé 1, Cameroun
FOUAZOU LONTOUO Perez, University of Dschang, Cameroon
FOUOTSA Emmanuel, University of Bamenda, Cameroon
FOUOTSA TAKO Boris, University of Roma 3, Italy
GARUTI Marco, Universita Degli Studi Di Padova, Italy
HANWA Anne, University of Ngaoundéré, Cameroon
HASSAN Hoyam, University of Khartoum, Sudan
IBARA NGIZA MFUMU Roslan, University Marien Ngouabi, Brazaville, Congo
KAMWA DJOMOU Franck Rivel, University of Dschang, Cameroon
KEM-MEKA Peguy, AIMS-Cameroon
LELIEVRE Samuel, University Paris-Sud, France
LEPEYI-LEBOUMA Junior, Ecole Normale Supérieure, Libreville, Gabon
LORENZO GARCIA Elisa, University Rennes 1, France
MAIGA Abdoulaye, AIMS-Senegal, Dakar, Senegal
MAIRE Christian, University of Franche-Comté, France
MANTIKA Gilbert, University of Maroua, Cameroon
MEMIAGHE LENGA Fermi Adrien, Ecole Normale Supérieure, Libreville, Gabon
MOHAMMED FAGEER KHAKIFA Ibrahim, Sudan University, Khartoum, Sudan
MONNEAU Régis, Ecole des Ponts, ParisTech, France
NDONG'A OWINO Julia, Jaramogi University of Science and technology, Bondo, Kenya
NGO BABEM Annette, AIMS-Cameroon, Cameroon
NKOTTO NKUNG ASSONG Sedric, University of Kassel, Germany
NZAGANYA Nzaganya Edilson, University of Dar es salaam, Tanzania
OKANZA-PEA Mélodie, University Marien Ngouabi, Brazaville, Congo
OULD MOHAMED Rezki, University Houari Boumediene, Alger, Algeria
PECHA Amina, University of Maroua, Cameroon

PONCHO-KOTEY Ephraim Nii Amon, AIMS Rwanda, Kigali, Rwanda
RAVELOMANANA Vlady, CIMPA and University Paris Diderot, France
ROY Marie-Françoise, University Rennes 1, France
SAINHERY Phrador, University of Padova, Italy
SALIOU Douboula, University of Maroua, Cameroon
SALISSOU DANGO Mamane Djamilou, University Abdou Moumouni, Niamey, Niger
SALL Mohamadou, Senegal
SANKARA Karim, University Nazi Boni, Burkina Faso
SETH-KOUMLA Kang-Rang, University Abdou Moumouni, Niamey, Niger
SEYDOU Moussa, University Dan Dicko Dankoulodo de Maradi, Niger
SONKOUE Jacques, University Yaoundé 1, Cameroon
YOUEGO Jocelyne, University of Ngaoundere, Cameroon
YOUMBI Norbert, St-Francis University, Poretto PA, USA

July 21, 2019

Annexes

- Exercices by Elisa Lorenzo Garcia
- Exercices by Tony Ezome
- Exercices by Marie-Françoise Roy
- Exercices by Michel Coste
- Projects by M.-F. Roy and E. Lorenzo Garcia
- Projects by M. Coste
- Questionnaire

Algebraic Number Theory and Class Field Theory. Exercises

Elisa Lorenzo García

Exercise 0.1. *Let d be a free-square integer, prove the following:*

$$\mathcal{O}_{\sqrt{d}} = \begin{cases} \mathbb{Z}[\sqrt{d}] \text{ if } d \equiv 2,3 \text{ mod } 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \text{ if } d \equiv 1 \text{ mod } 4 \end{cases}$$

Exercise 0.2. *Is the extension $\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}$ Galois? If yes, compute its Galois group.*

Exercise 0.3. *Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Compute the trace $Tr_{L/K}$ and norm $N_{L/K}$ of $1, \zeta_3, \sqrt[3]{5}$ and $\sqrt{-3}$.*
Take now $L = \mathbb{Q}(\sqrt{2+\sqrt{3}})$ and compute the trace and norm of $1, \sqrt{3}$ and $\sqrt{2+\sqrt{3}}$.

