

WORKSHEET 2.3: VALUATION RINGS

Fix a field \mathbb{K} . In this worksheet we will explore a special, but important type of rings called valuation rings.

Definition 1. A *valuation ring* of a field \mathbb{K} is a subring $R \subset \mathbb{K}$ with the property that for all $x \in \mathbb{K}^\times$ either $x \in R$ or $x^{-1} \in R$.

Note that, since a valuation ring R of a field \mathbb{K} is a subring of \mathbb{K} it is necessarily a domain. We first study valuation rings directly, then show how certain functions that broadly measure some notion of divisibility, called valuations, produce them. Lastly, we compare discrete and non-discrete examples.

(1) **Examples of Valuation Rings.** Recall $\mathbb{C}(x, y)$ is the field of formal rational functions in x and y , which concretely is the set of elements f/g where $f, g \in \mathbb{C}[x, y]$ with $g \neq 0$. For each of the following subsets $\mathcal{S} \subset \mathbb{C}(x, y)$ determine whether or not they are valuation rings by showing whether for every $h \in \mathbb{C}(x, y)^\times$ either $h \in \mathcal{S}$ or $h^{-1} \in \mathcal{S}$.

(a) Hint: Use that $\mathbb{C}[x, y]$ is a UFD to understand when g is divisible by y .

$$\mathcal{S}_1 := \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[x, y] \text{ and } g \notin \langle y \rangle \right\}$$

(b) Hint: Consider the element $\frac{x}{y}$.

$$\mathcal{S}_2 := \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[x, y] \text{ and } g(0, 0) \neq 0 \right\}$$

(c) Define the *order* of a non-zero polynomial $f \in \mathbb{C}[x, y]$ to be $\text{ord}(f)$, the lowest degree of a monomial in f and $\text{ord}(0) = \infty$.

$$\mathcal{S}_3 := \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[x, y], g \neq 0, \text{ and } \text{ord}(f) \geq \text{ord}(g) \right\}$$

(2) **Ideals in Valuation Rings.** Let R be a valuation ring of \mathbb{K} .

(a) Show that for any two non-zero elements $x, y \in R$, either $x|y$ or $y|x$.

(b) Show that every finitely generated ideal of R is principal.

(c) Prove that the ideals of R form a totally ordered set. That is, for any two ideals I, J in R , either $I \subseteq J$ or $J \subseteq I$. (Hint: Given $x \in I$ with $x \notin J$ consider whether an element $y \in J$ can divide x .)

(d) What does the previous parts say about the poset structure on $\text{Spec}(R)$?

(3) **Local Rings & Valuation Rings.** An arbitrary ring R is said to be a *local ring* if it has exactly one maximal ideal. We often write a local ring R as a pair (R, \mathfrak{m}) where $\mathfrak{m} \subset R$ is the unique maximal ideal.

- (a) Describe $\mathfrak{m}\text{Spec}(R)$ if R is a local ring.
- (b) Describe the closed points of $\text{Spec}(R)$ if R is a local ring.
- (c) Prove that a valuation ring is a local ring.

(4) **p -Adic Integers.** Fix a prime p . The p -adic numbers \mathbb{Q}_p are the completion of \mathbb{Q} with respect to the p -adic absolute value $|\cdot|_p$, defined as follows: for a nonzero rational number x , write $x = p^k \frac{a}{b}$ where $a, b \in \mathbb{Z}$ are not divisible by p . Then

$$|x|_p = p^{-k}, \quad |0|_p = 0.$$

Note $|\cdot|_p$ extends uniquely to \mathbb{Q}_p . The p -adic integers are defined by

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Similar to decimal expansion in \mathbb{R} , it is a fact that every element $x \in \mathbb{Q}_p$ can be written uniquely as a formal series

$$x = \sum_{i=k}^{\infty} a_i p^i \quad \text{where} \quad a_i \in \{0, 1, \dots, p-1\}, \quad a_k \neq 0,$$

and that

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, \dots, p-1\} \right\}.$$

- (a) Prove that the p -adic absolute value is well-defined. (Hint: Use the fact that \mathbb{Z} is a UFD to show that every element $x \in \mathbb{Q}$ can be written uniquely (up to sign and reordering) as $p_1^{a_1} \dots p_t^{a_t}$ where the p_i are distinct primes and $a_i \in \mathbb{Z}$.)
- (b) Prove the p -adic absolute value satisfies the *non-Archimedean (ultrametric) inequality*:

