

Kapitel II

Valuation theory

§ 7 Discrete valuations

Example 7.1 Let $P \in \mathbb{N}$ prime. For $x \in \mathbb{Z} \setminus \{0\}$ let

$$\nu_p(x) = \max\{k \in \mathbb{N} \mid p^k \mid x\}.$$

Then $p^{\nu_p(x)} \mid x$, $p^{\nu_p(x)+1} \nmid x$. Example: $\nu_2(12) = 2$. Write $x = p^{\nu_p(x)} \cdot x'$ where $p \nmid x'$. For $\frac{x}{y} \in \mathbb{Q}^\times$ define

$$\nu_p\left(\frac{x}{y}\right) = \nu_p(x) - \nu_p(y).$$

This defines a map $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z}$, such that

- (i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ (clear)
- (ii) $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$, since: Write $a = p^{\nu_p(a)} \cdot a'$, $b = p^{\nu_p(b)} \cdot b'$. Let w.l.o.g $\nu_p(b) \leq \nu_p(a)$. Then we have

$$a+b = p^{\nu_p(a)} \cdot a' + p^{\nu_p(b)} \cdot b' = p^{\nu_p(b)} \cdot (b' + a' \cdot p^{\nu_p(a)-\nu_p(b)}).$$

Hence $p^{\nu_p(b)} \mid a+b$ and thus $\nu_p(a+b) \geq \nu_p(b) = \min\{\nu_p(a), \nu_p(b)\}$.

Definition 7.2 Let k be a field. A *discrete valuation* on k is a surjective group homomorphism $\nu_k^\times \longrightarrow (\mathbb{Z}, +)$ satisfying

$$\nu(x+y) \geq \min\{\nu(x), \nu(y)\} \quad \text{for all } x, y \in k^\times, x \neq -y.$$

Remark 7.3 Let R be a factorial domain, $k = \text{Quot}(R)$. Let further be $p \in R \setminus \{0\}$ be a prime element. Then $\nu_p : k^\times \longrightarrow \mathbb{Z}$ can be defined as in Example 7.1: Write

$$x = e \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(x)}, \quad e \in R^\times$$

where \mathbb{P} denotes set of representatives of prime elements of R . Then ν_p is a discrete valuation on k .

Example 7.4 Let k be a field, $a \in k$, $R = k[X]$ and $p_a = X - a \in k[X]$. For $f \in k[X]$ define $\nu_{p_a}(f) = n$ if f has an n -fold root in a , i.e. $f = (X - a)^n \cdot g$ for some $0 \neq g \in k[X]$. Then ν_{p_a} is a discrete valuation on $k(X) = \text{Quot}(k[X])$ satisfying $\nu_p|_k = 0$.

Remark 7.5 There is no discrete valuation on \mathbb{C} .

proof. Assume there exists a discrete valuation on \mathbb{C} , say $\nu : \mathbb{C}^\times \rightarrow \mathbb{Z}$. Since ν is surjective, there exists $z \in \mathbb{C}^\times$ such that $\nu(z) = 1$.

Let now $y \in \mathbb{C}^\times$ such that $y^2 = z$. Then we have

$$1 = \nu(z) = \nu(y^2) = \nu(y \cdot y) = \nu(y) + \nu(y) = 2\nu(y) \iff \nu(y) = \frac{1}{2} \notin \mathbb{Z}$$

which is a contradiction. □

Example 7.6 Let $\nu : \mathbb{Q}^\times \rightarrow \mathbb{Z}$ be a nontrivial discrete valuation. Then there exists $a \in \mathbb{Z}$ such that $\nu(a) \neq 0$ and hence we find $p \in \mathbb{P}$: $\nu(p) \neq 0$.

If $\nu(q) = 0$ for all $q \in \mathbb{P}$, then $\nu = \nu_p$.

Assume we have $\nu(p) \neq 0 \neq \nu(q)$ for some $p \neq q \in \mathbb{P}$ and write $1 = ap + bq$ for suitable $a, b \in \mathbb{Z}$.

Then

$$0 = \nu(1) = \nu(ap + bq) \geq \min\{\nu(ap), \nu(bq)\} = \min\{\underbrace{\nu(a)}_{\geq 0 (*)} + \nu(p), \underbrace{\nu(b)}_{\geq 0 (*)} + \nu(q)\} \geq \min\{\nu(p), \nu(q)\} > 0$$

Hence a contradiction, i.e. we have $\nu(p) \neq 0$ for at most one $p \in \mathbb{P}$, thus $\nu = \nu_p$.

(*) obtain that we have $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \Rightarrow \nu(1) = 0$ and by induction

$$\nu(a) = \nu(1 + (a - 1)) \geq \min\{\nu(1), \nu(a - 1)\} \geq 0$$

Proposition 7.7 Let k be a field and $\nu : k^\times \rightarrow \mathbb{Z}$ be a discrete valuation on k .

- (i) $\nu(1) = \nu(-1) = 0$.
- (ii) $\mathcal{O}_\nu := \{x \in k^\times \mid \nu(x) \geq 0\} \cup \{0\}$ is a ring, called the valuation ring of ν .
- (iii) $\mathfrak{m}_\nu := \{x \in k^\times \mid \nu(x) > 0\} \cup \{0\} \triangleleft \mathcal{O}_\nu$ is an ideal in \mathcal{O}_ν , called the valuation ideal of ν .
More precisely, \mathfrak{m}_ν is the only maximal ideal in \mathcal{O}_ν , i.e. \mathcal{O}_ν is a local ring.
- (iv) \mathfrak{m}_ν is a principal ideal.
- (v) \mathcal{O}_ν is a principal ideal domain. More precisely, any ideal $I \neq \{0\}$ in \mathcal{O}_ν is of the form $I = (t^d)$ for some $d \in \mathbb{N}$ and $t \in \mathfrak{m}_\nu$ with $\nu(t) = 1$.
- (vi) We have $k = \text{Quot}(\mathcal{O}_\nu)$ and for $x \in k^\times$: $x \in \mathcal{O}_\nu$ or $\frac{1}{x} \in \mathcal{O}_\nu$.

proof. (ii) This is strict calculating, which may be verified by the reader.

(iii) \mathfrak{m}_ν is an ideal, since for $x, y \in \mathfrak{m}_\nu, \alpha \in \mathcal{O}_\nu$ we have

$$\nu(x + y) \geq \min\{\nu(x), \nu(y)\} > 0, \quad \nu(\alpha x) = \underbrace{\nu(\alpha)}_{\geq 0} + \nu(x) \geq \nu(x) > 0.$$

Let now $x \in \mathcal{O}_\nu$ with $\nu(x) = 0$. Then

$$\nu\left(\frac{1}{x}\right) = \nu(1) - \nu(x) = -\nu(x) = 0,$$

hence $x \in \mathcal{O}_\nu^\times$. Thus we have $\mathfrak{m}_\nu = \mathcal{O}_\nu \setminus \mathcal{O}_\nu^\times$ and the claim follows.

(iv) Let $t \in \mathfrak{m}_\nu$ such that $\nu(t) = 1$. Then for $x \in \mathfrak{m}_\nu$ let $\nu(x) = d > 0$. Then we have

$$\nu\left(x \cdot t^{-d}\right) = \nu(x) + \nu\left(\frac{1}{t^d}\right) = d + 0 - d = 0$$

Define $e := x \cdot t^{-d} \in \mathcal{O}_\nu^\times$. Then $x = e \cdot t^d$, hence $\mathfrak{m}_\nu = (t)$.

(v) Let $\{0\} \neq I \neq \mathcal{O}_\nu$ be an ideal in \mathcal{O}_ν . Let $d := \min\{\nu(x) \mid x \in I \setminus \{0\}\} > 0$.

