

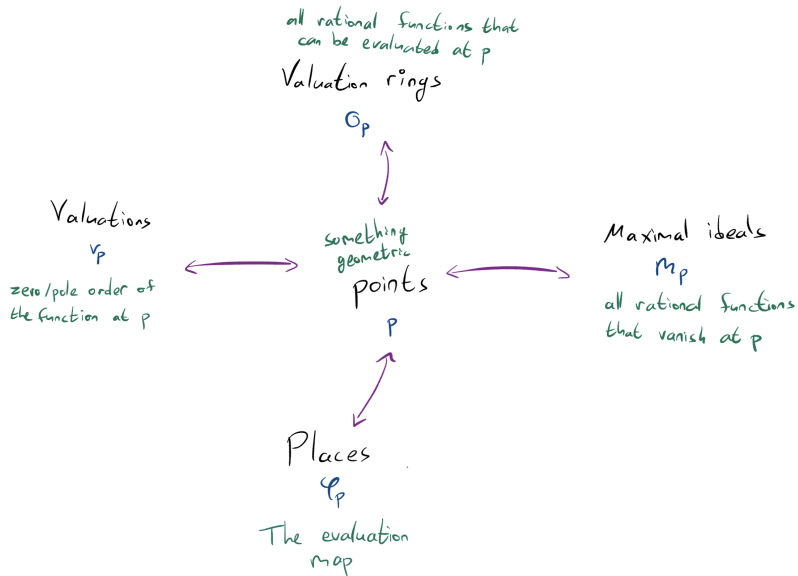
# Valuations

## Unit 4

Gil Cohen

October 30, 2024

# Recall



# Overview

- 1 Valuations
- 2 Examples
- 3 Valuations and absolute values
- 4 Basic properties of valuations
- 5 Discrete valuations
- 6 Example
- 7 Equivalent valuations

## Definition 1 (Valuations)

A **valuation** on a field  $F$  is map  $v : F^\times \rightarrow \Gamma$ , where  $\Gamma$  is an ordered group, satisfying

- 1 additivity:  $v(ab) = v(a) + v(b)$ . That is,  $v$  is a group homomorphism from the multiplicative group of  $F$  to  $\Gamma$ .
- 2 triangle inequality:  $v(a + b) \geq \min(v(a), v(b))$ ,

assuming  $a, b, a + b \in F^\times$ .

It is convenient to extend the definition to  $v : F \rightarrow \Gamma \cup \{\infty\}$  by setting

$$v(a) = \infty \iff a = 0.$$

Doing so, we do not have to assume anything about  $a, b, a + b$  as  $\infty > \Gamma$ .

# Overview

- 1 Valuations
- 2 Examples**
- 3 Valuations and absolute values
- 4 Basic properties of valuations
- 5 Discrete valuations
- 6 Example
- 7 Equivalent valuations

# $p$ -adic valuations of $\mathbb{Q}$

A trivial example for a valuation is given by the **trivial valuation**  $v : F^\times \rightarrow \{0\}$ . Let's look at more interesting examples.

Let  $p \in \mathbb{N}$  be a prime. We define

$$v_p : \mathbb{Q}^\times \rightarrow \mathbb{Z}$$

as follows. Given  $q \in \mathbb{Q}^\times$ , write

$$q = p^n \cdot \frac{a}{b}$$

with  $a, b \in \mathbb{Z} \setminus \{0\}$  are coprime to  $p$ . As  $\mathbb{Z}$  is UFD,  $n$  is unique. We define the  **$p$ -adic valuation** by

$$v_p(q) = n.$$

**Exercise.** What is  $v_3\left(\frac{5}{9}\right)$ ?

# $p(x)$ -adic valuations of $K(x)$

Let  $K$  be a field and  $p(x) \in K[x]$  irreducible. We define

$$v_{p(x)} : K(x)^\times \rightarrow \mathbb{Z}$$

as follows. Let  $q(x) \in K(x)^\times$ . Write

$$q(x) = p(x)^n \cdot \frac{a(x)}{b(x)}$$

with  $a(x), b(x) \in K[x] \setminus \{0\}$  and  $a(x), b(x)$  coprime to  $p(x)$ .