Exercise 0.4. *Let $K = \mathbb{Q}(\alpha)$ be a cubic extension with $\alpha^3 + A\alpha + B = 0$ for some $A, B \in \mathbb{Z}$. Assume that $< 1, \alpha, \alpha^2 >$ is a basis of $\mathcal{O}_K$ (then $\mathcal{O}_K$ is monogenetic). Prove that $\Delta_K = disc(P_\alpha) = -4A^3 - 27B^2$.*

Exercise 0.5. *Let A be a ring and I a maximal ideal. Prove that I is prime.*

Exercise 0.6. *Compute the inverse of $I = (2, 1+\sqrt{-5})$ in $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$.*

Exercise 0.7. *Can you explain why the following equality*

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

looks like implying that the uniqueness of the prime ideal factorization is not true in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$?

Exercise 0.8. *Factorize the ideal (7) in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-13})$ and write down the prime ideas in its decomposition in the standard form we saw during the course.*

Exercise 0.9. *Find the fundamental units of $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{17})$.*

Exercise 0.10. *Find the decomposition of (p) in $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ for $p = 2, 3, 5, 7, 11, 13, 17$ and 19.*

Exercises

Lecturer : Tony EZOME

1. Download and install Pari/GP (it is free, you just need to google PARI/GP Bordeaux)

2. Let t be a uniformizer at 0 on the projective line $\mathbb{P}^1$. Show that $\mathrm{div}(dt) = -2[\infty]$ and deduce the genus of $\mathbb{P}^1$. Compute the Zeta function of the projective line.

3. Assume that $\mathrm{Char}(k) \neq 2$. Let $e_1, e_2, e_3 \in \overline{k}$ be distinct, and consider the curve

$$E/k : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

   Show that its closure $\overline{E}$ in $\mathbb{P}^2$ has a single point at infinity which is smooth (we denote it ∞). Compute the divisors $\mathrm{div}(x - e_i)$, $\mathrm{div}(y)$, $\mathrm{div}(x)$ and deduce the genus of E.

4. Show that

$$C_a/\mathbf{F}_{11} : y^2 = x^5 - 1$$

   is a smooth affine (irreducible) curve. Show that C_a defines a hyperelliptic curve C over $\mathbf{F}_{11}$. Determine the genus of C. Compute the Zeta function of C and compute also $\#J_C(\mathbf{F}_{11})$.

5. Let $p = 557,\ d = 1$ and $\mathbf{F}_q = \mathbf{F}_{557}$. Show that

$$E/\mathbf{F}_{557} : Y^2Z = X^3 - 10XZ^2 + 21Z^3$$

   is an elliptic curve. Using Baby-step-giant-step algorithm compute the cardinality $\#E(\mathbf{F}_{557})$ and compute also the order of $P = (2 : 3 : 1)$.

6. Show that

$$E/\mathbf{F}_5 : Y^2Z = X^3 - 2XZ^2 + 1Z^3$$

   is an elliptic curve. Check that $3(0 : 1 : 1) = (2 : 1 : 1)$ on E and show that $(0 : 1 : 1)$ generates $E(\mathbf{F}_5)$.

7. Show that

$$E/\mathbf{F}_{19} : Y^2Z = X^3 - 2XZ^2 + 1Z^3$$

   is an elliptic curve. Using Schoof algorithm compute the cardinality $\#E(\mathbf{F}_{19})$.

EXERCISES: QUANTITATIVE AND ALGORITHMIC METHODS IN REAL ALGEBRAIC GEOMETRY LIMBE AIMS CAMEROON CIMPA SCHOOL, 2019

MARIE-FRANÇOISE ROY

Exo 1. Determine the number of real roots of $X^3 - X$, $X^3 - 1$, $X^3 - X^2$

- using Sturm sequence
- using the signs of subresultant coefficients.

Exo 2. Consider

$$P = X^3 + aX + b$$

with a,b, c parameters.

- Discuss, in terms on sign conditions depending on a, b, what is its number of real roots.
- Discuss, in terms on sign conditions dependant on a, b, how many roots are > 1 and how many roots are < 1 ?

Geometric representation in the plane a, b.

