Elliptic Curves – an Introduction

BERND KREUSSLER

The following four articles constitute expanded versions of talks given during a mini-workshop which took place at Mary Immaculate College, Limerick, on the 29^{th} and 30^{th} of November 2006. The titles of these talks were the following:

(1) *Solving Cubic Equations in Two Variables.*
(2) *Group Law on the Cubic Curve.*
(3) *Theta Functions.*
(4) *Rank two Vector Bundles on Elliptic Curves.*

Elliptic curves are very interesting because their study involves several fields of mathematics. The study of elliptic curves has a long history and still there are many unsolved problems. The goal of the mini-workshop was to provide an introduction for the non-specialist to several aspects of elliptic curves.

Elliptic curves reside at the crossroads of *arithmetic*, *geometry* and *analysis*. This was reflected in the talks as follows: talk (1) dealt with the arithmetic of elliptic curves whereas in talk (2) elliptic curves were studied from the point of view of complex algebraic geometry. The complex analytic side of elliptic curves was touched within talk (3). After these basics were laid down, talk (4) gave an introduction to the study of vector bundles on an elliptic curve. This highlighted the fact that it is not only interesting to study elliptic curves on their own but also to investigate other geometric objects of interest constructed on them.

It is clear from the number of pages used that the four articles can provide only a small bit of the available huge amount of knowledge and techniques related to elliptic curves. None of the many applications in physics, engineering and modern communication technology are discussed. To give the reader a first idea of the subject, a brief description of included and excluded material is given below.

I would like to thank Pat O'Sullivan for acting as a critical reader of the first drafts of all the four articles.

Solving Cubic Equations in Two Variables (Bernd Kreussler)

The first article starts with the elementary question of finding all Pythagorean triples of integers and goes on to apply similar ideas in order to find integer solutions of equations of degree three in two variables. The material is illustrated through many explicit examples. This part is probably suited for interested second-level students (in fact there was one among the audience for the first talk). The last section gives a brief overview of the most basic results about the Mordell–Weil group of a cubic curve.

However, there are many things which are not even mentioned in this article but which are no less important or fascinating than the material included. In particular, zeta-functions and L-functions are not included. As a consequence, the Birch and Swinnerton-Dyer conjecture is not formulated even though this is one of the Millennium Prize Problems. The important method of infinite descent as well as the Selmer and Tate–Shafarevich groups did not find their way into the article. The very interesting connection of elliptic curves with the solution of Fermat's Last Theorem (through the Frey curve) is another omission. The growing practical relevance of elliptic curves in modern cryptography is another issue missing. This list is certainly not complete. A few books which may help the interested reader to satisfy his or her thirst for knowledge are [6, 7, 13, 14, 15].

Group Law on the Cubic Curve (Madeeha Khalid)

The aim of the second article is to give an introduction to some basic concepts from complex algebraic geometry which allow a geometric understanding of the group structure introduced in the first talk. A brief introduction is given to complex manifolds, vector bundles on them and the Picard group (the group of all line bundles). Moreover the relationship between line bundles and divisors on a curve is explained, which allows a better understanding of the group structure introduced in the previous article.

The Weierstraß $\wp$-function and elliptic integrals are used to explain how complex analysis enters the picture. As a result, each cubic curve can also be seen as a complex torus, which comes with its own group structure. The gem of this article is a sketch of a proof that this analytically defined group structure coincides with the one introduced algebraically. This is based on Abel's Theorem. The analytic details are provided in the third article.

Again, many more things could have been included here. For example, higher dimensional Abelian Varieties and the Abel–Jacobi map which naturally emerge in the study of curves of higher genus are not mentioned. The idea of a scheme over an arbitrary commutative ring with unity are definitely beyond the scope of this article. To introduce the ideas of a moduli space and of a universal object would be a natural next step after the introduction of the Poincaré bundle. A higher dimensional analogue of an elliptic curve would be a so-called K3-surface. Their study has much in common with the theory of elliptic curves but they couldn't be touched either. There are many excellent textbooks available, among which are [3, 5, 16].

Theta Functions (Marina Franz)

This article gives a brief introduction to some basics in the modern theory of elliptic functions. The starting point are theta functions, which are nothing but global sections of line bundles on a one-dimensional complex torus. Their main properties are investigated from a purely analytic point of view. Moreover, these theta functions are related to the Weierstraß $\wp$-function, which can be considered to be the most basic elliptic function. A proof that this function satisfies a certain differential equation is given. This equation shows that a complex torus of dimension one can be embedded in the projective plane as a cubic curve. A proof of Abel's Theorem, which plays a major role in the previous article is also provided.