' \supseteq ' Let $x \in I$ such that $\nu(x) = d$. By part (iv) we have $x = e \cdot t^d$ for some $e \in \mathcal{O}_\nu^\times$, hence we have $t^d \in I$; thus $(t^d) \subseteq I$.

' \subseteq ' Let now $y \in I \setminus \{0\}$ and write $y = e \cdot t^{\nu(y)}$ for some $e \in \mathcal{O}_\nu^\times$ and $\nu(y) > d$. Then $y = t^d \cdot e \cdot t^{\nu(y)-d}$, hence $y \in (t^d)$ and thus $I \subseteq (t^d)$.

(vi) If $\nu(x) \geq 0$, then $x \in \mathcal{O}_\nu$. If $\nu(x) < 0$, we have

$$\nu\left(\frac{1}{x}\right) = \nu(1) - \nu(x) = -\nu(x) > 0, \quad \text{hence } \frac{1}{x} \in \mathfrak{m}_\nu \subseteq \mathcal{O}_\nu,$$

which we wanted to show. □

Definition 7.8 An integral domain R is called a *discrete valuation ring*, if there exists a discrete valuation ν of $k = \text{Quot}(R)$ such that $R = \mathcal{O}_\nu$.

Proposition 7.9 Let R be a lokal integral domain. Then the following statements are equivalent.

- (i) R is a discrete valuation ring.
- (ii) R is a principal ideal domain.
- (iii) There exists $t \in R \setminus \{0\}$ such that every $x \in R \setminus \{0\}$ can uniquely be written in the form

$$x = e \cdot t^d \quad \text{for some } e \in R^\times, d \geq 0$$

proof. '(i) \Rightarrow (ii)' This follows by 7.7.

'(ii) \Rightarrow (iii)' We know that principal ideal domains are factorial. Let $t \in R$ be a generator of the maximal ideal \mathfrak{m} of R . Then t is prime, since any maximal ideal is also prime. Let now $p \in R \setminus \{0\}$ a prime element. Then $p \notin R^\times$, hence $p \in \mathfrak{m}$, thus we can write $p = t \cdot x$ for some $x \in R$. Since p is prime, hence irreducible, we have $x \in R^\times \Rightarrow (p) = (t)$. Thus we

have $p = t$ and we have only one prime element in R . The unique prime factorization in factorial domains gives us $x = e \cdot t^d$ for some $e \in R^\times$ and $d \geq 0$.

'(iii) \Rightarrow (i)' For $x = e \cdot t^d \in R \setminus \{0\}$, $e \in R^\times$, $d \geq 0$ define $\nu(x) = d$. We claim that ν is discrete valuation. We have

$$\nu(xy) = \nu(et^d \cdot e't^{d'}) = \nu(ee't^{d+d'}) = \nu(e''t^{d+d'}) = d + d'.$$

Let w.l.o.g. $d \leq d'$. Then

$$\nu(x + y) = \nu(et^d + e't^{d'}) = \nu(t^d(e + e't^{d'-d})) \geq d = \min\{d, d'\}$$

which we extend to

$$\nu : k^\times \longrightarrow \mathbb{Z}, \quad \nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y).$$

This is well defined: For $\frac{x}{y} = \frac{x'}{y'}$ we have $xy' = x'y$ and $\nu(xy') = \nu(x) + \nu(y') = \nu(x') + \nu(y)$, thus

$$\nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y) = \nu(x') - \nu(y') = \nu\left(\frac{x'}{y'}\right).$$

Finally we have $\nu(t) = 1$, hence $\nu : k^\times \longrightarrow \mathbb{Z}$ is surjective. Thus ν is a discrete valuation on k and $R = \mathcal{O}_\nu$. \square

Definition + proposition 7.10 Let R be a local ring with maximal ideal \mathfrak{m} .

- (i) $k := R/\mathfrak{m}$ is called the *residue field* of R .
- (ii) $\mathfrak{m}/\mathfrak{m}^2$ has a structure of a k -vector space.
- (iii) If R is a discrete valuation ring, then $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

proof. (ii) For $a \in R$, $x \in \mathfrak{m}$ define $\overline{ax} = \overline{a}\overline{x}$, where $\overline{a}, \overline{x}$ are the images of a, x in k .

This is well defined: Let $a' \in R$ with $\overline{a'} = \overline{a}$ and $x' \in \mathfrak{m}$ with $\overline{x'} = \overline{x}$. We have to show that

$$\overline{a'x'} = \overline{ax} \iff a'x' - ax \in \mathfrak{m}^2$$

We have $\overline{a'} = \overline{a}$, hence $a' = a + y$ for some $y \in \mathfrak{m}$. Analogously we have $\overline{x'} = \overline{x}$, hence $x' = x + z$ for some $z \in \mathfrak{m}$. Thus we have

$$a'x' = (a + y)(x + z) = ax + az + xy + yz \equiv ax \pmod{\mathfrak{m}^2},$$

which finishes the proof. \square

§ 8 The Gauß Lemma

Let R be a UFD (unique factorization domain), \mathbb{P} a set of representatives of the primes in R with respect to *associateness*, i.e. $x \sim y \Leftrightarrow y = u \cdot x$ for some $u \in R^\times$. Every $x \in R \setminus \{0\}$ has a unique factorization

$$x = u \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(x)}, \quad \nu_p(x) \geq 0 \text{ for } p \in \mathbb{P}, u \in R^\times$$

where $\nu_p : k^\times \rightarrow \mathbb{Z}$ is a discrete valuation on $k = \text{Quot}(R)$.

Definition + proposition 8.1 Let R be a factorial domain, $k = \text{Quot}(R)$ and

$$f = \sum_{i=0}^n a_i X^i \in k[X] \setminus \{0\}, \quad a_n \neq 0.$$

- (i) For $p \in \mathbb{P}$ let $\nu_p(f) = \min\{\nu_p(a_i) \mid 0 \leq i \leq n\}$.
- (ii) f is called *primitive*, if $\nu_p(f) = 0$ for all $p \in \mathbb{P}$.
- (iii) If f is primitive, then $f \in R[X]$.
- (iv) If $f \in R[X]$ is monic, i.e. $a_n = 1$, then f is primitive.
- (v) There exists $c \in k^\times$ such that $c \cdot f$ is primitive.

proof. (iii) If f is primitive, we have $\min_{1 \leq i \leq n} \{\nu_p(a_i)\} = 0$, i.e. $\nu_p(a_i) \geq 0$ for all $1 \leq i \leq n$.

Thus $a_i \in R$ and $f \in R[X]$.

- (iv) If $a_i \in R$ we have $\nu_p(a_i) \geq 0$ for all $1 \leq i \leq n$. Moreover $\nu_p(a_n) = \nu_p(1) = 0$, hence $\nu_p(f) = \min_{1 \leq i \leq n} \{\nu_p(a_i)\} = 0$. thus f is primitive.