Exo 3. Prove that, if R is a real closed field,

- all positive numbers have a square root,
- all polynomials of odd degree have a root.

Exo 4. Prove Rolle's theorem in a real closed field: if $a < b$ $P(a) = P(b) = 0$, there exists $c \in (a, b)$ with $P'(c) = 0$.

Exo 5. Using IVT, the Intermediate Value Theorem, determine the Thom encodings of the roots of all the derivatves of $X^3 - X$.

Exo 6. Prove that the field of real algebraic numbers $\mathbb{R}_{\mathrm{alg}}$ is real closed,

Marie-Françoise Roy Laboratoire IRMAR, Université de Rennes 1, Campus de Beaulieu, bât. 22-23, 35042 Rennes Cédex, France

Email address: `marie-francoise.roy@univ-rennes1.fr`

Exercises in Robot Kinematics
CIMPA school, Limbe, July 2–12, 2019

Michel Coste

Exercises with * are better dealt with using Sage.

Exercise 1*. Compute the Jaconbian determinant for the Inverse Kinematic Mapping $(\varphi, x, y) \mapsto (\rho_1, \rho_2, \rho_3)$. Verify that the Jacobian determinant vanishes iff the three lines $(A_1B_1), (A_2B_2), (A_3B_3)$ are concurrent or parallel. (This can be done fixing the dimensions of the robot, or leaving them as parameters; computations are easier to make with the help of Sage).

Exercise 2. Fix $\mathbf{x} = (x_0, x_1, x_2, x_3) \in \mathbb{R}^4$ such that $\sum_{i=0}^{3} x_i^2 \neq 0$. Show that for any vector $\mathbf{t} \in \mathbb{R}^3$, there is a unique $\mathbf{y} = (y_0, y_1, y_2, y_4) \in \mathbb{R}^4$ such that $\sum_{i=0}^{3} x_i y_i = 0$ and the rigid motion given by the Study parameters $\mathbf{x}, \mathbf{y}$ has translation vector equal to $\mathbf{t}$.

Exercise 3. Find Study parameters for the half-turn with axis the line through $(1, 0, 0)$ parallel to vector $(0, 1, 0)$.

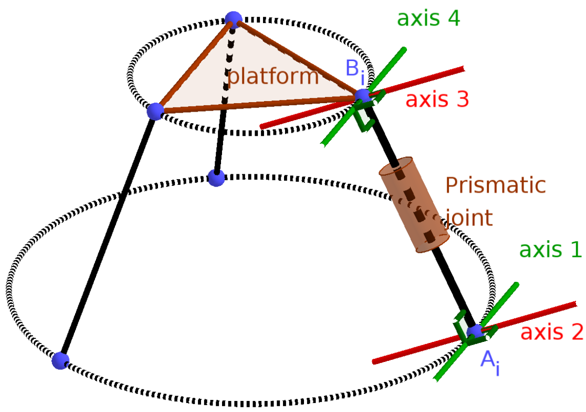
Exercise 4. Justify the description of the operation modes of the SNU 3-UPU:

$K_0 = \langle y_0, y_1, y_2, y_3 \rangle$: rotation around the origin
$K_1 = \langle y_0, x_1, x_2, x_3 \rangle$: translation
$K_2 = \langle x_0, y_1, x_2, x_3 \rangle$: half-turn with vertical axis, then translation
$K_3 = \langle y_0, y_1, x_2, x_3 \rangle$: motion in the base plane
$K_4 = \langle x_0, x_1, y_2, y_3 \rangle$: horizontal flip, then motion in the base plane
$K_5 = \langle x_0, y_1, y_2, y_3 \rangle$: half-turn then translation in the direction of the axis of half-turn
$K_6 = \langle y_0, x_1, y_2, y_3 \rangle$: half-turn with vertical axis, then K_5

(Hint: relationship between K_1 and K_2, or K_3 and K_4, or K_5 and K_6 can be understood by computing $(p + \epsilon q)\,\mathbf{i}$ or $(p + \epsilon q)\,\mathbf{j}$.)

Exercise 5*. Let $\mathfrak{I} = \langle X^2 - Y^2 - 1, XY^2 - X^2Y \subset \mathbb{Q}[X, Y] = R$. What can you say about the quotient ring $R/\mathfrak{I}$? (Computing a Groebner basis by hand may help, and you can check your computation with Sage).

