# Contents

# 1. Basic theory

**Example**. Let $f(x_1, ..., x_r) \in \mathbb{Z}[x_1, ..., x_r]$, a Diophantine equation asks to solve $f(x_1, ..., x_r) = 0$. Easier questions are when is $f(x_1, ..., x_r) \equiv 0 (\operatorname{mod} p)$ and $f(x_1, ..., x_r) \equiv 0 (\operatorname{mod} p^n)$. Local fields "package" all this information together for all $n$.

## 1.1. Absolute values

**Definition**. Let $K$ be a field. An **absolute value** on $K$ is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that $\forall x, y \in K$:
- $|x| = 0 \Longleftrightarrow x = 0$.
- $|xy| = |x| \cdot |y|$ (multiplicative).
- $|x + y| \leq |x| + |y|$ (triangle inequality).

$(K, |\cdot|)$ is a **valued field**.

**Example**.
- $K = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ with usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$. We write $|\cdot|_\infty$ for this absolute value.
- The **trivial** absolute value is $|x| = 0$ if $x = 0$ and $|x| = 1$ otherwise.

**Definition**. Let $K = \mathbb{Q}$, $p$ be prime. For $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$ where $p \nmid a, b$. The ***p*-adic absolute value** $|\cdot|_p$ is defined as

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x = p^n \frac{a}{b} \end{cases}.$$

**Proposition**. The $p$-adic absolute value is an absolute value.

*Proof.*
- The first axiom is trivial.
- Let $y = p^m \frac{c}{d}$.
- $|xy|_p = |p^{m+n} \frac{ac}{bd}|_p = p^{-m-n} = |x|_p \cdot |y|_p$.
- WLOG, assume that $m \geq n$. $|x + y|_p = |p^n \frac{ad + p^{m-n} bc}{bd}|_p \leq p^{-n} = \max\{|x|_p, |y|_p\}$.

□

**Proposition**. An absolute value $|\cdot|$ on $K$ induces a metric $d(x, y) = |x - y|$ (and hence a topology) on $K$.

*Proof.* Exercise. □

**Definition**. Two absolute values on $K$ are **equivalent** if they induce the same topology.

A **place** is an equivalence class of absolute values.

**Proposition**. Let $|\cdot|$ and $|\cdot|'$ be non-trivial absolute values on $K$. Then TFAE:
1. $|\cdot|$ and $|\cdot|'$ are equivalent.
2. $|x| < 1$ iff $|x|' < 1$ for all $x \in K$.
3. There exists $c > 0$ such that $|x|^c = |x|'$ for all $x \in K$.

*Proof.*

- $(1 \Rightarrow 2)$:
  - $|x| < 1$ iff $x^n \to 0$ w.r.t $|\cdot|$ iff $x^n \to 0$ w.r.t $|\cdot|'$ iff $|x|' < 1$.
- $(2 \Rightarrow 3)$:
  - Note $|x|^c = |x|'$ iff $c \log|x| = \log|x|'$.
  - Let $a \in K^\times$ such that $|a| > 1$ (this exists since $|\cdot|$ is non-trivial).
  - We show that $\log|x| \,/ \log|a| = \log|x|' \,/ \log|a|'$ for all $x \in K^\times$.
  - Assume not, then $\log|x| \,/ \log|a| < \log|x|' \,/ \log|a|'$.
  - Choose $m, n \in \mathbb{Z}$ such that $\log|x| \,/ \log|a| < \frac{m}{n} < \log|x| \,/ \log|a|$.
  - Then $n \log|x| < m \log|a|$ and $n \log|x|' > m \log|a|'$, so $|\frac{x^n}{a^m}| < 1$ but $|\frac{x^n}{a^m}|' > 1$: contradiction.
  - Similarly for $\log|x| \,/ \log|a| > \log|x|' \,/ \log|a|'$.
- $(3 \Rightarrow 1)$:
  - Trivial, as open balls they define are the same.

□

**Remark.** $|\cdot|_\infty^2$ on $\mathbb{C}$ is not an absolute value by out definition since it violates the triangle inequality. Note some authors replace the triangle inequality axiom with $|x + y|^\beta \le |x|^\beta + |y|^\beta$ for some fixed $\beta > 0$.

**Definition.** An absolute value $|\cdot|$ on $K$ is **non-Archimedean** if it satisfies the **ultrametric inequality**:

$$|x + y| \le \max\{|x|, |y|\}.$$

Otherwise, it is **Archimedean**.

**Example.**

- $|\cdot|_\infty$ on $\mathbb{R}$ is Archimedean.
- $|\cdot|_p$ on $\mathbb{Q}$ is non-Archimedean.

**Lemma.** Let $(K, |\cdot|)$ be non-Archimedean and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$ (i.e. all triangles are isosceles).