- (v) For $\nu_p(f) := d$ choose $c := p^{-d} \in k^\times$. Then

$$\nu_p(c \cdot f) = \nu_p(c) + \nu_p(f) = \nu_p(p^{-d}) + d = -d + d = 0,$$

thus $c \cdot f$ is primitive. □

Proposition 8.2 (Gauß-Lemma) For $f, g \in k[X]$ and $p \in \mathbb{P}$ we have

$$\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g).$$

proof. Write

$$f = \sum_{i=0}^n a_i X^i, \quad g = \sum_{j=0}^m b_j X^j, \quad f \cdot g = \sum_{k=0}^{m+n} c_k X^k, \quad c_k = \sum_{i=0}^k a_i b_{k-i}$$

case 1 Assume $m = 0$, i.e. $g = b_0 \in k^\times$. Then $c_k = a_k \cdot b_0$, hence

$$\nu_p(c_k) = \nu_p(a_k) + \nu_p(b_0).$$

Then we obtain

$$\nu_p(f \cdot g) = \min_{0 \leq k \leq n} \nu_p(c_k) = \min_{0 \leq k \leq n} \{\nu_p(a_k) + \nu_p(b_0)\} = \nu_p(b_0) + \min_{0 \leq k \leq n} \{\nu_p(a_k)\} = \nu_p(g) + \nu_p(f)$$

case 2 Assume $\nu_p(f) = 0 = \nu_p(g)$, i.e. f, g are primitive. Clearly $\nu_p(fg) \geq 0$. We have to show: $\nu_p(fg) = 0$. Let $i_0 := \max\{i \mid \nu_p(a_i) = 0\}$ and $j_0 := \max\{j \mid \nu_p(b_j) = 0\}$. Then

$$c_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} a_i b_{i_0+j_0-i} = \underbrace{\sum_{i=0}^{i_0-1} a_i b_{i_0+j_0-i}}_{(A)} + a_{i_0+j_0} + \underbrace{\sum_{i=i_0+1}^{i_0+j_0} a_i b_{i_0+j_0-i}}_{(B)}$$

We have $\nu_p(a_{i_0} b_{j_0}) = \nu_p(a_{i_0}) + \nu_p(b_{j_0}) = 0$. We have $i_0 + j_0 - i > j_0$, hence $\nu_p(b_{i_0+j_0-i}) \geq 1$ for $0 \leq i \leq i_0 - 1$. Then

$$\begin{aligned} \nu_p(A) &= \nu_p \left(\sum_{i=0}^{i_0-1} a_i b_{i_0+j_0-i} \right) \geq \min_{0 \leq i \leq i_0-1} \{\nu_p(a_i b_{i_0+j_0-i})\} \\ &= \min_{0 \leq i \leq i_0-1} \{\nu_p(a_i) + \nu_p(b_{i_0+j_0-i})\} \\ &\geq \min_{0 \leq i \leq i_0-1} \{\nu_p(b_{i_0+j_0-i})\} \\ &\geq 1 \\ \nu_p(B) &= \nu_p \left(\sum_{i=i_0+1}^{i_0+j_0} a_i b_{i_0+j_0-i} \right) \geq 1. \end{aligned}$$

Since we have

$$0 = \nu_p(a_{i_0} b_{j_0}) \geq \min\{\nu_p(c_{i_0+j_0}), \nu_p(A), \nu_p(B)\} = \nu_p(c_{i_0+j_0}) = 0$$

we get $\nu_p(c_{i_0+j_0}) = 0$. Hence we obtain

$$\nu_p(fg) = \min\{\nu_p(c_i) \mid 0 \leq i \leq m+n\} = \nu_p(c_{i_0+j_0}) = 0.$$

case 3 Consider now the general case, i.e. f, g are arbitrary. Multiply f and g by suitable constants a and b , such that $\tilde{f} := af$ and $\tilde{g} := bg$ are primitive. Then by the first two cases we have

$$\begin{aligned} \nu_p(fg) &= \nu_p \left(\frac{1}{a} \frac{1}{b} \tilde{f} \tilde{g} \right) \stackrel{1}{=} \nu_p \left(\frac{1}{a} \frac{1}{b} \right) + \nu_p(\tilde{f} \tilde{g}) \stackrel{2}{=} \nu_p \left(\frac{1}{a} \right) + \nu_p \left(\frac{1}{b} \right) + \underbrace{\nu_p(\tilde{f})}_{=0} + \underbrace{\nu_p(\tilde{g})}_{=0} \\ &= \nu_p \left(\frac{1}{a} \right) + \nu_p(\tilde{f}) + \nu_p \left(\frac{1}{b} \right) + \nu_p(\tilde{g}) = \nu_p \left(\frac{1}{a} \tilde{f} \right) + \nu_p \left(\frac{1}{b} \tilde{g} \right) \\ &= \nu_p(f) + \nu_p(g), \end{aligned}$$

which finishes the proof. □

Theorem 8.3 (*Eisenstein's criterion for irreducibility*) Let R be a factorial domain, $p \in \mathbb{P}$ and

$$f = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$$

Assume that f is primitive and we have

- (i) $\nu_p(a_0) = 1$,
- (ii) $\nu_p(a_i) \geq 1$ or $a_i = 0$ for $1 \leq i \leq n-1$ and
- (iii) $\nu_p(a_n) = 0$

Then f is irreducible over $R[X]$.

proof. Assume that $f = g \cdot h$ with some $g, h \in R[X]$. Write

$$g = \sum_{i=0}^r b_i X^i, \quad h = \sum_{j=0}^s c_j X^j, \quad \text{with } r + s = n$$

Then we have $a_0 = b_0 c_0$. W.l.o.g. $\nu_p(b_0) = 1$ and $\nu_p(c_0) = 0$. Further $a_n = b_r c_s$, thus we must have $\nu_p(b_r) = \nu_p(c_s) = 0$ for $\nu_p(a_n) = 0$. Let now

$$d := \max\{i \mid \nu_p(b_j) \geq 1 \text{ for } 0 \leq j \leq i\}$$

Obviously $0 \leq d \leq r-1$. Consider

$$a_{d+1} = \underbrace{b_{d+1} c_0}_{=:A} + \underbrace{\sum_{i=0}^d b_i c_{d+1-i}}_{=:B}.$$

We have

$$\nu_p(A) = \nu_p(b_{d+1}) + \nu_p(c_0) = 0 + 0 = 0,$$

$$\nu_p(B) \geq \min_{0 \leq i \leq d} \{\nu_p(b_i c_{d+1-i})\} \geq 1$$

and thus $\nu_p(a_{d+1}) = 0$. But this implies $d+1 = n \Leftrightarrow n-1 = d \leq r-1 \Rightarrow n \leq r \Rightarrow n = r$. Then we have $s = 0$, thus $h = c_0$ is constant. Further for $q \in \mathbb{P}$ we have

$$0 = \nu_q(f) = \nu_q(g c_0) = \underbrace{\nu_q(g)}_{\geq 0} + \nu_q(c_0)$$

i.e. $\nu_q(c_0) = 0$, hence $c_0 \in R^\times$ and f is irreducible. □

Theorem 8.4 (*Gauß*) Let R be a factorial domain. Then $R[X]$ is factorial.

proof. Let $f \in R[X] \setminus \{0\} \subseteq k[X]$ where $k = \text{Quot}(R)$. Since $k[X]$ is factorial, we can write

$$f = c \cdot f_1 \cdots f_n, \quad f_i \in k[X] \text{ prime}, \quad c \in k^\times$$

W.l.o.g the. f_i are primitive, otherse multiply them by suitable constants. In particular we have $f_i \in R[X]$. Note that $c \in R$: For $p \in \mathbb{P}$, we have

$$0 = \nu_p(f) = \nu_p(c) + \sum_{i=1}^n \nu_p(f_i) = \nu_p(c).$$

Write $c = \epsilon \cdot p_1 \cdots p_r$ with some $\epsilon \in R^\times$ and $p_i \in \mathbb{P}$. Then by

Claim (a) $f_i \in R[X]$ are prime for $1 \leq i \leq n$.

Claim (b) $p_i \in R[X]$ are prime for $1 \leq i \leq r$.

we have found a factorization of f into prime elements and hence $R[X]$ is factorial. Now prove the claims.

(a) Let $g, h \in R[X]$ such that $gh \in (f_i) = f_i R[X]$.

