Seminar

Gil Cohen

June 13, 2022

Overview

The Hasse-Weil & Drinfeld-Vladut bounds

Riemann's Hypothesis is considered by many as the most fundamental open problem in number theory. It was proposed by Bernhard Riemann in 1859.

This cluster is about the proof of the Riemann Hypothesis in the context of function fields, a problem raised by Artin in 1924.

Hasse proved the hypothesis for genus 1 and thenm in 1948, Weil proved the hypothesis in general.

Weil conjectured higher dimension analogs which were proved by Deligne (1974, 1980).

Generally, if one faces a problem in number theory, it is a good practice to consider the function field analog and try to prove it using the now available tools from algebraic geometry.

For example, in the recitation you will prove Fermat's Last Theorem for polynomials.

The Hasse-Weil & Drinfeld-Vladut bounds

Recall the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \qquad s \in \mathbb{C},\ \mathrm{Re}(s) > 1$$

which can be extended uniquely to a meromorphic function on the entire complex plane. We also have Eurler's product formula,

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Riemann's hypothesis states that $\zeta(s) = 0$ only if $\mathrm{Re}(s) = \frac{1}{2}$ (as well as on other trivial cases).

The Hasse-Weil & Drinfeld-Vladut bounds

A natural analog of the Riemann ζ function can be defined over any function field $F/\mathbb{F}_q$, namely,

$$\zeta_F(s) = \sum_{\mathfrak{a} \geq 0} q^{-s \deg \mathfrak{a}} = \prod_{\mathfrak{p} \in \mathbb{P}(F)} \frac{1}{1 - q^{-s \deg \mathfrak{p}}}.$$

The non-trivial roots of ζ_F was shown to have real component $\frac{1}{2}$ thus establishing a proof for Riemann Hypothesis for function fields.

This establishes, in our context, impossibility results for AG codes.

The Hasse-Weil & Drinfeld-Vladut bounds

Sources:

1. For the Hasse-Weil bound, Dan's lecture notes, chapters 24-31. You may consult Sections 5.1, 5.2 of Stichtenoth if you wish.
2. Afterwards, for the Drinfeld-Vladut bound, you should cover Section 5.3 and Section 7.1 of Stichtenoth.

This is a project for 4-5 students.

Requires some basic knowledge in complexity analysis.

Building on Riemann-Roch, constant field extensions, analysis of automorphisms, etc. It essentially involves everything we did but for adeles and differentials.

Overview

Differentials

Weil differentials, which were used for the proof of Riemann-Roch and Hurwitz Genus Formula, are very abstract. In this cluster we connect Weil differentials with “ordinary” differentials.

Moreover, we will explore dual AG codes via differentials.

Sources:

1. Section 1.7 - local components of Weil differentials.
2. Section 2.2 (after Remark 2.2.5) - dual AG codes.
3. Section 4.1 - derivatives and differentials.
4. Section 4.2 - The $\mathfrak{p}$-adic completion.
5. Section 4.3 - Differentials and Weil differentials (here the Residue Theorem is proved).
6. Section 8.1 - The residue representation.

This is a project for 4-5 students.

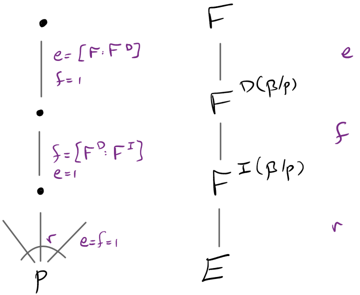
Overview

Ramification

Recall that in Galois extensions we have

$$efr = p.$$

In this cluster we will dig deeper into this, ramification, and the different exponent. E.g., we will decompose F/E to



$$\mathrm{D}(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\},$$
$$\mathrm{I}(\mathfrak{P}/\mathfrak{p}) = \ker(\text{something}).$$

Ramification

We will further consider a more refined filtration via ramification groups.