*Proof.* For $\le$, use ultrametric inequality. For $\ge$, use that $|y| = |x - y - x|$. □

**Proposition.** Let $(K, |\cdot|)$ be non-Archimedean. Let $(x_n)$ be a sequence in $K$. If $|x_n - x_{n+1}| \to 0$, then $x_n$ is Cauchy. In particular, if $K$ is complete with respect to $|\cdot|$, then $(x_n)$ converges.

*Proof.*

- For $\varepsilon > 0$, choose $N$ such that $|x_n - x_{n+1}| < \varepsilon$ for all $n > N$.
- Then for $N < n < m$, $|x_n - x_m| = |(x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \cdots + (x_{m-1} - x_m)| < \varepsilon$.

□

**Example.** Let $p = 5$ and consider the sequence $(x_n)$ in $\mathbb{Z}$ satisfying:

- $x_n^2 + 1 \equiv 0 \bmod 5^n$.
- $x_n \equiv x_{n+1} \bmod 5^n$.

Take $x_1 = 2$. Suppose we have constructed $x_1, ..., x_n$. Then write $x_n^2 + 1 = a5^n$ and set $x_{n+1} = x_n + b5^n$. Then $x_{n+1}^2 + 1 = x_n^2 + 2bx_n5^n + b^2 5^{2n} + 1 = a5^n + 2bx_n5^n + b^2 5^{2n}$. We choose $b$ such that $a + 2bx_n \equiv 0 \bmod 5$ (this congruence is solvable). Then we have $x_{n+1}^2 + 1 = 0 \bmod 5^{n+1}$.

Hence $(x_n)$ is Cauchy. Suppose $x_n \to l \in \mathbb{Q}$. Then $x_n^2 \to l^2 \in \mathbb{Q}$. But the first condition implies that $x_n^2 \to -1 = l^2$, contradiction. So $(x_n)$ doesn't converge in $\mathbb{Q}$. So $(\mathbb{Q}, |\cdot|_5)$ is not complete.

**Definition**. The set of ***p*-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

**Remark**. There is an analogy with the construction of $\mathbb{R}$ with respect to $|\cdot|_\infty$.

**Definition**. For $x \in K$ and $r > 0$, define

$$B(x, r) \coloneqq \{y \in K : |x - y| < r\},$$
$$\overline{B}(x, r) = \{y \in K : |x - y| \leq r\}.$$

**Lemma**. Let $(K, |\cdot|)$ be a non-Archimedean valued field.
- If $z \in B(x, r)$, then $B(z, r) = B(x, r)$, i.e. open balls don't have a centre.
- If $z \in \overline{B}(x, r)$, then $\overline{B}(z, r) = \overline{B}(x, r)$. i.e. closed balls don't have a centre.
- $B(x, r)$ is closed.
- $\overline{B}(x, r)$ is open.

*Proof.*
- Let $y \in B(x, r)$. Then $|x - y| < r$ so $|z - y| = |(z - x) + (x - y)| \leq \max\{|z - x|, |x - y|\} < r$. Hence $B(x, r) \subseteq B(z, r)$. Converse is obtained by symmetry.
- Same as above.
- Let $y \notin B(x, r)$. If $z \in B(x, r) \cap B(y, r)$ then $B(x, r) = B(z, r) = B(y, r)$ by above, hence $y \in B(x, r)$: contradiction. Hence $B(x, r) \cap B(y, r) = \emptyset$.
- Let $z \in \overline{B}(x, r)$, then $B(z, r) \subseteq \overline{B}(z, r) = \overline{B}(x, r)$ by above.

$\square$

# 2. Valuation rings

**Definition**. Let $K$ be a field. $t : K^\times \to \mathbb{R}$ is a **valuation** on $K$ if:
- $v(xy) = v(x) + v(y)$.
- $v(x + y) \geq \min\{v(x), v(y)\}$.

Fix $\alpha \in (0, 1)$. Then for a valuation $v$ on $K$, we can define a non-Archimedean absolute value

$$|x| = \begin{cases} \alpha^{v(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

Conversely, a non-Archimedean absolute value determines a valuation

$$v(x) = \log_\alpha |x|$$

**Remark**.

- We ignore the trivial valuation $v(x) = 0$ (corresponds to trivial absolute value).
- We say $v_1$ and $v_2$ are equivalent valuations if there exists $c > 0$ such that $v_1(x) = cv_2(x)$ for all $x \in K^\times$.