May assume that $g \in f_i k[X]$, i.e. $g = f_i \tilde{g}$ for some $\tilde{g} \in k[X]$. For $p \in \mathbb{P}$ we obtain

$$0 \leq \nu_p(g) = \underbrace{\nu_p(f_i)}_{=0} + \nu_p(\tilde{g}) = \nu_p(\tilde{g}).$$

Thus we get $\tilde{g} \in R[X]$, which implies $g = f_i \tilde{g} \in f_i R[X] = (f_i)$.

(b) Since $\pi : R \longrightarrow R/(p)$ induces a map $\psi : R[X] \longrightarrow R/(p)[X]$ with $\ker(\psi) = pR[X]$ we have

$$R[X]/pR[X] \cong R/pR[X].$$

Since R/pR is an integral domain, (p) is prime. □

Corollary 8.5 *Let k be a field. Then $k[X_1, \dots, X_n]$ is factorial for any $n \in \mathbb{N}$.*

Corollary 8.6 *Let R be a factorial domain, $k = \text{Quot}(R)$. If $f \in R[X]$ is irreducible over $R[X]$, then f is irreducible over $k[X]$.*

proof. Let $0 \neq f = c \cdot f_1 \cdots f_n$ be decomposition of f in $k[X]$, i.e. $c \in k^\times$ and $f_i \in k[X]$ irreducible for $1 \leq i \leq n$. We may assume that the f_i are primitive, hence contained in $R[X]$, since we can multiply them by suitable constants. We still have to show $c \in R$. Since $f \in k[X]$, i.e. $\nu_p(f) \geq 0$ we have

$$\nu_p(f) = \nu_p(c \cdot f_1 \cdots f_n) = \nu_p(c) + \sum_{i=1}^n \underbrace{\nu_p(f_i)}_{=0} = \nu_p(c) \stackrel{!}{\geq} 0$$

Thus $c \in R$. Then the decomposition from above is in R - but since f is irreducible in R , we have $n = 1$ and $c \in R^\times$. □

§ 9 Absolute values

Definition 9.1 Let k be a field. A map

$$|\cdot| : k \longrightarrow \mathbb{R}_{\geq 0}$$

is called an *absolute value*, if

- (i) *positive definiteness*: $|x| = 0 \iff x = 0$
- (ii) *multiplicativeness*: $|xy| = |x| \cdot |y|$ for all $x, y \in k$.
- (iii) *triangle inequality*: $|x + y| \leq |x| + |y|$ for all $x, y \in k$.

Example 9.2 (i) The 'normal' absolute value $|\cdot|_\infty$ on \mathbb{C} and on any of its subfields denotes an absolute value.

(ii) Let $\nu_k^\times \longrightarrow \mathbb{Z}$ be a discrete valuation, $\rho \in (0, 1)$. Then

$$|\cdot|_\nu : k \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} \rho^{\nu(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

is an absolute value on k , since

- (1) Trivial, since $|0| = 0$ and $\rho^x \neq 0$ for any $x \in \mathbb{Z}$.
- (2) Clearly $|xy|_\nu = \rho^{\nu(xy)} = \rho^{\nu(x)+\nu(y)} = \rho^{\nu(x)}\rho^{\nu(y)} = |x|_\nu|y|_\nu$.
- (3) Further

$$|x+y|_\nu = \rho^{\nu(x+y)} \leq \rho^{\min\{\nu(x), \nu(y)\}} = \max\{\rho^{\nu(x)}, \rho^{\nu(y)}\} = \max\{|x|_\nu, |y|_\nu\} \leq |x|_\nu + |y|_\nu$$

(iii) For the p -adic valuation ν_p on \mathbb{Q} we choose $\rho := \frac{1}{p}$. Then $|x|_p = p^{-\nu_p(x)}$ is an absolute value.

Remark + definition 9.3 Let k be a field, $|\cdot|$ an absolute value on k .

- (i) $|1| = |-1| = 1$ and $|x| = |-x|$ for all $x \in k$.
- (ii) The absolute value is called *trivial*, if $|x| = 1$ for all $x \in k$.

proof. We have $|1| = |1 \cdot 1| = |1| \cdot |1|$, hence $|1| = 1$. Moreover $|-1| = |1 \cdot (-1)| = |1| \cdot |-1|$, hence $|-1| = 1$. For $x \in k$ we have $|-x| = |(-1) \cdot x| = |-1| \cdot |x| = |x|$. \square

Proposition + definition 9.4 Let k be a field with $\text{char}(k) = 0$, i.e. $k \supseteq \mathbb{Q}$ and $|\cdot|$ an absolute value on k .

- (i) $|\cdot|$ is called *archimedean*, if $|n| > 1$ for all $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$.
- (ii) $|\cdot|$ is called *nonarchimedean*, if $|n| \leq 1$ for all $n \in \mathbb{Z}$.
- (iii) $|\cdot|$ is either archimedean or nonarchimedean.
- (iv) The p -adic absolute value on \mathbb{Q} is nonarchimedean.

proof of (iii). Since $|n| = |-n|$, it suffices to check $n \in \mathbb{N}$. Let $a \in \mathbb{N} \subseteq k$ with $|a| > 1$. Assume there exists $b \in \mathbb{N}_{>1}$ with $|b| \leq 1$. Write

$$a = \sum_{i=0}^N \alpha_i b^i \quad \alpha_i \in \{0, \dots, b-1\}, \quad |N| = \lfloor \log_b(a) \rfloor.$$

Then we have

$$|a| \leq \sum_{i=0}^{\lfloor \log_b(a) \rfloor} |\alpha_i| |b|^i \leq \log_b(a) \cdot \max_{0 \leq i \leq \lfloor \log_b(a) \rfloor} \{|\alpha_i|\} =: \log_b(a) \cdot c,$$

$$|a^n| \leq \log_b(a^n) \cdot c = n \cdot \log_b(a) \cdot c$$

and $|a^n|$ grows linearly in n . Likewise we get for $n \in \mathbb{N}$

$$a^n = \sum_{i=0}^{\lfloor \log_b(a^n) \rfloor} \alpha_i^{(n)} b^i, \quad \alpha_i^{(n)} \in \{0, \dots, b-1\},$$

$$|a^n| = |a|^n \leq (\log_b(a) \cdot c)^n$$

which grows exponentially in n , which is a contradiction. Hence the claim follows. \square

Remark 9.5 An absolute value $|\cdot|$ on a field k induces a metric

$$d(x, y) := |x - y|, \quad x, y \in k$$

Therefore, k as a topology and aspects as 'convergence' and 'cauchy sequences' are meaningful.

Definition + remark 9.6 (i) Two absolute values $|\cdot|_1, |\cdot|_2$ on k are called *equivalent*, if there exists $s \in \mathbb{R}$, such that $|x|_1 = |x|_2^s$ for all $x \in k$. In this case, we write $|\cdot|_1 \sim |\cdot|_2$.
(ii) Two absolute values $|\cdot|_1, |\cdot|_2$ are equivalent if and only if they induce the same topology on k .

proof. Is left for the reader as an exercise.

Example 9.7 The p -adic absolute values on \mathbb{Q} are not equivalent for $p \neq q \in \mathbb{P}$. Consider

$$|p^n|_p = p^{-n} \xrightarrow{n \rightarrow \infty} 0, \quad |p^n|_q = 1 \quad \text{for all } n \in \mathbb{N}$$

Moreover we have $|\cdot|_p \not\sim |\cdot|_\infty$, since by the transitivity of equivalence of absolute values, we have

$$|\cdot|_p \sim |\cdot|_\infty \sim |\cdot|_q$$

which is not true.

