ON LOCAL FUNCTION FIELDS RELATED TO $\mathbb{Q}_p$ AND $\mathbb{Z}_p$

AASHIR MEHROTRA

1. Body

We start with the definitions of the local function ring:

Definition 1.1. Let $\mathbb{F}_p$ be the unique finite field with p elements (which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Then the symbol $\mathbb{F}_p[[x]]$ represents the ring of formal power series in the variable x, with coefficients in $\mathbb{F}_p$. The

We thus have elements of the form

$$\sum_{i=0}^{\infty} \overline{a_i} x^i$$

where $\overline{a_i} \in \mathbb{F}_p$.
We are aware of the fact that every element in $\mathbb{Z}_p$ can be expressed as a power series of the form:

$$\sum_{i=0}^{\infty} a_i p^i$$

Where $a_i \in \{0, 1, 2, \ldots, p-1\}$
We can think creating a canonical map from $\mathbb{F}_p[[x]]$ to $\mathbb{Z}_p$ by send x to p. However, such a map wouldn't be a ring homomorphism as both these fields have different characteristics.
Another reason why a homomorphism doesn't work out is that in $\mathbb{F}_p[[x]]$ doesn't "carry over", whereas $\mathbb{Z}_p$ does.
The field of fractions for $\mathbb{F}_p[[x]]$ is the field of all **Laurent series** in $\mathbb{F}_p$ (denoted as $\mathbb{F}_p((x))$).
This means that we have elements of the form (where $\overline{a_i} \in \mathbb{F}_p$, and k is an integer):

$$\sum_{i=k}^{\infty} \overline{a_i} x^i$$

This field is also closely related to p-adic numbers, it has a similar representation to $\mathbb{Q}_p$.
However, this also does not turn into a homomorphism of fields.
In fact, there exists no homomorphism between $\mathbb{F}_p[x]$ (the polynomial ring) and $\mathbb{Z}_p$, this is again due to the carrying over property $\mathbb{Z}_p$ has.

Date: August 13, 2022.

We now define the notion of a valuation ring and a discrete valuation ring:

Definition 1.2. An integral domain D is a **valuation ring** if in it's field of fractions K, we must have either $x \in D$ or $x^{-1} \in D$ for every $x \in K$.

It turns out that for every valuation ring, we can assign it a valuation:

Theorem 1.3. *Let D be an integral domain. Then D is a valuation ring if and only if there exists a totally ordered abelian group Γ (called the* ***value group****) and a* ***valuation*** *$v : K \longrightarrow \Gamma \cup \{\infty\}$ such that D is set of x for which $v(x)$ is ≥ 0.*

Recall the definition of a valuation:

Definition 1.4. A **valuation** on a a field K is a totally ordered abelian group Γ and a function $v : K \longrightarrow \Gamma$ that satisfies the following properties for every x and y in K:

- $v(x) = \infty \iff x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min\{v(x), v(y)\}$

We first make a remark on how to adjoin ∞ to Γ. We let $\gamma + \infty = \infty$ for all $\gamma \in \Gamma \cup \{\infty\}$. Also make ∞ the unique maximal element of Γ, meaning that $\infty > \gamma$ for all $\gamma \in \Gamma$.
Let's see some examples and non-examples of valuation rings:
$\mathbb{Z}$ is not a valuation ring. This is because we can consider elements like $\frac{2}{3} \in \mathbb{Q}$, where neither $\frac{2}{3}$ nor $\frac{3}{2}$ are integers.
To extend $\mathbb{Z}$ to a valuation ring, we pick a prime p and construct the field $\mathbb{Z}_{(p)}$ (called the **localization** of $\mathbb{Z}$ with respect to p).
Elements of $\mathbb{Z}_{(p)}$ is the subset of all rational numbers whose denominator in its irreducible form is not divisible by p.
For example, $\frac{31}{4} \in \mathbb{Z}_{(3)}$ but $\frac{49}{18} \notin \mathbb{Z}_{(3)}$ as 18 is divisible by 3.

$\mathbb{Z}_p$ is also a valuation ring. We can prove this using the power series representation, but it's easier to use absolute values. If $x \in \mathbb{Q}_p$, then either $|x| \leq 1$ or $|x| > 1$.
In the former case, we have $x \in \mathbb{Z}_p$ by definition. In the latter case, we have that $|x^{-1}| = |x|^{-1} < 1$, making x^{-1} an element of $\mathbb{Z}_p$.
Let's now define the notion of a discrete value ring:

Definition 1.5. A valuation ring D is a **discrete valuation ring** when $\Gamma = \mathbb{Z}$ (the additive group of integers).