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

- (c) Prove the p -adic absolute value is multiplicative: $|xy|_p = |x|_p |y|_p$.
- (d) Use parts 4b and 4c to show that \mathbb{Z}_p is closed under addition and multiplication.
- (e) Conclude that \mathbb{Z}_p is a ring (called the ring of p -adic integers).
- (f) Prove that \mathbb{Z}_p is a valuation ring.

The previous exercises suggest why valuation rings are called *valuation* rings: they arise from functions that measure divisibility, generalizing the p -adic absolute value. Such functions are called valuations. An *ordered abelian group* is an abelian group $(\Gamma, +)$ together with a total order $<$ on Γ that is compatible with addition, in the sense that if $\alpha < \beta$ then $\alpha + \gamma < \beta + \gamma$ for all $\alpha, \beta, \gamma \in \Gamma$. We will frequently extend the

total ordering on an ordered abelian group Γ to $\Gamma \cup \{\infty\}$ by making the convention that $\gamma < \infty$ for all $\gamma \in \Gamma$. Similarly, we will extend addition to $\Gamma \cup \{\infty\}$ by declaring $\infty + \gamma = \gamma + \infty = \infty$ for all $\gamma \in \Gamma$.

Definition 2. Let $(\Gamma, +, <)$ be an ordered abelian group. A Γ -valued valuation, or just a valuation, on \mathbb{K} is a function: $v : \mathbb{K} \rightarrow \Gamma \cup \{\infty\}$, which satisfies the following axioms for all $x, y \in \mathbb{K}$:

- (i) $v(xy) = v(x) + v(y)$
- (ii) $v(x + y) \geq \min\{v(x), v(y)\}$, and
- (iii) $v(x) = \infty$ if and only if $x = 0$.

Note that this means v defines a group homomorphism $v : \mathbb{K}^\times \rightarrow \Gamma$. Indeed, it is standard to define a valuation as a group homomorphism $v : \mathbb{K}^\times \rightarrow \Gamma$ satisfying axiom (ii), and then extend it to all of \mathbb{K} by setting $v(0) = \infty$. This convention is implicit throughout the remainder of the worksheet.

The *value group* of a valuation $v : \mathbb{K}^\times \rightarrow \Gamma$ is the image of v . A valuation is a *discrete valuation* if its value group is isomorphic to \mathbb{Z} . If $\mathbb{F} \subset \mathbb{K}$ is a subfield, we say that v is a \mathbb{F} -valuation if $v(\lambda) = 0$ for all $\lambda \in \mathbb{F}^\times$.

(5) **Examples of Valuations.** Prove that the following are valuations.

(a) The p -adic valuation:

$$v_p : \mathbb{Q}^\times \rightarrow \mathbb{Z}, \quad v_p\left(p^k \frac{a}{b}\right) = k$$

where $a, b \in \mathbb{Z}$ are not divisible by p .

(b) The order valuation on $\mathbb{C}(x)$:

$$v_0 : \mathbb{C}(x)^\times \rightarrow \mathbb{Z}, \quad v_0(f/g) = \text{ord}_{x=0}(f) - \text{ord}_{x=0}(g).$$

(c) More generally, if $a \in \mathbb{C}$, define

$$v_a : \mathbb{C}(x)^\times \rightarrow \mathbb{Z}$$

by order of vanishing at $x = a$. Show this is again a valuation.

(d) On $\mathbb{C}(x, y)$, define

$$v(f/g) = \text{ord}(f) - \text{ord}(g),$$

where $\text{ord}(h)$ is the degree of the lowest-degree nonzero term of $h \in \mathbb{C}[x, y]$. Show that this is a valuation with value group \mathbb{Z} .