Theorem 9.8 (Ostrowski) Any nontrivial absolute value $|\cdot|$ on \mathbb{Q} is equivalent either to the standard absolute value $|\cdot|_\infty$ on \mathbb{Q} or to a p -adic absolute value $|\cdot|_p$ for some $p \in \mathbb{P}$.

proof. **case 1** Assume $|\cdot|$ is nonarchimedean. We want to show, that in this case $|\cdot| \sim |\cdot|_p$ for some $p \in \mathbb{P}$. Since $|\cdot|$ is non-trivial, there exists $x \in \mathbb{N}$ such that

$$|x| = \left| \prod_{p \in \mathbb{P}} p^{\nu_p(x)} \right| = \prod_{p \in \mathbb{P}} |p|^{\nu_p(x)} \neq 1$$

for at least one $x \in \mathbb{Q}$, hence, we have $|p| \neq 1$ for at least one $p \in \mathbb{P}$, i.e. $|p| < 1$. Assume there is another prime $q \neq p$ with $|q| < 1$. Then we find $N \in \mathbb{N}$, such that

$$|p|^N \leq \frac{1}{2}, \quad |q|^N \leq \frac{1}{2}.$$

Moreover, since p^N, q^N are coprime, we can write

$$1 = a \cdot p^N + b \cdot q^N \quad \text{for suitable } a, b \in \mathbb{Z}.$$

So the contradiction follows by

$$1 = |1| = |ap^N + bq^N| \leq \underbrace{|a|}_{\leq 1} \underbrace{|p^N|}_{< \frac{1}{2}} + \underbrace{|b|}_{\leq 1} \underbrace{|q^N|}_{< \frac{1}{2}} < 1,$$

hence we have $|q| = 1$ for any $q \neq p \in \mathbb{P}$. Let now $s := -\log_p |p|$. For $x \in \mathbb{Q}^\times$ we obtain

$$|x| = \left| \prod_{\tilde{p} \in \mathbb{P}} \tilde{p}^{\nu_{\tilde{p}}(x)} \right| = \prod_{\tilde{p} \in \mathbb{P}} |\tilde{p}|^{\nu_{\tilde{p}}(x)} = |p|^{\nu_p(x)} = p^{-s \cdot \nu_p(x)} = \left(p^{-\nu_p(x)} \right)^s = |x|_p^s$$

thus we have $|\cdot| \sim |\cdot|_p$.

case 2 Let now $|\cdot|$ be archimedean. We now have to show $|\cdot| \sim |\cdot|_\infty$. For $n \in \mathbb{N}_{\geq 2}$ we have

$$1 < |n| = \left| \sum_{i=1}^n 1 \right| \leq \sum_{i=1}^n |1| = n.$$

For any $a \in \mathbb{N}_{\geq 2}$ we find $s := s(a) \in \mathbb{R}_{<0}$ such that

$$|a| = |a|_\infty^s = a^s$$

namely

$$s = \log_a(|a|) = \frac{\log(|a|)}{\log(a)}.$$

Claim (a) We have

$$\frac{\log(|a|)}{\log(a)} = \frac{\log(|2|)}{\log(2)}.$$

Since now s is independent of a , we have $|\cdot| \sim |\cdot|_\infty$. Prove now the claim:

(a) For $n \in \mathbb{N}$ write

$$2^n = \sum_{i=0}^N \alpha_i a^i \quad \text{with } \alpha_i \in \{0, \dots, a-1\} \text{ and } N \leq \log_a 2^n = n \cdot \frac{\log(2)}{\log(a)}.$$

Then we have

$$|2|^n = |2^n| \leq \sum_{i=0}^N \underbrace{|\alpha_i|}_{\leq a} \overbrace{|a|^i}^{\leq a} \leq |a|^N \leq (N+1) \cdot a \cdot |a|^N,$$

hence we get

$$\begin{aligned} n \cdot \log(|2|) &\leq \log(N+1) + \log(a) + N \log(|a|) \\ &\leq \log\left(n \cdot \frac{\log(2)}{\log(a)} + 1\right) + \log(a) + n \cdot \frac{\log(2)}{\log(a)} \cdot \log(|a|). \end{aligned}$$

Multiplying the equation by $\frac{1}{n} \cdot \frac{1}{\log(2)}$ gives us

$$\frac{\log(|2|)}{\log(2)} \leq \frac{1}{n} \cdot \log\left(n \cdot \frac{\log(2)}{\log(a)} + 1\right) + \frac{\log(|a|)}{\log(a)}$$

and thus

$$\frac{\log(|2|)}{\log(2)} \leq \frac{\log(|a|)}{\log(a)}.$$

Swapping the roles of a and 2 in the equation above gives us the other inequality.

Hence we have equality, which proves the claim. \square

Proposition 9.9 *Let $|\cdot|$ be a nonarchimedean absolute value on a field k .*

- (i) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in k$.
- (ii) If $|x| \neq |y|$, then equality holds in (i).

proof. (i) If $x = 0$, we have $|y + x| = |y| \leq \max\{0, |y|\} = \max\{|x|, |y|\}$. Thus assume $x \neq 0$.

We have $|x + y| = |x| \left|1 + \frac{y}{x}\right|$. It suffices to show $|x + 1| \leq \max\{1, |x|\}$. Then we get

$$|x + y| = |y| \cdot \left|1 + \frac{x}{y}\right| \leq |y| \cdot \max\left\{\left|\frac{x}{y}\right|, |1|\right\} \leq \max\{|x|, |y|\}$$

For $n \in \mathbb{N}$ we have

$$(x + 1)^n = \sum_{k=0}^n \binom{n}{k} x^k.$$

Then we have

$$|x+1|^n = |(x+1)^n| = \left| \sum_{k=0}^n \binom{n}{k} x^k \right| \leq \sum_{k=0}^n \underbrace{\left| \binom{n}{k} \right|}_{\leq 1} \underbrace{|x|}_{\leq 1}^k \leq n+1,$$

hence

$$|x+1| \leq \sqrt[n]{n+1} \quad \text{for all } n \in \mathbb{N}.$$

Thus $|1+x| \leq 1$. Since we clearly have $|x+1| \leq |x|$, we all in all have

$$|x+1| \leq \max\{|x|, 1\}.$$

(ii) Let $z = x + y$ and assume $|x| < |y|$. We have to show $|z| = |y|$. Assume $|z| < |y|$. Then

$$|y| = |z - x| \stackrel{(i)}{\leq} \max\{|z|, |-x|\} < |y| \quad \nexists$$

and the proof is done. □

Proposition 9.10 *Let $|\cdot|$ be an a nonarchimedean absolute value on a field k . Then*

(i) *We have a local ring*

$$\overline{\mathcal{B}}_1(0) := \{x \in k \mid |x| \leq 1\} =: \mathcal{O}_k$$

with maximal ideal

$$\mathcal{B}_1(0) := \{x \in k \mid |x| < 1\} =: \mathfrak{m}_k$$

(ii) *Every point in ball is its center.*

(iii) *Balls are either disjoint or one of them is contained in the other one.*

(iv) *All triangles are isosceles.*

proof. (i) By 9.8(i), $\mathcal{B}_1(0)$ is closed under Addition. The remaining is calculating.

(ii) Let $z \in \overline{\mathcal{B}}_r(x)$. To show: $\overline{\mathcal{B}}_r(z) = \overline{\mathcal{B}}_r(x)$.

' \subseteq ' Let $y \in \overline{\mathcal{B}}_r(z)$, i.e. we have $|y - z| \leq r$. Then

$$|y - x| = |y - z + z - x| \leq \max\{|y - z|, |z - x|\} \leq r \quad \Rightarrow \quad y \in \overline{\mathcal{B}}_r(x).$$

Thus we have $\overline{\mathcal{B}}_r(z) \subseteq \overline{\mathcal{B}}_r(x)$.