**Example**.

- For $K = \mathbb{Q}$, $v_p(x) = -\log_p|x|_p$ is the $p$-adic valuation.
- Let $k$ be field, $K = k(t) = \operatorname{Frac}(k[t])$ be the rational function field. Define the $t$-adic valuation $v\left(t^n \frac{f(t)}{g(t)}\right) = n$ where $f, g \in k[t]$, $f(0), g(0) \neq 0$.
- $K = k((t)) = \operatorname{Frac}(k[[t]]) = \{\sum_{i=n}^{\infty} a_i t^i : a_i \in k, n \in \mathbb{Z}\}$ is the field of formal Laurent series over $k$. Define the $t$-adic valuation

$$v\left(\sum_i a_i t^i\right) = \min\{i \in \mathbb{Z} : a_i \neq 0\}$$

**Definition**. Let $(K, |\cdot|)$ be a non-Archimedean valued field. The **valuation ring** of $K$ is

$$\begin{aligned}\mathcal{O}_K &= \{x \in K : |x| \leq 1\} = \overline{B}(0,1) \\ &= \{x \in K^\times : v(x) \geq 0\} \cup \{0\}\end{aligned}$$

**Proposition**.

- $\mathcal{O}_K$ is an open subring of $K$.
- The subsets $\{x \in K : |x| \leq r\}$ and $\{x \in K : |x| < r\}$ are both open ideals in $\mathcal{O}_K$ for $r \leq 1$.
- $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$.

*Proof.*

- To show ring:
  - $|0| = 0, |1| = 1 \leq 1$ so $0, 1 \in \mathcal{O}_K$.
  - If $x \in \mathcal{O}_K$, then $|-x| = |x| \leq 1$ so $-x \in \mathcal{O}_K$.
  - If $x, y \in \mathcal{O}_K$, then $|x + y| \leq \max\{|x|, |y|\} \leq 1$ so $x + y \in \mathcal{O}_K$.
  - If $x, y \in \mathcal{O}_K$, then $|xy| = |x|\ |y| \leq 1$ so $xy \in \mathcal{O}_K$.
- $\mathcal{O}_K$ is open since it is a "closed" ball.
- Showing open ideals is similar to above.
- $|x|\ |x^{-1}| = |xx^{-1}| = 1$ so $|x| = 1$ iff $|x^{-1}| = 1$, i.e. $x, x^{-1} \in \mathcal{O}_K$, i.e. $x \in \mathcal{O}_K^\times$.

$\square$

**Notation**. Write $m := \{x \in \mathcal{O}_K : |x| < 1\}$ which is a maximal ideal in $\mathcal{O}_K$. $k = \mathcal{O}_K/m$ be the **residue field**.

**Corollary**. $\mathcal{O}_K$ is a local ring (i.e. it has a unique maximal ideal) with unique maximal ideal $m$.

*Proof.* Let $m' \neq m$ be a maximal ideal, then there exists $x \in m' \setminus m$, hence $|x| = 1$ so $x$ is a unit, so $m' = R$: contradiction. $\square$

**Example**.

- Let $K = \mathbb{Q}$ with $|\cdot|_p$. Then $\mathcal{O}_K = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b\right\}$. $m = p\mathbb{Z}_{(p)}$ and $k = \mathbb{F}_p$.

**Definition**. A valuation $v : K^\times \to \mathbb{R}$ is **discrete** if $v(K^\times) \cong \mathbb{Z}$. In this case, $K$ is a **discretely valued field**, and element $\pi \in \mathcal{O}_K$ is a **uniformiser** if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$.

**Example**.
- $K = \mathbb{Q}$ with the $p$-adic valuation is discretely valued.
- $K = k(t)$ with the $t$-adic valuation is discretely valued.
- $K = k(t)\left(t^{1/2}, t^{1/4}, ...\right)$ with the $t$-adic valuation is not discrete.

**Remark**. If $v$ is a discrete valuation, then we can replace it with an equivalent valuation such that $v(K^\times) = \mathbb{Z}$. Such valuations are called **normalised** valuations (in this case, $\pi$ is a uniformiser iff $v(\pi) = 1$).

**Lemma**. Let $v$ be a valuation on $K$. TFAE:
1. $v$ is discrete.
2. $\mathcal{O}_K$ is a PID.
3. $\mathcal{O}_K$ is Noetherian.
4. $m$ is principal.

*Proof.*
- $(1 \Rightarrow 2)$:
  - $\mathcal{O}_K$ is ID as subring of a field.
  - Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal, $x \in I$ such that $v(x) = \min\{v(a) : a \in I\}$ (which exists as valuation is discrete).
  - We claim $x\mathcal{O}_K = \{a \in K : v(a) \geq v(x)\}$ is equal to $I$.
  - $\subseteq$: since $I$ is ideal.
  - $\supseteq$: let $y \in I$, then $v(x^{-1}y) \geq 0$ so $y = x(x^{-1}y) \in x\mathcal{O}_{\mathcal{K}}$ TODO: finish.
- $(2 \Rightarrow 3)$: clear.
- $(3 \Rightarrow 4)$: write $m = x_1\mathcal{O}_K + \cdots + x_n\mathcal{O}_K$. WLOG $v(x_1) \leq \cdots \leq v(x_n)$. Then $x_2, ..., x_n \in x_1\mathcal{O}_K$ so $m = x\mathcal{O}_K$.
- $(4 \Rightarrow 1)$: let $m = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$, let $c = v(\pi)$. Then if $v(x) > 0$, $x \in m$, hence $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \emptyset$. Since $v(K^\times)$ is a subgroup, we must have $v(K^\times) = c\mathbb{Z}$.

$\square$