# Summary

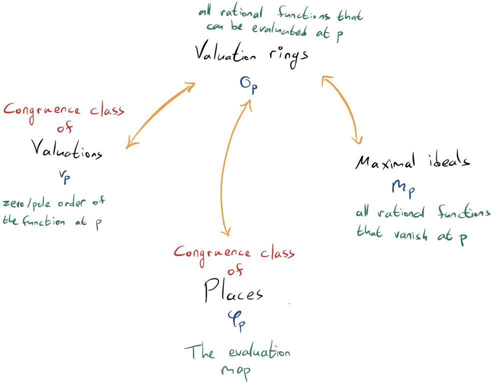
Gil Cohen

June 5, 2022

# Abstracting the notion of a point

In the course we studied algebraic function fields in one variable and codes that are based on them.

We first abstracted the notion of a point


all rational functions that can be evaluated at p
Valuation rings
$\mathcal{O}_P$
Congruence class of Valuations
$v_P$
zero/pole order of the function at p
Maximal ideals
$m_P$
all rational functions that vanish at p
Congruence class of Places
$\varphi_P$
The evaluation map

and called the thing we abstract a prime divisor, $\mathfrak{p}$.

# Summary - The genus and Riemann's Theorem

We then developed the theory of function fields, introducing the language of divisors and Riemann-Roch spaces so to ask the question:

> How many functions in the given function field have this many zeros here and at most that many poles there?

A divisor $\mathfrak{a}$ encoded the "input" to the question, and the answer was a vector space, the Riemann-Roch space $\mathcal{L}(\mathfrak{a})$. Its dimension was of interest, especially compared to $\deg \mathfrak{a}$.

Even partially answering this question, we discovered the genus of a function field, and proved Riemman's Theorem

$$\dim \mathfrak{a} \triangleq \dim \mathcal{L}(\mathfrak{a}) \geq \deg \mathfrak{a} - g + 1.$$

# Summary - Goppa codes

At this point we were at a position to understand Goppa's suggestion for codes based on function fields and saw the importance of the ratio

$$\frac{\mathsf{N}}{g} = \frac{\text{number of rational points}}{\text{genus}},$$

which we wanted to maximize for a given $q$. Indeed, Goppa codes satisfy

$$\rho + \delta \geq 1 - \frac{g-1}{\mathsf{N}}.$$

As we will see in the seminar part, the Drinfeld-Vladut bound states that

$$\frac{\mathsf{N}}{g} \leq \sqrt{q} - 1,$$

and so Goppa codes at best yield the guarantee

$$\rho + \delta \geq 1 - \frac{1}{\sqrt{q}-1}.$$

# Summary - $g$ vs. N

$$\rho + \delta \geq 1 - \frac{1}{\sqrt{q} - 1}.$$

If attainable (and attainable it is), this would be a significant improvement over the Gilbert-Varshamov bound (random codes) that "only" give

$$\rho + \delta = 1 - \Theta\left(\frac{1}{\log q}\right).$$

Our goal thus was to find function fields that attain the Drinfeld-Vladut bound.

This will be achieved by a carefully chosen sequence of function field extensions, and so we turned to study function field extensions.

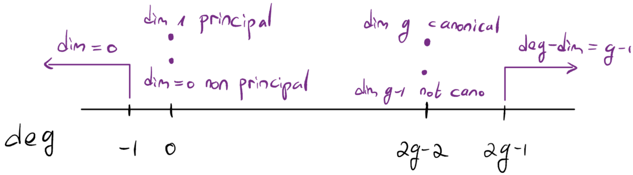
# Summary - The Riemann-Roch Theorem

Before study extensions, we proved the fundamental Riemann-Roch Theorem. To this end we introduced the notions of adeles, Weil differentials and canonical divisors. We proved that

$$\dim \mathfrak{a} = \deg \mathfrak{a} - g + 1 + \dim(\mathfrak{c} - \mathfrak{a})$$

for any canonical divisor $\mathfrak{c}$.

From Riemann-Roch we deduced



and the strong approximation theorem.

# Summary - Function field extensions

From this point on, we studied function field extensions F/L over E/K.

We understood the prime divisors lying above a prime divisor, in particular, the ramification index and the residual degree, and proved the fundamental equality

$$\forall \mathfrak{p} \in \mathbb{P}(\mathsf{E}) \qquad [\mathsf{F} : \mathsf{E}] = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}).$$

# Summary - Normal function field extensions

We then focused on Galois extensions in which one understands the extension via $G = \mathsf{Gal}(\mathsf{F}/\mathsf{E})$ (or $\mathsf{Gal}(\mathsf{E}_s/\mathsf{E})$ for normal extensions).

We proved that $G$ acts transitvily on $\{\mathfrak{P} \mid \mathfrak{P}/\mathfrak{p}\}$.

We defined the decomposition group $\mathcal{D}(\mathfrak{P}/\mathfrak{p})$ and inertia group $\mathrm{I}(\mathfrak{P}/\mathfrak{p})$, and proved that, assuming separability of everything,

$$e(\mathfrak{P}/\mathfrak{p}) = |\mathrm{I}(\mathfrak{P}/\mathfrak{p})| \qquad f(\mathfrak{P}/\mathfrak{p}) = \frac{|\mathcal{D}(\mathfrak{P}/\mathfrak{p})|}{|\mathrm{I}(\mathfrak{P}/\mathfrak{p})|}$$

These are two examples of the ramification groups that we will cover in the seminar.