' \supseteq ' Follows by symmetry.

(iii) Let $\mathcal{B} := \overline{\mathcal{B}}_r(x)$, $\mathcal{B}' := \overline{\mathcal{B}}_{r'}(x')$ and $y \in \mathcal{B} \cap \mathcal{B}'$. W.l.o.g. $r \leq r'$.

Then for $z \in \mathcal{B}$ we have

$$|z - x'| = |z - x + x - y + y - x'| \leq \max\{|z - x|, |x - y|, |y - x'|\} = \max\{r, r, r'\} = r'$$

which implies $z \in \mathbb{B}'$. Hence we have $\mathcal{B} \subseteq \mathcal{B}'$.

(iv) Follows from 9.8(ii). □

Corollary 9.11 *Let k be a field, $|\cdot|$ a nonarchimedean absolute value on k .*

- (i) *All balls are closed and open, considering the topology on k induced by the metric $d(x, y) = |x - y|$.*
- (ii) *k is totally disconnected, i.e. no subset of k containing more than one element is connected.*

proof. (i) Let $\mathcal{B} := \overline{\mathcal{B}}_r(x)$ be a closed ball for some $x \in k$, $r \in \mathbb{R}_{\geq 0}$. Then \mathcal{B} topologically clearly is closed. Let now $y \in \mathcal{B}$. Then $\mathcal{B}_r(y) \subseteq \mathcal{B}$ by 9.9(ii), i.e. \mathcal{B} is open.

Let now $\mathcal{B} := \mathcal{B}_r(x)$ be an open ball and $y \in k$ a boundary point. Thus for all $s > 0$ we find $z \in \mathcal{B}_s(x) \cap \mathcal{B}_r(x)$. Choose $s \leq r$. Then

$$d(x, y) \leq \max\{d(y, z), d(x, z)\} < \max\{s, r\} = r.$$

Thus $y \in \mathcal{B}_r(x)$, hence $\mathcal{B}_r(x)$ contains its boundary and is closed.

(ii) Let $X \subseteq k$ be a subset with $x \neq y \in X$. Then for $r := |x - y| > 0$ we get

$$X = \left(\overline{\mathcal{B}}_{\frac{r}{2}}(x) \cap X \right) \cup \left(X \setminus \overline{\mathcal{B}}_{\frac{r}{2}}(x) \right)$$

which is a decomposition of X into two nonempty, disjoint open subset, i.e. the claim follows.

Example 9.12 (*Geometry on $(\mathbb{Q}, |\cdot|_p)$*) The unit disc in $(\mathbb{Q}, |\cdot|_p)$ is

$$\left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\} =: \mathbb{Z}_{(p)}$$

The maximal ideal is

$$\left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b, p \mid a \right\} = p \cdot \mathbb{Z}_{(p)} = \overline{\mathcal{B}}_{\frac{1}{p}}(0)$$

We have

$$\{x \in \mathbb{Q} \mid |x|_p < 1\} = \left\{ x \in \mathbb{Q} \mid |x|_\infty < \frac{1}{p} \right\}$$

Moreover

$$\mathbb{Z}_{(p)} / p\mathbb{Z}_{(p)} \cong \mathbb{Z} / p\mathbb{Z} = \mathbb{F}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$$

$\overline{\mathcal{B}}_1(0)$ is the disjoint union of the $\overline{\mathcal{B}}_{\frac{1}{p}}(i)$ for $0 \leq i \leq p-1$, where $\overline{\mathcal{B}}_{\frac{1}{p}}(i) = i + p\mathbb{Z}_{(p)}$.

§ 10 Completions, p -adic numbers and Hensel's Lemma

Remark 10.1 Let $|\cdot|$ be an absolute value on a field k . Let

$$\mathcal{C} := \{(a_n)_{n \in \mathbb{N}} \mid (a_n) \text{ is Cauchy sequence in } (k, |\cdot|)\}$$

be the ring (!) of Cauchy sequences in k and

$$\mathcal{N} := \left\{ (a_n)_{n \in \mathbb{N}} \mid \lim_{n \rightarrow \infty} a_n = 0 \right\} \trianglelefteq \mathcal{C}$$

the ideal (!) of Cauchy sequences converging to 0. Then

- (i) \mathcal{N} is a maximal ideal.
- (ii) $k' := \mathcal{C}/\mathcal{N}$ is a field extension of k .
- (iii) $|\overline{(a_n)_{n \in \mathbb{N}}}| := \lim_{n \rightarrow \infty} |a_n| \in \mathbb{R}_{\geq 0}$ is an absolute value on k' extending $|\cdot|$.
- (iv) k' is complete with respect to $|\cdot|$.

Remark 10.2 If $|\cdot|$ is nonarchimedean, for every Cauchy sequence $(a_n)_{n \in \mathbb{N}} \notin \mathcal{N}$ we have $|a_m| = |a_n|$ for all $m, n \gg 0$.

proof. Since $(a_n) \notin \mathcal{N}$, 0 is not an accumulation point of (a_n) . $\implies |a_n| \geq \epsilon$ for some $\epsilon > 0$ and all $n \geq n_0(\epsilon) =: n_0$. Thus for $n, m \geq n_0$ we have $|a_n - a_m| < \epsilon$. This implies by 9.8 (ii)

$$|a_n - a_m| \leq \max\{|a_n|, |a_m|\} \implies |a_n| = |a_m|,$$

which was the claim. □

Definition 10.3 Let $k = \mathbb{Q}$, $|\cdot| = |\cdot|_p$ for some $p \in \mathbb{P}$. Then the field k' on 10.1 is called the field of p -adic numbers and denoted by \mathbb{Q}_p . The valuation ring is called the ring of p -adic integers and is denoted by \mathbb{Z}_p .

Remark 10.4 (i) $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$.

(ii) The maximal ideal in \mathbb{Z}_p is $p\mathbb{Z}_p$.

(iii) $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

(iv) \mathbb{Z}_p is a discrete valuation ring.

proof. (i) The first inclusion is clear. For the second one consider $x = \frac{r}{s} \in \mathbb{Z}_{(p)}$. Then by definition of localization we have $p \nmid s$ and hence

$$|x| = \left| \frac{r}{s} \right| = \frac{|r|}{|s|} = |r| \leq 1$$

and thus $x \in \mathbb{Z}_p$. Now prove that \mathbb{Z} is dense in \mathbb{Z}_p : Let $x \in \mathbb{Z}_p$ with p -adic expansion

$$x = \sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \{0, 1, \dots, p-1\}.$$

Define a sequence $(x_n)_{n \in \mathbb{N}}$ by

$$x_n := \sum_{i=0}^n a_i p^i \in \mathbb{Z}.$$

Then we have

$$|x - x_n| = \left| \sum_{i=n+1}^{\infty} a_i p^i \right| = \max_{i \geq n+1} \{|p^i|\} = |p^{n+1}| = p^{-(n+1)} \xrightarrow{n \rightarrow \infty} 0$$

and hence \mathbb{Z} is dense in \mathbb{Z}_p .

(ii) Recall that the maximal ideal is given by

$$\mathfrak{m} = \{x \in \mathbb{Z}_p \mid |x| < 1\} \stackrel{!}{=} p\mathbb{Z}_p$$

' \subseteq ' Let $x \in \mathfrak{m}$, i.e. $|x| < 1$. Thus we have $|x| < |\frac{1}{p}|$. This implies

$$|p^{-1}x| \leq 1 \iff p^{-1}x \in \mathbb{Z}_p.$$

and thus $p^{-1}x = y$ for some $y \in \mathbb{Z}_p$. Then we have $x = py \in p\mathbb{Z}_p$.

