Summary

Gil Cohen

June 10, 2019

Discussion

We have learned so much!

- *We started with plane curves $Z_f(K)$ (oh, youth!)*
- *The ring of polynomial functions C_f*
- *Played a little bit with resultants*
- *First significant theorem - Hilbert's Nullstellensatz*

The latter hinted that we should go algebraic so we did!

Discussion

- *Modules*
- *Integral extensions*
- *Field embeddings, separable extensions*
- *Krull dimension of a ring*
- *Noetherian rings and Dedekind domains*
- *Localization of rings and modules*
- *Factorization of ideals*
- *Hilbert's basis theorem*

Discussion

Then we used our new algebraic machinery.

- *Local PID and singularity*
- *Dedekind domains and unique factorization of ideals*
- *Dedekind domains and nonsingular curves*

At this point we turned things around and started from the abstract algebra (motivated by the geometric investigation)

- *Affine curves*
- *Valuations and local PIDs*
- *Complete nonsingular curves*
- *Function fields*

This enabled us to formally define poles, zeros and their multiplicities, and also to work with fields that are not algebraically closed.

Discussion

We stated Riemann's theorem and (finally!) defined Goppa codes. We also took a brief look at projective geometry - the geometry that corresponds to complete nonsingular curves.

At the end of the day, this course was about the basic language: Dedekind domains, dimension, nonsingular complete curves, valuations, function fields. To even define those we needed a fair amount of commutative algebra and some field theory.

If in the current course we learned the ABCs, the next course is poetry :) It will be less about basic algebraic machinery and more concrete work on curves over finite fields. The next course will have 4 main topics.

(1) Factorization in ring extensions

- Some beautiful Galois theory being employed including the study of "special" extensions such as Artin-Schreier extensions ($y^p - y = f(x)$) and Kummer extensions ($y^n = f(x)$).
- Commutative algebra - mostly using the going up / down theorems.
- Questions about ramification analogous to question in algebraic number theory, involving the study of traces, norms, resultants and discriminants.

(2) The Zeta function attached to a curve. Absolutely beautiful mathematics!

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

$$\zeta(s) = \sum_{I \neq 0} \frac{1}{|A/I|^s} = \prod_{M \in \mathrm{Max}(A)} \left(1 - \frac{1}{|A/M|^s}\right)^{-1}$$

If we let $b_d = |\{M \in \mathrm{Max}(A) \mid |A/M| = q^d\}|$ then

$$\zeta(T) = \prod_{d \in \mathbb{N}} \left(1 - T^d\right)^{b_d} = \frac{f(T)}{(1 - qT)(1 - T)}.$$

$$\zeta(T) = \prod_{d \in \mathbb{N}} \left(1 - T^d\right)^{b_d} = \frac{f(T)}{(1 - qT)(1 - T)}.$$

$$f(T) = \prod_{i=1}^{2g} (1 - \omega_i T)$$

Amazingly, Riemann hypothesis for curves over finite fields, proved by Weil in the 1940, states that

$$|\omega_i| = \sqrt{q}.$$

We will see the proof and much more.

(3) Constructions of curves with optimal ratio g/n These are super elegant constructions. For example: over $\mathbb{F}_8$

$$y^2 + y = x + 1 + \frac{1}{x}$$

$$z^2 + z = y + 1 + \frac{1}{y}$$

Or over every even prime power $q = \ell^2$

$$y^\ell + y = \frac{x^\ell}{x^{\ell-1} + 1}.$$

Another example

$$y^2 = \frac{x(x-1)}{x+1}.$$

(4) More applications as time permits

- List decodable codes
- Exponential sums and applications to explicit constructions.

It is going to be amazing! Be brave and register :)