# Summary - constant field extensions

We then studied constant field extensions which is required for the rest of the theory, in particular:

- For guaranteeing that the constant field does not grow in extensions by verifying a certain polynomial irreducibly condition.
- As we will see in the seminar, for the proof of the Hasse-Weil (and the Drinfeld-Vladut) bound.

We proved that essentially nothing changes in constant field extensions.

# Summary - integral closure and the complementary module

From this point we mostly wanted to understand how the genus behaves in an extension.

We started this by first learning about the integral closure of a ring, and proved that

$$\mathcal{O}'_{\mathfrak{p}} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}.$$

We defined the complementary module

$$\mathsf{C}_{\mathfrak{p}} = \{z \in \mathsf{F} \mid \mathsf{Tr}_{\mathsf{F}/\mathsf{E}}(z\mathcal{O}'_{\mathfrak{p}}) \subseteq \mathcal{O}_{\mathfrak{p}}\},$$

and proved that

$$\mathsf{C}_{\mathfrak{p}} = t_{\mathfrak{p}}\mathcal{O}'_{\mathfrak{p}}$$

for some $t_{\mathfrak{p}} \in \mathsf{F}$. The choice of $t$ is fully determined by $\{v_{\mathfrak{P}}(t) \mid \mathfrak{P}/\mathfrak{p}\}$.

# Summary - the Different

This led us to define the different exponent

$$d(\mathfrak{P}/\mathfrak{p}) = -v_{\mathfrak{P}}(t_{\mathfrak{p}}).$$

We proved that $t_{\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$-s. This in turn led us to define the different divisor

$$\mathsf{Diff}(\mathsf{F}/\mathsf{E}) = \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{E})} \sum_{\mathfrak{P}/\mathfrak{p}} d(\mathfrak{P}/\mathfrak{p})\mathfrak{P}.$$

We proved Dedekind Different Theorem which states that

$$d(\mathfrak{P}/\mathfrak{p}) \geq e(\mathfrak{P}/\mathfrak{p}) - 1,$$

with equality iff $\operatorname{char} \mathsf{K} \nmid e(\mathfrak{P}/\mathfrak{p})$.

This phenomena alerted us to distinguish between tame and wild extensions.

# Summary - Hurwitz Genus Formula

We gave the quite implicit definition of the co-trace

$$\begin{tikzcd}
\mathbb{A}_F \arrow[r, "\exists!\, \omega'"] \arrow[ddr, bend left, "\omega_2"] & L \arrow[dd, "\mathrm{Tr}_{L/k}"] \\
\mathbb{A}_{F/E} \arrow[d, "\mathrm{Tr}_{F/E}"'] \arrow[dr, "\omega_1"] & \\
\mathbb{A}_E \arrow[r, "\forall \omega"'] & K
\end{tikzcd}$$

and based on the co-trace and the Riemann-Roch Theorem, deduced the Hurwitz Genus Formula

$$2g_F - 2 = \frac{[F:E]}{[L:K]} \cdot (2g_E - 2) + \deg \mathrm{Diff}(F/E).$$

# Summary - Kummer's Theorem and more on the different

Starting to "descend" from the abstract to the more concrete, we proved Kummer's Theorem which gives an effective way of "finding" the prime divisors $\mathfrak{P}$ lying over $\mathfrak{p}$.

We also developed tools to compute the different by relating it to the valuation of a certain derivative. E.g., if $\mathsf{F} = \mathsf{E}(y)$ for a "nice" $y$ having minimal polynomial $\varphi$, then

$$d(\mathfrak{P}/\mathfrak{p}) = \upsilon_{\mathfrak{p}}(\varphi'(y)).$$

# Summary - Kummer extensions

Based on all we did, we were able to fully understand Kummer extensions

$$y^n = f(x),$$

with $(n, p) = 1$ and under some minimal conditions on $f$.

This includes our running-example

$$y^2 = x^3 - x$$

which we fully analyzed, as well as the better choice

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

# Summary - Towers of function fields

We gave a systematic way of studying function fields that are defined by a sequence of extensions, in particular recursive towers.

We defined the limit of a tower

$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{n_i}{g_i},$$

and defined the notion of bad ($\lambda = 0$), good ($\lambda > 0$), and optimal ($\lambda = \sqrt{q} - 1$) towers over $\mathbb{F}_q$.

For computing $\lambda(\mathcal{F})$, the key objects are the splitting and ramification loci.

The first example we saw for an optimal tower (though the proof is per field) is given by the recursive tower with the defining equation

$$Y^2 = \frac{X^2 + 1}{2X}.$$

# Summary - Artin-Schreier type extensions

We then turned to consider cyclic extensions with degree that is divisible by the characteristic, namely, Artin-Schreier and AS-type extensions.

We analyzed the Hermitian tower

$$Y^q + Y = X^{q+1},$$

over $\mathbb{F}_{q^2}$, and the celebrated Garcia-Stichtenoth tower

$$Y^q - Y = \frac{X^q}{1 - X^{q-1}},$$

over $\mathbb{F}_{q^2}$ which we proved is optimal, modulo the assertion

$$d(\mathfrak{P}/\mathfrak{p}) = 2 \cdot (e(\mathfrak{P}/\mathfrak{p}) - 1)$$

which we will prove in the seminar part using the ramification groups.

# Summary

Thank you for taking the course!

I hope you appreciate and enjoy this beautiful mathematics as much as I do, and that you'll find it useful in your research.

Special thanks to Shir Peleg for doing an optimal job "TA-ing" the course.