It is easy to prove that

$$\mathrm{D}(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \forall z \in \mathcal{O}_{\mathfrak{P}} \quad v_{\mathfrak{P}}(\sigma z - z) \geq 0\}.$$

One can further show that

$$\mathrm{I}(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \forall z \in \mathcal{O}_{\mathfrak{P}} \quad v_{\mathfrak{P}}(\sigma z - z) \geq 1\}.$$

So it is natural to consider

$$G_i(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \forall z \in \mathcal{O}_{\mathfrak{P}} \quad v_{\mathfrak{P}}(\sigma z - z) \geq i+1\}.$$

It turns out that $G_{i+1} \triangleleft G_i$ and that G_i/G_{i+1} is isomorphic to an additive subgroup of the residue field $\mathrm{F}_{\mathfrak{P}}$, hence is an elementary abelian p-group of exponent p.

Ramification

Based on these results some important theorems are proven, e.g., Hilbert's Different Formula

$$d(\mathfrak{P}/\mathfrak{p}) = \sum_{i=0}^{\infty} (|G_i(\mathfrak{P}/\mathfrak{p})| - 1),$$

as well as Abhyankar's Lemma and other results we used about ramification in compositum.

This is a beautiful and insightful cluster that involves Galois theory and some nice group theory.

Ramification

Sources:

1. Section 3.8 - Galois extensions II.
2. Section 3.9 Ramification and splitting in compositum of function fields.
3. Proof of Lemma 7.4.6 ($d = 2(e-1)$ for the GS tower; pages 266–268).

This is a project for 3-4 students.

Overview

Geometry

In the course we only hinted at the underlying geometry. In this cluster we make the connection.

We will follow Lorenzini's fantastic book: "An invitation to arithmetic geometry".

Only for student that did not take a course on algebraic geometry.

May require basic knowledge in topology & commutative algebra.

1. Chapter 2 - plane curves.
2. Chapter 6 - projective curves.
3. Chapter 7 - nonsingular complete curves.

Geometry

Chapter 2 is about plane curves.

1. 2.2 Rings of functions.
2. 2.3 Points and maximal ideals.
3. 2.4 Morphisms of curves.
4. 2.5 Singular points.
5. 2.7 More on dimension.
6. 2.8 Local principal ideal domains.
7. 2.9 Localization of modules (starting from Corollary 9.8).

This is a job for 3 students.

Geometry

Chapter 6 is about projective curves.

1. 6.2 Projective spaces.
2. 6.3 Projective curves.
3. 6.4 Plane projective curves.
4. 6.6 Projections.
5. 6.7 The tangent line at a point of a projective curve.
6. 6.8 Functions on projection curves.
7. 6.9 Projective curves and valuations.

This is a job for 3 students.

Geometry

Chapter 7 is about nonsingular complete curves.

1. 7.2 Nonsingular curves and Dedekind domains, revisited.
2. 7.3 Fields of definition and Galois actions on curves.
3. 7.4 Function fields.

This is a job for 3 students.

Overview

More about AG Codes

We have only seen the main connection between function fields and codes. In this cluster we explore other relations, and explore AG codes deeper.

1. Section 8.2 - Automorphisms of AG codes.
2. Section 8.3 - Hermitian codes.
3. Section 8.5 - Decoding AG codes.
4. Section 9.1 - On the dimension of subfield subcodes and trace codes.
5. Section 9.2 - Weights of trace codes.

This is a project for 5 students.

Overview

Genus estimation

Some general bounds on the genus: Castelnuovo's inequality and (as a special case) Riemann's inequality.

1. Section 3.10 - Inseparable extensions.
2. Section 3.11 - Estimates for the genus of function fields.

This is a project for 2 students.

Overview

How to proceed

- The clusters are mostly independent.
- Each student will email me its top 3 choices, in order, of a cluster.
- If you have a group set to take a cluster, please mention that as well as the name of your fellow students.
- I expect some coordination of talks within a cluster.
- I will most definitely want to cover clusters 1–4 so these are a priority.
- You don't have to split the work according to sections, etc.
- Each student is expected to give a talk (board or slides) for about an hour (no less than 50 minutes; no more than 90 minutes).
- The talk must be well-organized and clear. You should welcome questions from the audience.