By the UFD-ness of  $K[x]$ ,  $n$  is unique. We define the  $p(x)$ -adic valuation by

$$v_{p(x)}(q(x)) = v_p(q) = n.$$

If  $p(x)$  is of the form  $p(x) = x - \alpha$  for some  $\alpha \in K$ , and  $q(x) \in K(x)^\times$  then  $v_p(q) = v_{x-\alpha}(q)$  is the multiplicity of  $\alpha$  as a root or pole of  $q$ . We sometimes write  $v_\alpha$  for short.

# Overview

- 1 Valuations
- 2 Examples
- 3 Valuations and absolute values**
- 4 Basic properties of valuations
- 5 Discrete valuations
- 6 Example
- 7 Equivalent valuations



# Valuations and absolute values

Let  $v : F \rightarrow \Gamma \cup \{\infty\}$  a valuation and assume  $\Gamma \triangleleft \mathbb{R}$ . For  $a \in F^\times$  define

$$|a| = 2^{-v(a)}.$$

Informally, “ $2^{-v(0)} = 2^{-\infty} = 0$ ”, and so we extend  $|\cdot|$  to  $F$  by setting  $|0| = 0$ . We have that

$$|ab| = 2^{-v(ab)} = 2^{-(v(a)+v(b))} = 2^{-v(a)}2^{-v(b)} = |a||b|.$$

Further, by the triangle inequality,

$$|a+b| = 2^{-v(a+b)} \leq 2^{-\min(v(a),v(b))} = \max(2^{-v(a)}, 2^{-v(b)}) = \max(|a|, |b|),$$

and so

$$|a + b| \leq \max(|a|, |b|) \leq |a| + |b|.$$

# Valuations and absolute values

Therefore, a valuation gives rise to an absolute value. In fact, it yields a stronger notion called a **non-Archimedean absolute value**: not only is

$$|a + b| \leq |a| + |b|$$

but also

$$|a + b| \leq \max(|a|, |b|).$$

Otherwise, an absolute value is called **Archimedean**.

We think of a valuation as measuring closeness. It is instructive and productive to study the topology induced by the valuation but in this course we will not proceed in this direction.

Several results establish that “close” polynomials have similar properties. E.g., if  $f(x)$  is separable and irreducible then so is any sufficiently close  $g(x)$ .

# Overview

- 1 Valuations
- 2 Examples
- 3 Valuations and absolute values
- 4 Basic properties of valuations**
- 5 Discrete valuations
- 6 Example
- 7 Equivalent valuations

## Claim 2

Let  $v : F \rightarrow \Gamma \cup \{\infty\}$  be a valuation. Then,

- 1  $v(1) = 0$
- 2  $v(a) = v(-a)$ . In particular,  $v(-1) = 0$ .
- 3  $v(a^{-1}) = -v(a)$ .
- 4 If  $v(a) \neq v(b)$  then

$$v(a + b) = \min(v(a), v(b)).$$

- 5  $v(\sum_i a_i) \geq \min(v(a_i))$ .
- 6 If  $\sum_{i=1}^n a_i = 0$  and  $n > 1$  then  $\exists i \neq j$  with  $v(a_i) = v(a_j)$ .

# Basic properties of valuations

The proof of the claim is straightforward and is left as an exercise. We only prove (4)—the **strict triangle inequality**.

Proof.