Exercise 6*. Explore the modes of operation of the Tsai 3-U$\underline{\text{P}}$U. In this architecture, axes 1 and 4 for each limb are tangent to the circumscribed circles of the base and platform respectively:



1. Quantitative and algorithmic methods in real algebraic geometry. Marie-Francoise Roy: Projects

1.1. Project 1: Discriminant. The aim of the project is to study the classical notion of discriminant and the ways to determine it.

The discriminant of a univariate polynomial expresses the condition for the existence of multiple roots. Its sign gives some information about the number of real roots.

In the case of a plane curve given as the zero set of a bivariate polynomaisl p, the real zeroes of the discriminant of P play an important role in the determination of the topology of the curve.

When a polynomial is given, its roots are not easily known but there are two methods to compute the discriminant as the determinant of a matrix obtained from its coefficients.

The project is based on part of [1] Chapter 4 Section 1 and the beginning of Chapter 11 Section 6 (for the case of a curve).

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in real algebraic geometry. Springer. Available at https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.pdf.

1.2. Project 2: Virtual roots. The aim of the project is to study the recent notion of virtual roots and their properties.

A univariate polynomial of degree d does not have always d real roots, even counted with multiplicities and the real roots of a polynomial depending on a parameter are not continuous (because some real roots become complex).

But there are always d virtual roots counted with virtual multiplicities, and they vary continuously.

Virtual roots are closely related to Budan-Fourier's theorem.

The project is based on [1] Chapter 2 Section 1.1

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in real algebraic geometry. Springer. Available at https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.pdf.

1.3. Project 3: Geometric representations of degree 4 polynomials having a given number of real roots. The aim of the project is to represent geometrically the various zones of the space (a, b, c) with the number of real roots of $X^4 + aX^2 + bX + c$ is fixed.

The pictures will be drawn using SageMath.

The project uses results given in the course of Marie-Francoise Roy on computing the number of roots using signs of subresultant coefficients.

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in real algebraic geometry. Springer. Available at https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.pdf.

2. Algebraic Number Theory and Class Field Theory. Elisa Lorenzo Garcia: Projects

2.1. **Project** 1. What is the definition of the resultant $Res_x(f,g)$ of 2 polynonials $f,g \in A[x]$ with entries in a ring A?
Prove that: if $f,g \in k[x]$ are monic polynomials in one variable over an algebraic closed field and over $\bar{k}$ we have $f = \prod_i^n (x-\alpha_i)$ and $g = \prod_j^m (x-\beta_j)$, then

$$Res_x(f,g) = (-1)^{mn} \prod (\alpha_i - \beta_j).$$

Use this property to show that given $a,b \in L/K$ with minimal polynomials $P_a(x)$ and $P_b(x)$, then the minimal polynomial of $a+b$ is $P_{a+b}(y) \mid Res_x(P_a(x), P_b(y-x))$. Apply this to compute the minimal polynomial of $\sqrt{2}+\sqrt[3]{5}$.

2.2. **Project** 2. (pages 51-52 and ...) Let K be the cyclotomic field $\mathbb{Q}(\zeta_n)$. Assume $n=p$ is an odd prime number.Prove the following:

- $\mathcal{O}_K =< 1, \zeta_n, \zeta_n^2, ..., \zeta_n^{n-1} >$,
- $Tr(\zeta_n) = -1$,
- $N(\zeta_n) = 1$,
- $\Delta_K = (-1)^{(p-1)/2} p^{p-2}$.

2.3. **Project** 3. (pages 97-100 in Samuel's book) Prove Lagrange Theorem saying that every positive integer is the sum of 4 squares. Ex.: $1 = 1^2+0^2+0^2+0^2$, $5 = 2^2+1^2+0^2+0^2$, $9 = 2^2+2^2+1^2+0^2$, ...

2.4. **Project** 4. (pages 72-75 in Samuel's book) Prove Dirichlet Theorem saying that: let K be a number field of degree $n = r_1 + 2r_2$ (r_1 stands for the number of real embedding of K). Then the group $\mathcal{O}_K^*$ of unities of K is isomorphic to $\mathbb{Z}^r \times G$ where $r = r_1 + r_2 - 1$ and G is a finite cyclic group made off the roots of unity contained in K.

