

A course on number theory II

Discrete Valuation Ring

$$K, R(v) = \{\alpha \in K \mid v(\alpha) \leq 1\}$$

$$v \text{ valuation: } K \longrightarrow \mathbb{R}^+$$

If $v(K^*) \subset \mathbb{R}^+$ is discrete, then $R(v)$ is called a DVR.

Completion

Def K : field, v : valuation, $d(x, y) = v(x - y)$ metric

K : complete if every Cauchy sequence in K converges to an element of K .

$$K \hookrightarrow \hat{K} = \{\text{Cauchy sequences}\} / \mathcal{N}$$

with $\mathcal{N} = \{\text{null sequences}\}$

$$\hat{v}(\{a_n\} + \mathcal{N}) = \lim_{n \rightarrow \infty} v(a_n)$$

\hat{K} is complete w.r.t \hat{v} .

L/K : finite extension of degree n .

\hookrightarrow complete w.r.t. non-Archimedean valuation v

R : DVR

$\Rightarrow \exists!$ extension v' of v to L s.t.

$$L \text{ complete w.r.t } v', \quad v'(y) = v(N_{L/K}(y))^{1/n} \quad \forall y \in L$$

valuation ring R' for v' is DVR.

k : number field.

v : Archimedean $k_v \cong \mathbb{R}$ or \mathbb{C}

v_p : non-Archimedean $k_{v_p} \cong k_p$: p -adic field

R_p (DVR) is called the ring of p -adic integers.

ex) \mathbb{Q} , (∞ place: \mathbb{R})

finite places: $\mathbb{Q}_p = \left\{ \sum_{i \geq n} a_i p^i \mid 0 \leq a_i < p-1 \right\}$
for some integer n

\mathbb{Z}_p : p -adic integers.

ℓ/k number fields, $n = [\ell:k]$

$$\bigcup \mathcal{P}_\ell = \mathcal{O}_1^{e_1} \mathcal{O}_2^{e_2} \dots \mathcal{O}_g^{e_g}$$

$$\ell_{\mathcal{O}_i} \mid k_p, \quad f_i = [R_\ell / \mathcal{O}_i : R_k / \mathcal{P}], \quad n_i = e_i f_i$$

Hensel's Lemma

R_p ring of p -adic integers

the residue field $\bar{k} = R_p / \pi R_p \cong R(\mathcal{V}_p) / \mathcal{P}(\mathcal{V}_p)$

(π is called a uniformiser.) \mathcal{P} maximal ideal of R_p

Let $f(x)$ be a monic polynomial in $R_p[x]$

such that $\bar{f}(x) = \bar{g}(x) \bar{h}(x)$ where $\bar{g}, \bar{h} \in \bar{k}[x]$ are relatively prime polynomials.

Then $\exists g, h \in R_p[x]$ s.t. $g, h \pmod{\pi R_p} = \bar{g}, \bar{h}$
 $f = gh, \deg g = \deg \bar{g}, \deg h = \deg \bar{h}$.

Theorem k_p has a unique unramified quadratic extension $L = k_p(\sqrt{u})$ where $u \in R_p^*$.

$R_p^* \subset N_{L/k_p}(R_L) & k_p^* / N_{L/k_p}(L^*)$ has order 2 with cosets represented by 1 and $\pi \leftarrow$ uniformiser.

Adèles & Idèles

k_p , $\{a + \pi^n R_p : n \geq 0\}$: fundamental system of neighbourhoods of a

k_p^+ locally compact $\supset R_p$ is compact

k_p^* " $\supset R_p^*$ is compact

$$A_{\mathbb{Z}} = \mathbb{R} \times \prod_p \mathbb{Z}_p$$

$$A_{\mathbb{Q}} = \mathbb{Q} \otimes A_{\mathbb{Z}}$$

Idèle group $A_k^* \subset A_k = k \otimes_{\mathbb{Z}} A_{\mathbb{Z}}$: Adèles ring

Note A_k^* doesn't have an induced topology

Quadratic Forms

Def V finite-dimensional vector space / K

$B : V \times V \rightarrow K$ symmetric bilinear map

(V, B) : quadratic space

A quadratic map $q(v) = B(v, v)$

$$2B(v, w) = q(v+w) - q(v) - q(w)$$

$\{v_1, \dots, v_n\}$: basis of V

$$\text{quadratic form : } q(x_1, \dots, x_n) = \sum_{i,j} B(v_i, v_j) x_i x_j$$

with associated symmetric matrix $M = [B(v_i, v_j)]$

Two quadratic forms with associated matrices M, M' are equivalent

$$\Leftrightarrow \exists \text{ non-singular } X \in GL(n, K) \text{ s.t. } M' = X^t M X$$

$$\Leftrightarrow \text{associated quadratic spaces } (V, B), (V', B') \text{ are isometric}$$

(i.e. K -linear isomorphism $\tau: V \rightarrow V'$ s.t.

$$B'(\tau(v), \tau(w)) = B(v, w) \quad \forall v, w \in V.)$$

(V, B) is regular if

• $V \rightarrow V^*$ is an isomorphism $v \mapsto B(-, v)$

(or, • quadratic form q with matrix M

M is nonsingular)

The orthogonal complement

$W \subset V$ subspace

$$W^\perp = \{v \in V \mid B(v, w) = 0 \quad \forall w \in W\}$$

(If (V, B) regular $\Rightarrow (W^\perp)^\perp = W$

$$W \oplus W^\perp = V)$$

$$V = W_1 \perp W_2 \iff W_1 \oplus W_2 = V \quad \&$$

W_1 is orthogonal to W_2

(i.e. $B(w_1, w_2) = 0 \quad \forall w_1 \in W_1, w_2 \in W_2$)