' \supseteq ' Let $x \in p\mathbb{Z}_p$, i.e. we can write $x = py$ for some $y \in \mathbb{Z}_p$. Then $|x| = |py| = |p||y| < 1$ and hence $x \in \mathfrak{m}$.

(iii) Consider the surjective homomorphism

$$\psi_p : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad x = \sum_{i=0}^n a_i p^i \mapsto a_0.$$

We have

$$\ker(\psi_p) = \{x \in \mathbb{Z}_p \mid a_0 \equiv 0 \pmod{p}\} = p\mathbb{Z}_p,$$

thus we get $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ by homomorphism theorem.

(iv) The absolute value $|\cdot| = |\cdot|_p$ on \mathbb{Q}_p induces a discrete valuation ν on \mathbb{Q}_p^\times . With respect to this valuation we have

$$\mathcal{O}_\nu = \{x \in \mathbb{Q}_p \mid \nu(x) \geq 0\} \cup \{0\} = \{x \in \mathbb{Q}_p \mid |x| \leq 1\} = \mathbb{Z}_p,$$

which finishes the proof. □

Proposition 10.5 (i) Any $x \in \mathbb{Z}_p$ can uniquely be written in the form

$$x = \sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \{0, 1, \dots, p-1\}.$$

(ii) Any $x \in \mathbb{Q}_p$ can uniquely be written in the form

$$x = \sum_{i=-m}^{\infty} a_i p^i, \quad m \in \mathbb{Z}, \quad a_i \in \{0, 1, \dots, p-1\}, \quad a_m \neq 0.$$

proof. (i) We first obtain, that any series

$$\sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \{0, \dots, p-1\}$$

converges, since for $n > m$ we have

$$\left| \sum_{i=0}^n a_i p^i - \sum_{i=0}^m a_i p^i \right| = \left| \sum_{i=n+1}^m a_i p^i \right| = |p^{m+1}| \underbrace{\left| \sum_{i=n+1}^m a_i p^{i-(m+1)} \right|}_{\leq 1} \leq |p^{m+1}|.$$

uniqueness Let

$$x = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} b_i p^i, \quad a_i, b_i \in \{0, 1, \dots, p-1\}$$

representations of $x \in \mathbb{Q}_p$. Assume them to be different and define $i_o := \min\{i \in \mathbb{N}_0 \mid a_i \neq b_i\}$. Then

$$0 = \left| \sum_{i=0}^{\infty} a_i p^i - \sum_{i=0}^{\infty} b_i p^i \right| = \left| \underbrace{p^{i_o}(a_{i_o} - b_{i_o})}_{=:A} + p^{i_o+1} \cdot \underbrace{\left(\sum_{i=i_o+1}^{\infty} a_i p^{i-(i_o+1)} - \sum_{i=i_o+1}^{\infty} b_i p^{i-(i_o+1)} \right)}_{=:B} \right|.$$

We obtain $\nu_p(A) = p^{-i_o}$ and

$$B \in \mathbb{Z}_p, \quad \nu_p(p^{i_o+1} \cdot B) = \nu_p(p^{i_o+1}) \underbrace{\nu_p(B)}_{\leq 1} \leq \nu_p(p^{i_o+1}) = p^{-(i_o+1)},$$

so all in all

$$0 = |A + p^{i_o+1} \cdot B| \stackrel{9.8(ii)}{=} \max\{p^{-i_o}, p^{-(i_o+1)}\} = p^{-i_o} \not=.$$

existence Look at $\bar{x} \in \mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{F}_p$.

Let a_0 be the representative of x in $\{0, 1, \dots, p-1\}$. Then we have

$$|x - a_0| < 1 \Leftrightarrow |x - a_0| \leq \frac{1}{p}.$$

In the next step, let a_1 be the representative of $\frac{1}{p}(x - a_0)$ in $\{0, 1, \dots, p-1\}$. Then

$$\left| \frac{1}{p}(x - a_0) - a_1 \right| = \left| \frac{1}{p} \right| |x - a_0 - a_1 p| \leq \frac{1}{p}$$

and thus $|x - a_0 - a_1 p| \leq \frac{1}{p^2}$. Inductively we let a_n be the representative of

$$\frac{1}{p^n}(x - a_0 - a_1 p - \dots - a_{n-1} p^{n-1}) = \frac{1}{p^n} \left(x - \sum_{i=0}^{n-1} a_i p^i \right)$$

in $\{0, 1, \dots, p-1\}$. Then we have

$$\left| x - \sum_{i=0}^{n-1} a_i p^i \right| \leq \frac{1}{p^{n+1}}.$$

and finally

$$\lim_{n \rightarrow \infty} \left| x - \sum_{i=0}^{n-1} a_i p^i \right| \leq \lim_{n \rightarrow \infty} \frac{1}{p^{n+1}} = 0 \implies x = \sum_{i=0}^{\infty} a_i p^i.$$

(ii) If $|x| = p^m$ for some $m \in \mathbb{Z}$, we have

$$|x \cdot p^m| = |d| \cdot |p^m| = p^m \cdot p^{-m} = 1, \quad \text{i.e. } x \cdot p^m \in \mathbb{Z}_p^\times$$

By part (i) we conclude

$$x \cdot p^m = \sum_{i=0}^{\infty} a_i p^i, \quad a_0 \neq 0.$$

Thus we have

$$x = \frac{1}{p^m} \cdot x \cdot p^m = \frac{1}{p^m} \cdot \sum_{i=0}^{\infty} a_i p^i = \sum_{i=-m}^{\infty} a_{i+m} p^i,$$

which was the assertion. □

Remark 10.6 What is -1 in \mathbb{Q}_p ? We have $a_0 = p-1$, since $\overline{p-1} - \overline{(-a)} = \bar{p} = 0$. a_1 is the representative of $\frac{1}{p}(-1 - (p-1)) = -1$, i.e. $a_1 = p-1$. a_2 is the representative of $\frac{1}{p^2}(-1 - (p-1) - (p-1)p) = -1$, i.e. $a_2 = p-1$. Inductively we have $a_n = p-1$ for all $n \in \mathbb{N}_0$, so we get

$$-1 = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} (p-1) p^i.$$

Moreover we obtain

$$\sum_{i=0}^{\infty} (p-1) p^i = (p-1) \sum_{i=0}^{\infty} p^i = (p-1) \cdot \frac{1}{1-p} = \frac{p-1}{1-p} = -1.$$

Remark 10.7 *Let*

$$x = \sum_{i=0}^{\infty} a_i p^i, \quad y = \sum_{i=0}^{\infty} b_i p^i$$

p -adic integers. Then

$$x + y = \sum_{i=0}^{\infty} c_i p^i$$

with coefficients

$$c_0 = \begin{cases} a_0 + b_0 & \text{if } a_0 + b_0 < p \\ a_0 + b_0 - p & \text{if } a_0 + b_0 \geq p \end{cases}$$

$$c_1 = \begin{cases} a_1 + b_1 & \text{if } a_0 + b_0 < p \text{ and } a_1 + b_1 < p \\ a_1 + b_1 - p & \text{if } a_0 + b_0 < p \text{ and } a_1 + b_1 \geq p \\ a_1 + b_1 + 1 & \text{if } a_0 + b_0 \geq p \text{ and } a_1 + b_1 + 1 < p \\ a_1 + b_1 + 1 - p & \text{if } a_0 + b_0 \geq p \text{ and } a_1 + b_1 + 1 \geq p \end{cases}$$

Inductively let

$$\epsilon_0 := 0, \quad \epsilon_i := \begin{cases} 0 & \text{if } a_i + b_i + \epsilon_{i-1} < p \\ 1 & \text{if } a_i + b_i + \epsilon_{i-1} \geq p \end{cases} \quad \text{for } i \geq 1$$

Then we have

$$c_i = \begin{cases} a_i + b_i + \epsilon_i & \text{if } a_i + b_i + \epsilon_i < p \\ a_i + b_i + \epsilon_i - p & \text{if } a_i + b_i + \epsilon_i \geq p \end{cases}$$

Remark 10.8 (i) $\sqrt{p} \notin \mathbb{Q}_p$, since $|\sqrt{p}| = \sqrt{|p|} = \sqrt{\frac{1}{p}} \in \left(\frac{1}{p}, 1\right)$, which is not possible.