2.5. **Project** 5. (http://www.rzuser.uni-heidelberg.de/ hb3/fchrono.html) Explain a proof for the Quadratic Reciprocity Law:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}.$$

3. Semi-algeraic geometry and modelizaton in Robot Kineatics. Michel Coste: Projects

3.1. **Project** 1 **Number of solutions to the direct kinematic problem for a Gough-Stewart platform.** How many poses can a Gough-Stewart platform possess for given lengths of the limbs of the platform? There were several papers dedicated to this problem. The aim of the project is to study and understand (at least in the main lines) a rather simple solution to this problem, which is based on an adequate algebraic modelization using quaternions and dual quaternions presented in the course.

C. Wampler: *Forward displacement analysis of general six-in-parallel SPS (Stewart) platform manipulators using soma coordinates* (1996)

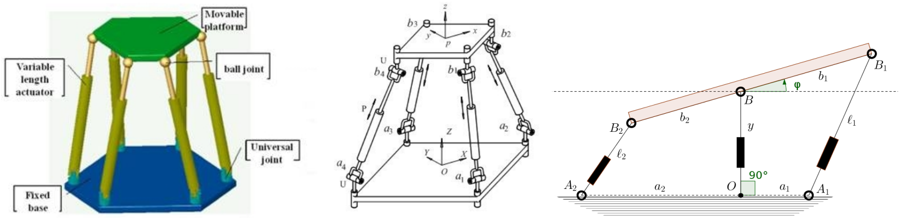
3.2. **Project** 2 **Unwanted modes of operation for some parallel robots.** A 4-U$\underline{\text{P}}$U is designed to give 4 degrees of freedom to a mobile horizontal platform: all translations in 3-space and rotations with vertical axis possible. It happens that, for a wide range of dimensions of this robot, there are extra modes of operation with 3 d.o.f. where the platform is no longer horizontal. The aim of the project is to use Sage to write down an algebraic modelization of the kinematics and exhibit the existence of these different modes of operation.

M. Coste, K.M. Demdah: *Extra modes of operation and self motions in manipulators designed for Schoenflies motion* (2014)

3.3. **Project** 3 **A simple parallel robot with strange singularities, and their perturbations.** A simple planar robot exhibits two singular poses with unusual features. A small perturbation of the architecture of the robot unfolds these singularities into folds ans cusps (stable singularities, explained in the course). The aim of the project is to use Sage to modelize the inverse kinematic mapping for te robot and its perturbed version and to study the singularities in both situations.

M. Coste, P. Wenger, D. Chablat: *Hidden cusps* (2016)

A Gough-Stewart platform (1), a 4-U$\underline{\text{P}}$U (2) and a 2-R$\underline{\text{P}}$R-PR (3):



Mini-projects on robotics - Michel Coste

1. **Number of solutions to the direct kinematic problem for a Gough-Stewart platform.**

   How many poses can a Gough-Stewart platform possess for given lengths of the limbs of the platform? There were several papers dedicated to this problem. The aim of the project is to study and understand (at least in the main lines) a rather simple solution to this problem, which is based on an adequate algebraic modelization using quaternions and dual quaternions presented in the course.

   C. Wampler: *Forward displacement analysis of general six-in-parallel SPS (Stewart) platform manipulators using soma coordinates* (1996)

2. **Unwanted modes of operation for some parallel robots**

   A 4-UPU is designed to give 4 degrees of freedom to a mobile horizontal platform: all translations in 3-space and rotations with vertical axis possible. It happens that, for a wide range of dimensions of this robot, there are extra modes of operation with 3 d.o.f. where the platform is no longer horizontal. The aim of the project is to use Sage to write down an algebraic modelization of the kinematics and exhibit the existence of these different modes of operation.