Assume  $v(a) < v(b)$ . We know that  $v(a + b) \geq v(a)$  by the triangle inequality but we wish to prove that  $v(a + b) = v(a)$ . Now,

$$\begin{aligned}v(a) &= v(a + b - b) \\ &\geq \min(v(a + b), v(-b)) \\ &= \min(v(a + b), v(b)).\end{aligned}$$

Hence, if  $v(a + b) > v(a)$  we would get  $v(a) > v(a)$ . □

# Basic properties of valuations

## Claim 3

Let  $R$  be a domain and  $\Gamma$  an ordered group. Assume  $v : R \rightarrow \Gamma \cup \{\infty\}$  satisfies

- 1  $v(ab) = v(a) + v(b)$ ,
- 2  $v(a + b) \geq \min(v(a), v(b))$ ,
- 3  $v(a) = \infty \iff a = 0$

for all  $a, b \in R$ . Then  $v$  can be extended to a valuation in a unique way to  $\text{Frac } R$ .

## Proof sketch.

For  $a \in R$ , the value of  $v(a^{-1})$  is determined as  $v(a^{-1}) = -v(a)$ . Thus, the only possible extension of  $v$  would map  $\frac{a}{b}$  to  $v(a) - v(b)$ . It is left to show that this is indeed a valuation.

# Overview

- 1 Valuations
- 2 Examples
- 3 Valuations and absolute values
- 4 Basic properties of valuations
- 5 Discrete valuations**
- 6 Example
- 7 Equivalent valuations

# Discrete valuations

Observe that if  $v : F^\times \rightarrow \Gamma$  is a valuation then  $v(F^\times)$  is an ordered subgroup of  $\Gamma$ . Thus, sometimes one replaces  $\Gamma$  with  $v(F^\times)$ . This allows us to assume essentially wlog that  $v$  is onto.

## Definition 4 (Discrete valuations)

When  $v(F^\times) \cong \mathbb{Z}$  we say that  $v$  is a **discrete** valuation.

By the above remark, we sometimes “normalize” a nontrivial discrete valuation so that  $v(F^\times) = \mathbb{Z}$ .



# Overview

- 1 Valuations
- 2 Examples
- 3 Valuations and absolute values
- 4 Basic properties of valuations
- 5 Discrete valuations
- 6 Example**
- 7 Equivalent valuations

# Some facts from Ring Theory

We recall the following basic definitions from ring theory.

## Definition 5 (Units)

Let  $R$  be a domain. An element  $a \in R$  is called a **unit** if  $a$  has an inverse in  $R$ , namely,

$$\exists b \in R \quad ab = ba = 1.$$

The set of units of  $R$  is denoted by  $R^\times$ . Note that  $R^\times$  is a group under multiplication and is referred to as the **unit group** of  $R$ .

## Definition 6 (Irreducible elements)

Let  $R$  be a domain. A non-zero non-unit element  $a \in R$  is **irreducible** if whenever  $a = bc$  then  $b$  or  $c$  is a unit.

## Definition 7 (Prime elements)

Let  $R$  be a domain. A non-zero non-unit element  $a \in R$  is **prime** if whenever  $a \mid bc$  then  $a \mid b$  or  $a \mid c$ .

# Some facts from Ring Theory

We recall that every prime is irreducible.

One can show (excluding the annoying  $a = 0$  case) that

$$\begin{aligned} a \in R \text{ is prime} &\iff \langle a \rangle \text{ is a prime ideal} \\ &\iff R/\langle a \rangle \text{ is a domain.} \end{aligned}$$

Perhaps slightly less known (yet trivial) is the equivalence

$$a \in R \text{ is irreducible} \iff \langle a \rangle \text{ is maximal amongst principal ideals.}$$

# Some facts from Ring Theory

As mentioned, a prime element is always irreducible. The converse holds in UFD. Thus, in a UFD

$$a \in R \text{ is irreducible} \iff R/\langle a \rangle \text{ is a domain.}$$

You may have seen that

$$R \text{ is a UFD} \implies R[x] \text{ is a UFD.}$$

Let  $K$  be a field.  $K[x]$  is a UFD (it is in fact a Euclidean domain  $\implies$  PID  $\implies$  UFD). Thus, so is  $K[x, y]$ .