A discrete valuation can give rise to an absolute value in K, and hence a metric in K. This can be done by taking an arbitrary $\alpha \in \mathbb{R}_{>1}$, and consider the absolute value given by:

$$|x| = \alpha^{-v(x)}$$

for every $x \in K$. Note that $\alpha^{-\infty} = 0$.
Such an absolute value satisfies not only the triangle inequality, but also the ultrametric inequality, making the metric given by $d(x, y) = |x - y|$ an ultrametric.
Why not denote the absolute value as $|\cdot|_\alpha$? This is because all such absolute values are **equivalent**, as they generate the same open sets.

We'll now define a discrete valuation on $\mathbb{F}_p((x))$.
The definition is simple: take the smallest power with a non-zero coefficient. For example, if we have the Laurent series $f = \sum_{i=-3}^{\infty}(i + 3)x^i$, then $v(f) = -2$.
This definition cannot be applied to the 0 Laurent series, hence just let $v(x) = \infty$.

Claim 1.6. *The absolute value defined above is a discrete valuation*

Proof of Claim: 1.6. It's impossible not to find a smallest power with a non-zero absolute value coefficient, unless $f = 0$. Hence the only time $v(f) = \infty$ is when $f = 0$.
Consider two Laurent series f and g. The smallest non-zero term of its product fg will be the the sum of the non-zero terms of f and g.
When f or $g = 0$, then fg has valuation ∞, and $v(f) + v(g) = \infty + c = \infty$ (for some $c \in \mathbb{Z} \cup \{\infty\}$).
Hence, we have that $v(fg) = v(f) + v(g)$.
Lastly, we observe that when we add f and g, we cannot get a smaller valuation than the minimum degree of both f and g, as all coefficients before the minimum of f and g's smallest degrees is 0.
Hence, we must get that $v(f + g) \geq \min\{v(f), v(g)\}$, which means that v is a discrete valuation. ∎

Before we proceed, let's define the discrete valuation ring, with respect to a discrete valuation on K.

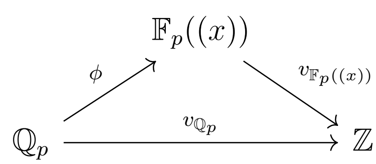
Definition 1.7. Let K be a field with discrete valuation K. Then the discrete valuation ring with respect to K is:

$$\mathcal{O}_K = \{x \in K | v(x) \geq 0\}$$

For example, we have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}_{(p)}$ when we use the valuation v_p from number theory on $\mathbb{Q}$. Also, it's obvious from the definitions that $\mathcal{O}_{\mathbb{F}_p((x))} = \mathbb{F}_p[[x]]$ (as all power series have smallest non-zero coefficient at least zero).
Now that we have a discrete valuation on $\mathbb{Z}_p[[x]]$, we can create an absolute value and hence a metric on it.
Since we have a "special" number associated with the ring that is greater than 1 (namely p), we can let $\alpha = p$ (it doesn't really matter as all such metrics are equivalent anyway).
I claim that we can construct a **homeomorphism** to $\mathbb{Z}_p$ from $\mathbb{F}_p[[x]]$ (similarly to $\mathbb{Q}_p$ from $\mathbb{F}_p((x))$).

Proof. We actually construct an isometry between the two spaces (meaning that the map preserves distances).
Isometries are always continuous, just take $\delta = \epsilon$ in the definition.
We'll actually use the canonical map described in the first page.
Actually such a map preserves valuations, as the valuation for $\mathbb{Z}_p$ using the power series is form has the exact same definition as the one for the formal power series in $\mathbb{F}_p$.
Hence, we've shown that $\mathbb{Z}_p$ and $\mathbb{F}_p[[x]]$ are homeomorphic to each other.
A similar proof shows that $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$ are homeomorphic to one another. ■

We can create the following commutative diagram now:



where ϕ is the homeomorphism described above.
Let us also discuss about local fields.

Definition 1.8. A topological space X in **locally compact** if every point $x \in X$ has a compact neighbourhood in X.

$\mathbb{Q}$ is not locally compact, as every neighbourhood contains a Cauchy sequence converging to an irrational number. Hence it's not complete, and hence not compact.

Definition 1.9. A topological field K with a non-discrete topology is a ⋖⋊⅁⋖℧⊐⋖ if it is locally compact as a topological space.

As mentioned before, $\mathbb{Q}$ is not a local field.
Note that all topologies that are discrete are locally compact, as one can take a single point set as the neighbourhood.
This space is complete (as the only Cauchy sequences are constant, which always converge).
This space is also totally bounded, as you can just the singleton set as the finite collection of open sets of constant radius to cover the neighbourhood.

Theorem 1.10. *Let K be a local field. Then is K is isomorphic to one of the following:*

- $\mathbb{R}$
- $\mathbb{C}$
- *Finite extensions of $\mathbb{Q}_p$ for any prime p*
- *$\mathbb{F}_q((x))$ for some prime power q.*

2. Bibliography

References

[1] Michael Atiyah. *Introduction to commutative algebra*. CRC Press, 2018.
[2] Alain M Robert. *A course in p-adic analysis*, volume 198. Springer Science & Business Media, 2013.

[1]
[2]