(6) Prove that every ordered abelian group is torsion-free. (Hint: Reduce to the case when $x > 0$.)

(7) **Basic Properties of Valuations.** Let $v : \mathbb{K}^\times \rightarrow \Gamma$ be an arbitrary valuation. Fix $f, g \in \mathbb{K}^\times$.

- (a) Show that $v(f^{-1}) = -v(f)$.
- (b) Show that if $v(g) < v(f)$, then $v(f + g) = v(g)$. (Hint: Use that $(f + g) + (-f) = g$.)
- (c) Show that $v(f) = v(-f)$. (Hint: Use part 7b.)

(8) Consider the field $\mathbb{C}(x, y)$. Throughout this question π refers to the number $\pi = 3.1415926\dots$

(a) Show that there is a unique \mathbb{C} -valuation $v_\pi : \mathbb{C}(x, y)^\times \rightarrow (\mathbb{R}, +)$ such that

$$v_\pi(x^a y^b) = a + \pi b.$$

What is the value group of v_π ? (Hint: Use Question 3.)

(b) Consider the group $\Gamma = \mathbb{Z} \oplus \mathbb{Z}$ ordered by the lexicographical ordering. Show that there exists a unique \mathbb{C} -valuation $v : \mathbb{C}(x, y)^\times \rightarrow \Gamma$ such that $v(x^a y^b) = (a, b)$.

(c) Are either of these valuations constructed in parts 8a or 8b discrete?

(9) **Valuations Determine Valuation Rings.** Let v be an arbitrary valuation on \mathbb{K} .

(a) Prove that the set $R \subset \mathbb{K}$ of elements $f \in \mathbb{K}$ with $v(f) \geq 0$ is a valuation ring of \mathbb{K} . We call this the *valuation ring* of v . (Hint: Remember our convention about $v(0)$.)

(b) Show that the following is an ideal of R :

$$\mathfrak{m} := \{f \in \mathbb{K} \mid 0 < v(f)\}.$$

(c) Prove that if $f \in R$ and $f \notin \mathfrak{m}$ then f is a unit.

(d) Combine the previous parts to deduce \mathfrak{m} is the unique maximal ideal of R .

(e) Fix an element $\gamma \in \Gamma$. Prove the sets below are ideals of R :

$$\{f \in R \mid v(f) > \gamma\} \quad \text{and} \quad \{f \in R \mid v(f) \geq \gamma\}.$$

(10) **Discrete Valuation Rings.** Let $v : \mathbb{K}^\times \rightarrow \mathbb{Z}$ be a discrete valuation on \mathbb{K} . Let (R, \mathfrak{m}) be the corresponding *discrete valuation ring*.

(a) Let $I \subset R$ be any non-zero ideal, explain why we can choose an element $f \in I$ such that $v(f)$ is minimal among elements in I .

(b) Prove that every ideal in R is principal. In particular, a discrete valuation ring is a PID.

(c) By part 10b there exists an element $t \in R$ such that $\langle t \rangle = \mathfrak{m}$. Show that every ideal of R is either 0 or of the form $\langle t^n \rangle$ for some $n \geq 0$.

(11) Consider the valuation v_π on $\mathbb{C}(x, y)$ constructed in Question 8a. Let (R, \mathfrak{m}) be the corresponding valuation ring for v_π .

(a) For a real number $x \in \mathbb{R}_{\geq 0}$ let $\{x\} := x - \lfloor x \rfloor$ denote its fractional part. Fix a positive integer N and consider the sequence consisting of the fractional parts of the first $N + 1$ multiples of π : $\{0\}, \{\pi\}, \{2\pi\}, \dots, \{N\pi\} \in [0, 1)$. Divide the interval $[0, 1)$ into N evenly spaced subintervals:

$$[0, 1) = \left[0, \frac{1}{N}\right) \cup \left[\frac{1}{N}, \frac{2}{N}\right) \cup \dots \cup \left[\frac{N-1}{N}, 1\right).$$

Prove there exist integers $0 \leq k, j \leq N$ such that $\{k\pi\}$ and $\{j\pi\}$ lie in the same subinterval. Deduce that for any positive integer N there exist integers $0 \leq k, j \leq N$ such that $|\{k\pi\} - \{j\pi\}| \leq \frac{1}{N}$. (Hint: Think about pigeons.)