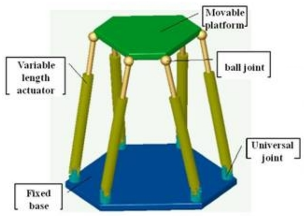
   M. Coste, K.M. Demdah: *Extra modes of operation and self motions in manipulators designed for Schoenflies motion* (2014)

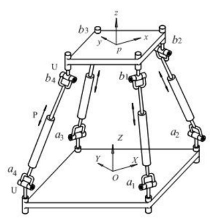
3. **A simple parallel robot with strange singularities, and their perturbations**

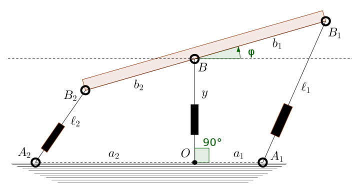
   A simple planar robot exhibits two singular poses with unusual features. A small perturbation of the architecture of the robot unfolds these singularities into folds ans cusps (stable singularities, explained in the course). The aim of the project is to use Sage to modelize the inverse kinematic mapping for te robot and its perturbed version and to study the singularities in both situations.

   M. Coste, P. Wenger, D. Chablat: *Hidden cusps* (2016)

A Gough-Stewart platform (1), a 4-UPU (2) and a 2-RPR-PR (3):







Dear attendee to the CIMPA school Algebraic Geometry, Number Theory and Applications in Cryptography and Robot kinematics at AIMS-Cameroon, Limbe

This questionnaire aims at evaluating this school and improving future ones
No need to give your name (unless you want to) but tell us your mathematical level

Master student / Ph D student / Already with Ph D

Male / Female

Courses

For each course evaluate from 1 to 5

Marie-Françoise Roy, Quantitative and algorithmic recent results in real algebraic geometry

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Was the topic new to you ? YES / NO

Elisa Lorenzo Garcia, Basic algebraic number theory and class field theory

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Was the topic new to you ? YES / NO

Tony Ezome, Point counting on algebraic varieties and applications in cryptography

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Was the topic new to you ? YES / NO

Christian Maire, Tate Module and Abelian Varieties

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all
Was the topic new to you ? YES / NO

Michel Coste, Advanced topics in semi-algebraic geometry and modelization in Robot Kinematics

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Was the topic new to you ? YES / NO

Marco Garuti, Fundamental groups in Algebraic and Arithmetic Geometry

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Was the topic new to you ? YES / NO

Samuel Lelievre, Introduction to SAGE

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Was the topic new to you ? YES / NO

Exercises sessions

evaluate from 1 to 5

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Did you participate actively in exercise sessions by going to the blackboard YES /NO

Short lectures by young researchers

evaluate from 1 to 5

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Mini project

Sessions presenting the mini-projects: evaluate from 1 to 5

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Did you participate to a ini-project ? YES/NO

If YES, how do you evaluate how difficult/useful/interesting it has been

1 very easy 2 easy 3 adequate 4 difficult 5 very difficult

1 very useful 2 useful 3 adequate 4 not very usefuf 5 not useful at all

1 very interesting 2 interesting 3 weakly interesting 4 not interesting 5 not interesting at all

Language

Are you francophone /anglophone

Was your level in englsh sufficient to follow the school ? YES / NO

Accomodation

Was your room cumfortable enough ? YES / NO

Remarks

Food

Was the quality of the food satisfactory ? YES / NO

Was there enough food ? YES / NO

Remarks

Global organizaton

Are you satisfied with the organization of the school?

1 very satisfied 2 satisfied 3 mildly satisfied 4 not satisfied 5 not satisfied at all

Your arrival: are you satisfied with the way you were taken care of upon arrival ?

1 very satisfied 2 satisfied 3 mildly satisfied 4 not satisfied 5 not satisfied at all

Global evaluation

Are you satisfied with the school?

1 very satisfied 2 satisfied 3 mildly satisfied 4 not satisfied 5 not satisfied at all

Was it an oppportunity to know better your research area ? YES / NO

Was it an oppportunity to discover a different research area ? YES / NO

Do you feel it helped you understand the nature of mathematical research ? YES / NO

Was it an opportunity to meet the professors of the school ? YES/NO

Was it an opportunity to meet students from other african countries ? YES/NO

Was it an opportunity to meet professors from other african countries ? YES/NO

General remarks helping us to improve the CIMPA schools

Please feel free to write what you thought