The same remark applies to this article as to the other two: there is much more material available than could be included. For example, an explicit description of the relationship between theta functions and holomorphic line bundles on elliptic curves is missing. Moreover, the fascinating theory of elliptic functions is only touched on. In particular, nothing is said about elliptic integrals. These arise, for example when the length of an ellipse is to be calculated. Historically, the study of elliptic integrals motivated the introduction of elliptic functions by Abel and Jacobi. Weierstraß built the theory of elliptic functions on the $\wp$-function, but beforehand Jacobi's elliptic functions $\mathsf{sn}(z), \mathsf{cn}(z), \mathsf{dn}(z)$ were the main players. Their role in mathematical applications in engineering are definitely beyond the scope of this short article. Theta functions are available on higher-dimensional tori as well, but this is not covered here. Such material and much more can be found in [12, 1, 10, 9].

Rank two Vector Bundles on Elliptic Curves (Ciara Daly)

In contrast to the three others, this fourth article is not primarily concerned with the group structure on an elliptic curve. But it is a direct continuation of these. Vector bundles of rank one and their sections were studied in the previous two articles. The moduli space interpretation of the Picard group is already mentioned in the second article. This article presents the main results about vector bundles of rank two on an elliptic curve. These go back to a seminal paper of Atiyah from 1959. This example is used to introduce to the theory of moduli, which is at the centre of modern algebraic geometry. The related notion of a stable vector bundle is also introduced.

Of course, there is much more that could be said in this context. Atiyah studied vector bundles of any rank, not only of rank two, but this did not find its way into this article. Also, the problems involved with the notion of stability of vector bundles on higher dimensional manifolds are not discussed. The theory of moduli of varieties as opposed to vector bundles is another huge area of algebraic geometry which is omitted. The relations of algebraic geometry to differential geometry and to theoretical physics through the theory of moduli spaces are not mentioned. Another quite recent development was the introduction of the space of stability conditions by Bridgeland. To define this invariant it would be necessary to introduce coherent sheaves and derived categories, so that this development could also not be covered here. The interested reader will find relevant starting points in [4, 8, 11, 17, 2].

REFERENCES

[1] N.I. Akhiezer, *Elements of the theory of elliptic functions.* Translations of Mathematical Monographs 79, AMS (1990)

[2] T. Bridgeland, *Derived categories of coherent sheaves.* Proceedings of the international congress of mathematicians (ICM), Madrid, Spain, August 22–30, 2006, Volume II, 563–582 (2006)

[3] P. Griffiths, J. Harris, *Principles of algebraic geometry.* John Wiley & Sons (1978)

[4] D. Huybrechts, M. Lehn, *The geometry of moduli spaces of sheaves.* Aspects of Mathematics E 31, Vieweg (1997)

[5] F. Kirwan, *Complex algebraic curves.* London Mathematical Society Student Texts 23, Cambridge University Press (1992)

[6] A.W. Knapp, *Elliptic curves.* Mathematical Notes (Princeton) 40, Princeton University Press (1992)

[7] N. Koblitz, *Algebraic Aspects of Cryptography.* Springer (2004)

[8] J. Le Potier, *Lectures on vector bundles.* Cambridge Studies in Advanced Mathematics 54, Cambridge University Press (1997)

[9] H. McKean, V. Moll, *Elliptic curves. Function theory, geometry, arithmetic.* Cambridge University Press (1999)

[10] G. Mittag-Leffler, *An introduction to the theory of elliptic functions.* Annals of Math. (2) 24, 271–351 (1923)

[11] S. Mukai, *An introduction to invariants and moduli.* Cambridge Tracts in Mathematics 81, Cambridge University Press (2003)

[12] D. Mumford, *Tata lectures on theta I, II, III.* Reprint of the 1991 edition, Modern Birkhäuser Classics, Birkhäuser (2007)

[13] J.H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer (1986)

[14] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics 151, Springer (1994)

[15] J.H. Silverman, J. Tate, *Rational points on elliptic curves.* Undergraduate Texts in Mathematics, Springer (1992)

[16] K. Ueno, *An introduction to algebraic geometry.* Translations of Mathematical Monographs 166, AMS (1997)

[17] E. Viehweg, *Quasi-projective moduli for polarized manifolds.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3. Folge) 30, Springer (1995)

Bernd Kreussler,
Mary Immaculate College,
South Circular Road,
Limerick, Ireland
bernd.kreussler@mic.ul.ie

Received in final form on 23 August 2007.