We can thus conclude that

$$K[x, y]/\langle f(x, y) \rangle \text{ is a domain} \iff f(x, y) \text{ is irreducible.}$$

# Example

Let  $K$  be a field. Let

$$f(x, y) = y^2 - x^3 + x \in K[x, y],$$

and consider the curve

$$Z_f = \{(x, y) \in K \times K \mid f(x, y) = 0\}.$$

$f(x, y)$  is irreducible as otherwise  $\exists g(x) \in K[x]$  s.t.

$$f(x, y) = (y - g(x))(y + g(x)).$$

But then  $g(x)^2 = x^3 - x$  which is impossible by degree considerations.  
Thus,

$$C_f = K[x, y] / \langle f(x, y) \rangle$$

is a domain. We denote its fraction field by  $K_f$ .

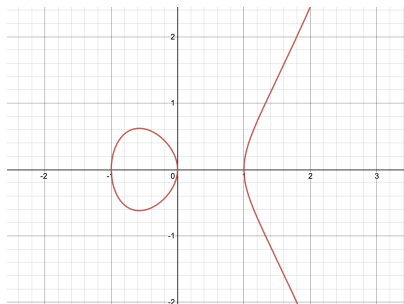
# Example

The point  $o = (0, 0)$  is on the curve  $Z_f$  as  $f(0, 0) = 0$ . Therefore, we may try to find a valuation  $v_o : K_f \rightarrow \mathbb{Z} \cup \{\infty\}$ .

We abuse notation and write  $x, y$  also for the projections of  $x, y$  via the map

$$K[x, y] \rightarrow C_f = K[x, y] / \langle y^2 - x^3 + x \rangle.$$

We do not yet have the tools to prove it, but trust me that such  $v_o$  exists with  $v_o(x) = 2$ .



# Example

Let's see what we can make of it. As  $y^2 = x^3 - x$  in  $C_f$ ,

$$v_o(y^2) = v_o(x^3 - x).$$

I promised you that  $v_o(x) = 2$ , and so

$$v_o(x^3) = 3v_o(x) = 6.$$

Thus, by the strict triangle inequality,

$$v_o(x^3 - x) = \min(v_o(x^3), v_o(x)) = 2.$$

Thus,

$$2v_o(y) = v_o(y^2) = 2,$$

and so we conclude that  $v_o(y) = 1$ .

# Example

As  $y^2 = x^3 - x$  in  $C_f$ , every element of  $K_f = \text{Frac } C_f$  can be written in the form

$$\frac{a(x) + b(x)y}{c(x) + d(x)y}$$

with  $a(t), b(t), c(t), d(t) \in K[t]$  and with the understanding that  $x, y$  are the images in  $C_f$  as discussed above. We can further simplify

$$\frac{a(x) + b(x)y}{c(x) + d(x)y} = \frac{a(x) + b(x)y}{c(x) + d(x)y} \cdot \frac{c(x) - d(x)y}{c(x) - d(x)y} = A(x) + B(x)y,$$

where  $A(t), B(t) \in K(t)$ .

To summarize, every element in  $K_f$  is of the form

$$A(x) + B(x)y$$

with  $A(t), B(t) \in K(t)$ .



## Example

Since  $v_o(y) = 1$ ,

$$v_o(A(x) + B(x)y) \geq \min(v_o(A(x)), 1 + v_o(B(x))).$$

Assume now further that  $K$  is a finite field,  $K = \mathbb{F}_q$ . Then,  $v_o(z) = 0$  for every  $z \in K^\times$ . Indeed, we have that  $z^q = z$  for every  $z \in K$ , and so

$$v_o(z) = v_o(z^q) = qv_o(z) \implies v_o(z) = 0.$$

As  $v_o(x) = 2$ , we get by the strict triangle inequality that  $v_o(g(x))$  is even for every  $g(x) \in K[x]$ . Indeed,

$$v_o(x^i) = iv_o(x) = 2i.$$

Thus, if  $g(x) = \sum_{i=0}^d a_i x^i$ , then

$$v_o(g(x)) = 2j$$

where  $j$  is the least integer such that  $a_j \neq 0$ .