\exists orthogonal basis v_1, \dots, v_n

\Rightarrow associated matrix M is diagonal

$$V = \langle v_1 \rangle \perp \langle v_2 \rangle \perp \dots \perp \langle v_n \rangle$$

$(V_1, B_1), (V_2, B_2)$ orthogonal sum $(V_1 \perp V_2, B)$

$$B((v_1, v_2), (v_1', v_2')) = B_1(v_1, v_1') + B_2(v_2, v_2')$$

$0 \neq v \in V$ is called isotropic if $q(v) = 0$

(V, B) is isotropic if \exists isotropic v

anisotropic otherwise

invariant

(V, B) regular quadratic space

determinant = $\det(M) (K^*)^2 \in K^*/(K^*)^2$
 \uparrow matrix w.r.t. the basis of V

$L|K$ extension

$(V, B)/K \Rightarrow (V \otimes L, B)$
 quadratic space quadratic space/ L

(V, B) regular quadratic space/ \mathbb{k} \leftarrow number field

\mathbb{k}_v : completion for a place v .

$\mathbb{k}_v = \mathbb{C}$ regular quadratic spaces are classified
 by $\dim V$ (up to isometry)

\mathbb{R} classified by \dim & signature

p -adic field \mathbb{k}_p is dyadic if $N(p) = 2^r$
 non-dyadic otherwise

$(V, B) \quad V = V_1 \perp V_2$

$q \quad q = q_1 \perp q_2$

$q_1(x_1, \dots, x_r) = \sum d_i x_i^2, \quad (d_i \in \mathbb{R}_p^*)$

$q_2(x_{r+1}, \dots, x_m) = \sum d'_i x_i^2, \quad (d'_i \in \mathbb{R}_p^*)$

anisotropic over \mathbb{k}_p

$\Leftrightarrow (\overline{V}_1, \overline{q}_1), (\overline{V}_2, \overline{q}_2)$ are both anisotropic over $\overline{\mathbb{k}}$.

Hasse-Minkowski Theorem

(V, B) isotropic over \mathbb{k}

$\Leftrightarrow V$ isotropic over all $\mathbb{k}_v \quad \forall$ places v .

Def (Orthogonal group)

$(V, B) \quad O(V, B) = O(V) = \{ T: V \rightarrow V \mid T \text{ is an isometry} \}$

$\mathcal{B} = \{v_1, \dots, v_n\}$ basis

$$GL(n, K) \supset O_{\mathcal{B}}(V) = \{T \in GL(n, K) \mid T^t M T = M\}$$

$$SO(V) = \{T \in O(V) \mid \det T = 1\} \quad [B(v_1, v_2)]$$

Fact $O(V, B)$ is generated by the reflections

For any anisotropic vector $v \in V$,

$$\text{reflection } \tau_v : V \rightarrow V \\ x \mapsto x - \frac{2B(x, v)}{q(v)} v$$

Quaternion Algebra

Def (F : field of characteristic $\neq 2$)

A quaternion algebra A/F is 4-dimensional F -space, basis vectors $1, i, j, k$

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k \quad \text{for some } a, b \in F^*$$

Hilbert symbol. $\left(\frac{a, b}{F}\right)$

$$\text{ex) } \mathcal{H} = \left(\frac{-1, -1}{\mathbb{R}}\right)$$

$$M_2(F) = \left(\frac{1, -1}{F}\right) \quad i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Properties

$$1. \left(\frac{a, b}{F}\right) \cong \left(\frac{ax^2, by^2}{F}\right) \quad \forall x, y, a, b \in F^*$$

$$2. Z(A) = \{x \in A \mid xy = yx \quad \forall y \in A\} = F$$

$$3. \left(\frac{a, b}{F}\right) \text{ is a simple algebra}$$

(i.e. no proper two-sided ideals)

$$\therefore A = \text{central simple algebra}$$

Def. $A = \left(\frac{a, b}{F}\right)$ $\{1, i, j, k\}$ standard basis J .

$A_0 \subset A$ subspace spanned by $\{i, j, k\}$

Elements in A_0 is called the pure quaternions.

$\forall x \in A, x = a + \alpha, a, \alpha$ unique.

$a \in F = Z(A), \alpha \in A_0$

Def. The conjugate $\bar{x} = a - \alpha$

$$\overline{x+y} = \bar{x} + \bar{y}, \quad \overline{xy} = \bar{y}\bar{x},$$

$$\overline{\bar{x}} = x, \quad r\bar{x} = \bar{r}x \quad \forall r \in F.$$

ex $M(2, F)$ $\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

(reduced) norm $n(x) = x\bar{x}$

(") trace $\text{tr}(x) = x + \bar{x}$

x invertible if $n(x) \neq 0$.

$$A^* = \{x \in A \mid \frac{\bar{x}}{n(x)}, x \text{ invertible}\}$$

$$A' = \{x \in A^* \mid n(x) = 1\}$$

Properties. Every 4-dimensional central simple algebra $/F$ is a quaternion algebra.

Wedderburn's structure theorem

If $A \not\cong M(2, F)$ then A is a division algebra.

Orders in Quaternion algebra.

Def V : vector space / k

R -lattice $L \subset V$: finitely generated R -module
in V .

complete R -lattice: $L \otimes_R k \cong V$.

$\alpha \in A$ is an integer over R

if $R[\alpha]$ is an R -lattice in A .

An ideal $I \subset A$ is a complete R -lattice.

Order \mathcal{O} is an ideal ring with 1

\mathcal{O} is maximal if it is maximal with
respect to inclusion.

ex) $A = \left(\frac{-1, 3}{\mathbb{Q}} \right)$, $\alpha = j$, $\beta = \frac{3j+4ij}{5}$

$A = M_2(k)$ R : PID

then all maximal orders are conjugate.