ARITHMETIC OF ELLIPTIC CURVES AND OF DRINFELD MODULES

DANIEL MACÍAS CASTILLO

1. Arithmetic of elliptic curves

For now, let F be a number field, that is, a finite extension of $\mathbb{Q}$. Let E be an elliptic curve defined over F, that is, the abelian group of solutions over the field of algebraic numbers of an equation $Y^2 = X^3 + AX + B$ with $A, B \in F$. Then the 'Mordell-Weil group' of E/F is the subgroup $E(F)$ of E comprising solutions (x, y) with $x, y \in F$. Said differently, $E(F)$ is the abelian group of solutions of the Diophantine problem defined by the above equation.

The foundational result of arithmetic geometry is the Mordell-Weil Theorem (1929). It states that the abelian group $E(F)$ is finitely generated, that is, there exists $r \geq 0$ and points $P_1, \ldots, P_r \in E(F)$, of infinite order, for which

$$E(F) = (\mathbb{Z} \cdot P_1 \oplus \ldots \oplus \mathbb{Z} \cdot P_r) \oplus E(F)_{\text{tor}},$$

where $E(F)_{\text{tor}}$ is the finite subgroup of points of finite order of $E(F)$. The determination of the 'rank' $r \geq 0$ of E/F is the content of the Birch and Swinnerton-Dyer Conjecture, one of the 'Millennium Prize Problems'.

The main objective of this project is to learn the basic algebraic number theory (that is, the theory of number fields) from chapters I and II of [2], and the basic theory of elliptic curves from [4], that are necessary to understand the main ideas involved in the proof of the Mordell-Weil Theorem (which is given in chapter VIII of [4]). Some complementary references for elliptic curves could be [1, 5].

2. Arithmetic of Drinfeld modules

A 'global function field' is a finite extension of the field of rational functions $\mathbb{F}_q(t)$ (over some finite field $\mathbb{F}_q$ and for a transcendental variable t). The theory of global function fields shares many similarities with that of number fields, with $\mathbb{F}_q(t)$ playing the role of $\mathbb{Q}$ and the polynomial ring $\mathbb{F}_q[t]$, which is a principal ideal domain with field of fractions $\mathbb{F}_q(t)$, playing the role of $\mathbb{Z}$.

In this setting, Vladimir G. Drinfeld introduced in the 1970s a notion of 'elliptic modules', now commonly referred to as Drinfeld modules, and used them to prove new cases of the Langlands conjectures. Despite the fact that their definition is very different, the theory of Drinfeld modules has striking analogies with the theory of elliptic curves.

Now let F be a global function field and let D be a Drinfeld module defined over F. One can define an obvious analogue $D(F)$ of Mordell-Weil groups, as a module over the polynomial ring $\mathbb{F}_q[t]$. However, the naive analogue of the Mordell-Weil Theorem turns out to be false: by a result due to Poonen, $D(F)$ is never finitely generated as a module over $\mathbb{F}_q[t]$.

It was not until 2010 that L. Taelman formulated the statement that is now regarded as the correct analogue of the Mordell-Weil Theorem. Taelman proved the validity of this statement by applying basic techniques of 'non-archimedean analysis'. Since this breakthrough, the arithmetic of Drinfeld modules has become a very active area of research.

Depending on time availability and on the students' interests and previous knowledge, another objective of this project could be to learn the basic theory of Drinfeld modules from the book [3]. We note that the structure and the topics of this book were directly inspired by [4] (through the aforementioned analogies with elliptic curves), so it provides a very natural counterpart for this objective.

In addition, this books includes a fully self-contained explanation and proof of Taelman's result (that is easier to follow than the original article [6]). It also contains a proof of Poonen's result.

References

[1] J. W. S. Cassels, Lectures on Elliptic Curves, LMS Student Texts, Cambridge University Press, 1991.
[2] J. Neukirch, Algebraic Number Theory, Springer, 1999.
[3] M. Papikian, Drinfeld Modules, Grad. Text. Math. **296**, Springer, Cham. (2023).
[4] J. Silverman, The Arithmetic of Elliptic Curves, 2nd Ed., Springer-Verlag, New York, 2009.
[5] J. Silverman, J. T. Tate, Rational Points on Elliptic Curves, 2nd Ed., Springer, New York, 1986.
[6] L. Taelman, A Dirichlet unit theorem for Drinfeld modules, Math. Ann. **348** (2010) 899-907.