# Example

Thus,  $v_o(g(x))$  is even for every  $g(x) \in K(x)$ . Now, recall that

$$v_o(A(x) + B(x)y) \geq \min(v_o(A(x)), 1 + v_o(B(x))).$$

As  $v_o(A(x)), v_o(B(x))$  are even, and since  $v_o(y) = 1$  we get, by the strict triangle inequality that

$$v_o(A(x) + B(x)y) = \min(v_o(A(x)), 1 + v_o(B(x))).$$

Some random examples include

$$v_o\left(\frac{1}{x} + y\right) = \min(-2, 1) = -2,$$

and

$$v_o(y^2 - x) = v_o(x^3 - 2x) = \min(6, 2) = 2.$$

# Example

Consider the function  $\frac{x}{y} \in C_f$ . Is it defined at  $(0,0)$ ?

Using valuations, we see that

$$v_o\left(\frac{x}{y}\right) = v_o(x) - v_o(y) = 2 - 1 = 1,$$

and so  $\frac{x}{y}$  is not only defined but also vanishes at  $(0,0)$ .

To see it in a different way, recall that  $y^2 = x^3 - x$  in  $C_f$  and so

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

Thus, using this representation it is easier to see that at  $(0,0)$  the function  $\frac{x}{y}$  evaluates to 0.

# Example

Some recommended exercises:

**Exercise.** Prove that  $C_f$  is not a UFD. Hint:

$$y^2 = x^3 - x = x(x-1)(x+1).$$

**Exercise.** Recall that  $K_f = \text{Frac } C_f$ , where

$$C_f = \mathbb{K}[x, y] / \langle y^2 - x^3 + x \rangle.$$

Prove that

$$K_f \cong \mathbb{K}(x)[y] / \langle y^2 - x^3 + x \rangle.$$

# Overview

- 1 Valuations
- 2 Examples
- 3 Valuations and absolute values
- 4 Basic properties of valuations
- 5 Discrete valuations
- 6 Example
- 7 Equivalent valuations**

# Equivalent valuations

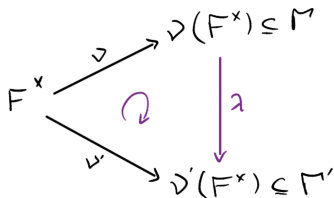
## Definition 8

Two valuations  $v : F^\times \rightarrow \Gamma, v' : F^\times \rightarrow \Gamma'$  are **equivalent** if

$$\forall a \in F^\times \quad v(a) \geq 0_\Gamma \iff v'(a) \geq 0_{\Gamma'}.$$

## Claim 9

$v, v'$  are equivalent  $\iff \exists$  an order-preserving group isomorphism  $\lambda : v(F^\times) \rightarrow v'(F^\times)$  s.t.  $v' = \lambda \circ v$ .



# Equivalent valuations

Proof.

For the nontrivial direction, as  $v, v'$  are equivalent,

$$v(a) = 0 \iff v'(a) = 0.$$

Indeed, assume  $v(a) = 0$ . Then, in particular,

$$v(a) \geq 0 \implies v'(a) \geq 0.$$

Moreover,  $v(a^{-1}) = -v(a) = 0 \geq 0$  and so  $v'(a^{-1}) \geq 0$ , implying  $v'(a) \leq 0$ . Overall then,  $v'(a) = 0$ .

Therefore,  $\ker v = \ker v'$ , and so by the first isomorphism theorem for groups,

$$v(F^\times) \cong F^\times / \ker v = F^\times / \ker v' \cong v'(F^\times).$$

This then induces a group isomorphism  $\lambda : v(F^\times) \rightarrow v'(F^\times)$ , and I leave it for you to show it is order preserving. □