- (b) Using that π is irrational show that $\{j\pi\} \neq \{k\pi\}$ whenever $j \neq k$.
- (c) Prove for every real number $\epsilon > 0$, there exist integers $a, b \in \mathbb{Z}$ such that $0 < a + b\pi < \epsilon$.
- (d) Prove that \mathfrak{m} is not finitely generated. (Hint: Use part 11c.)
- (e) Prove that \mathfrak{m} is the only non-zero radical ideal of R . (Hint: If $I \subset R$ is a non-zero radical ideal, let $f \in I$ be non-zero. For an arbitrary element $h \in \mathfrak{m}$ show that $h^n \in \langle f \rangle$ for $n \gg 0$.)
- (f) Describe $\text{Spec}(V)$.

(12) Consider the valuation v on $\mathbb{C}(x, y)$ constructed in Question 8b. Let (R, \mathfrak{m}) be the corresponding valuation ring for v .

- (a) Show that the maximal ideal of R is

$$\mathfrak{m} = \{f \in \mathbb{C}(x, y) \mid v(f) \geq (0, 1)\} = \langle y \rangle.$$

- (b) Show that the ideal $\langle x \rangle \subset R$ is not prime. (Hint: $x = xy^{-1} \cdot y$.)
- (c) Show that the set below is a prime, non-maximal ideal of R :

$$P := \{f \in R \mid v(f) = (a, b) \text{ where } a \geq 1\} \cup \{0\}.$$

- (d) Use the valuation to construct an infinite strictly ascending chain of ideals in R :

$$\langle xy^{-1} \rangle \subset \langle xy^{-2} \rangle \subset \langle xy^{-3} \rangle \subset \dots$$

Explain why all inclusions are strict.

(13) **Valuation Rings Determine Valuations.** Let R be a valuation ring of \mathbb{K} with $R \neq \mathbb{K}$. This problem shows how to recover a valuation from the divisibility structure of R .

- (a) Let Γ' be the set of nonzero principal ideals of R :

$$\Gamma' = \{\langle a \rangle \subset R \mid a \in R, a \neq 0\}.$$

Define a multiplication on Γ' by ideal multiplication: $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$.

- (i) Show that this operation is well-defined and makes Γ' into an abelian monoid (associative, commutative, binary operation with an identity element).
 - (ii) Show that Γ' is totally ordered by inclusion: for distinct elements $\langle a \rangle, \langle b \rangle \in \Gamma'$, either $\langle a \rangle \subseteq \langle b \rangle$ or $\langle b \rangle \subseteq \langle a \rangle$.
- (b) Define an equivalence relation \sim on \mathbb{K}^\times by $x \sim y$ if and only if $x = uy$ for some unit $u \in R^\times$. Let $\Gamma = \mathbb{K}^\times / \sim$ denote the set of equivalence classes. Given $x \in \mathbb{K}^\times$ write $[x]$ its equivalence class in Γ .

- (i) Show that \sim is a well-defined equivalence relation.
 - (ii) Show that multiplication in \mathbb{K}^\times induces a well-defined operation on Γ , making it into an abelian group.
 - (iii) Define $[x] \leq [y]$ if and only if $yx^{-1} \in R$. Show this is a well-defined total order on Γ .
 - (iv) Deduce that Γ is an ordered abelian group.
 - (v) Show that the map $\Gamma' \rightarrow \Gamma$ given by $\langle a \rangle \mapsto [a]$ is an order-preserving embedding whose image consists exactly of the elements $\geq [1]$.
- (c) Define $\nu : \mathbb{K}^\times \rightarrow \Gamma$ by $\nu(x) = [x]$. Prove that ν is a valuation on \mathbb{K} with value group Γ and

$$R = \{x \in \mathbb{K} \mid \nu(x) \geq [1]\}.$$

Moreover, $\nu(x) \in \Gamma'$ if and only if $x \in R$.