(ii) Let $a \in \mathbb{Z}_p^\times$ with image $\bar{a} \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$, where

$$\mathbb{F}_p^{\times 2} = \{x \in \mathbb{F}_p \mid \text{there exists } y \in \mathbb{F}_p : y^2 = x\}$$

denotes the set of squares. Then $\sqrt{a} \notin \mathbb{Q}_p$. Assume a is a square, i.e. $b^2 = a$. Then

$$|b| = \sqrt{|a|} = 1 \quad \Rightarrow \quad b \in \mathbb{Z}_p^\times$$

But then $\bar{b} \in \mathbb{F}_p$ satisfies $\bar{b}^2 \equiv a$, which is a contradiction, since $a \notin \mathbb{F}_p^{\times 2}$.

(iii) Let now $\overline{\mathbb{Q}}_p$ be the algebraic closure of \mathbb{Q}_p with valuation ring $\overline{\mathbb{Z}}_p$ and maximal ideal $\overline{\mathfrak{m}}_p$. Then $\overline{\mathbb{Z}}_p / \overline{\mathfrak{m}}_p$ is algebraically closed. Moreover \mathbb{Q}_p is complete with respect to $|\cdot|_p$. The completion \mathbb{C}_p of $\overline{\mathbb{Q}}_p$ is complete and algebraically closed, but:

- (1) $|\cdot|_p$ is not a discrete valuation.
- (2) $\overline{\mathbb{Z}}_p$ is not a discrete valuation ring.
- (3) $\overline{\mathfrak{m}}_p$ is not a principal ideal.

Theorem 10.9 (*Hensel's Lemma*) *Let*

$$f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}_p[X], \quad \bar{f} = \sum_{i=0}^n \bar{a}_i X^i \in \mathbb{F}[X]$$

where \bar{f} is the reduction of f in $\mathbb{F}[X]$. Suppose that $\bar{f} = f_1 \cdot f_2$ with $f_1, f_2 \in \mathbb{F}_p[X]$ relatively prime. Then there exist $g, h \in \mathbb{Z}_p[X]$, such that

$$f = g \cdot h, \quad \bar{g} = f_1, \bar{h} = f_2, \quad \deg(f_1) = \deg(g)$$

proof. Let $d := \deg(f), m := \deg(f_1)$. Then $\deg(f_2) \leq d - m$. Choose $g_0, h_0 \in \mathbb{Z}_p[X]$ such that $\bar{g}_0 = f_1, \bar{h}_0 = f_2, \deg(g_0) = m, \deg(h_0) = d - m$. *Strategy:* Find $g_1 = g_0 + pc_1, h_1 = h_0 + pd_1$ with some $c_1, d_1 \in \mathbb{Z}_p[X]$, such that

$$f - g_1 h_1 \in p^2 \mathbb{Z}_p[X].$$

Therefore we have a

Claim (a) For $n \geq 1$ there exists $c_n, d_n \in \mathbb{Z}_p[X]$ with $\deg(c_n) \leq m, \deg(d_n) \leq d - m$ and

$$f - g_n h_n \in p^{n+1} \mathbb{Z}_p[X], \quad \text{where } g_n = g_{n-1} + p^n c_n, \quad h_n = h_{n-1} + p^n d_n.$$

Assuming (a), write

$$g_n = \sum_{i=0}^m g_{n,i} X^i, \quad h_n = \sum_{i=0}^{d-m} h_{n,i} X^i.$$

By construction, the $(g_{n,i})$ converge to some $\alpha_i \in \mathbb{Z}_p$ and the $(h_{n,i})$ converge to some $\beta_i \in \mathbb{Z}_p$.

Let

$$g := \sum_{i=0}^m \alpha_i X^i, \quad h := \sum_{i=0}^{d-m} \beta_i X^i.$$

Observe, that $\deg(g) = m, \deg(h) = d - m$. Obviously we have

$$f = g \cdot h.$$

It remains to show the claim.

(a) c_n, d_n have to satisfy

$$\begin{aligned} f - g_n h_n &= f - (g_{n-1} + p^n c_n) \cdot (h_{n-1} + p^n d_n) \\ &= f - g_{n-1} h_{n-1} - p^n \cdot (g_{n-1} d_n + h_{n-1} c_n + p^n c_n d_n) \\ &\stackrel{!}{\in} p^{n+1} \mathbb{Z}_p[X] \end{aligned}$$

where $f - g_{n-1}h_{n-1} \in p^n\mathbb{Z}_p[X]$ by hypothesis. We get

$$\tilde{f}_n := \frac{1}{p^n}(f - g_{n-1}h_{n-1}) \equiv c_nh_{n-1} + d_ng_{n-1} \pmod{p} (*)$$

Since f_1, f_2 are relatively prime and $g_j \equiv g_k \pmod{p}$ for any j, k , we find integers $a, b \in \mathbb{Z}$, such that

$$af_1, bf_2 = 1 \implies ag_{n-1} + bh_{n-1} \equiv 1 \pmod{p}.$$

Multiplying the equation by \tilde{f}_n gives us

$$\tilde{f}_n \equiv \underbrace{a\tilde{f}_n}_{=: \tilde{d}_n} g_{n-1} + \underbrace{b\tilde{f}_n}_{=: \tilde{c}_n} h_{n-1} \pmod{p} (**).$$

Further $\mathbb{Z}_p[X]$ is euclidean, thus we can choose $q_n, r_n \in \mathbb{Z}_p[X]$, $\deg(r_n) < m$ such that

$$b\tilde{f}_n = q_ng_{n-1} + r_n.$$

By (**) we have

$$g_{n-1}(a\tilde{f}_n + q_nh_{n-1}) + r_n \equiv \tilde{f}_n \pmod{p}.$$

Let now $c_n = r_n, d_n = a\tilde{f}_n + q_nh_{n-1}$. All the terms are divisible by p . Then

$$d_n \equiv a\tilde{f}_n + q_nh_{n-1} \pmod{p}.$$

Thus (*) holds and we have

$$\deg(d_n) = \deg(\overline{d_n}) \leq \deg \left(\underbrace{\overline{\tilde{f}_n} - \overline{\tilde{c}_n} \overline{h_{n-1}}}_{\leq d} \right) - \underbrace{\deg(\overline{g_{n-1}})}_{=m} \leq d - m$$

since $\overline{d_n} \overline{g_{n-1}} = \overline{\tilde{f}_n} - \overline{\tilde{c}_n} \overline{h_{n-1}}$. Thus, the claim is proved. \square

Corollary 10.10 *Let $p \in \mathbb{P}$ odd. Then $a \in \mathbb{Z}_p^\times$ is a square if and only if $\bar{a} \in \mathbb{F}_p^\times$ is a square.*

Proposition 10.11 *$a \in \mathbb{Q}$ is a square if and only if $a > 0$ and a is a square in \mathbb{Q}_p for all $p \in \mathbb{P}$.*

Remark: This is a special case of the 'Hasse-Minkowski-Theorem'.

