Quadratic Forms

Marco Schlichting
Notes by Florian Bouyer

26th October 2012

Contents

In this course every ring is commutative with unit. Every module is a left module.

Definition 0.1. Let R be a (commutative) ring and M a (left) R-module. Then a *bilinear form on* M is a map $\beta : M \times M \to R$ which is R-linear in both variables. i.e. $\beta(ax+by,z) = a\beta(x,z)+b\beta(y,z)$ and $\beta(x,by+cz) = b\beta(x,y)+c\beta(x,z)\ \forall x,y,z \in M, a,b,c \in R$

Example. Standard Euclidean scalar product on $\mathbb{R}^n$. $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ is a bilinear form on the $\mathbb{R}$-module $\mathbb{R}^n$

Definition 0.2. A bilinear form $\beta : M \times M \to R$ is called *symmetric* if $\beta(x,y) = \beta(y,x)\ \forall x,y \in M$. It is called *skewed symmetric* if $\beta(x,y) = -\beta(y,x)\,\forall x,y \in M$. It is called *symplectic* if $\beta(x,x) = 0\,\forall x \in M$

Example. Standard scalar product on $\mathbb{R}^n$ is symmetric.
On $\mathbb{R}^2$ the bilinear form $(x_1,y_1) \times (x_2,y_2) \mapsto x_1y_2 - x_2y_1$ is symplectic and skew-symmetric

Remark. Any symplectic bilinear form is also skew-symmetric because β symplectic $\Rightarrow 0 = \beta(x+y,x+y) = \beta(x,x)+\beta(x,y)+\beta(y,x)+\beta(y,y) = \beta(x,y)+\beta(y,x)$ hence it is skew-symmetric.

If $2 \in R$ is a non-zero divisor (i.e. $2a = 0 \Rightarrow a = 0\,\forall a \in R$) then any skew-symmetric form is also symplectic because β skew-symmetric $\Rightarrow \beta(x,x) = -\beta(x,x) \Rightarrow 2\beta(x,x) = 0$ and 2 a non-zero divisors we can divide by 2 hence $\beta(x,x) = 0\,\forall x \in M \Rightarrow \beta$ symplectic

Example. For $R = \mathbb{F}_2$, the form $\mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$ defined by $x,y \mapsto xy$ is skewed-symmetric but not symplectic because $\beta(1,1) = 1 \neq 0 \in \mathbb{F}_2$

Definition 0.3. A bilinear form $\beta : M \times M \to R$ is called *regular or non-degenerate or non-singular* if

1. $\forall f : M \to R$ a R-linear map $\exists x_0, y_0 \in M$ such that $f(x) = \beta(x_0,x)$ and $f(x) = \beta(x,y_0)$
2. $\beta(x,y) = 0\,\forall x \in M \Rightarrow y = 0$, similarly $\beta(x,y) = 0\,\forall y \in M \Rightarrow x = 0$

Remark. $r,l : M \to M^v = \mathrm{Hom}_R(M,R) = \{f : M \mapsto R : f \text{ is } R\text{-linear}\}$ defined by $x \mapsto r(x) = \beta(x,-) : M \to R : t \mapsto \beta(x,t)$ and $y \mapsto l(y) = \beta(y,-) : M \to R : t \mapsto \beta(t,y)$. Then

1. says r,l are surjective
2. says r,l are injective

In particular, if $M = V$ a finite dimensional vector space over a field $R = F$ then 2. $\Rightarrow$ 1. (as $\dim V = \dim V^v$ and thus 1. injectivitiy$\Rightarrow$ 2. surjectivity)

Definition 0.4. Let $(M,\beta),(M',\beta')$ be bilinear forms. An isometry from M to M' is an R-linear isomorphism $f : M \to M'$ such that $\beta(x,y) = \beta'(f(x),f(y))\,\forall x,y \in M$

Two bilinear forms $(M,\beta),(M',\beta')$ are isometric if there exists an isometry between them

Exercise. Check that isometry is an equivalence relation

Check if (M,β) and (M',β') are isometric then (M,β) is symmetric (skew-symmetric, symplectic, regular) if and only if (M',β') is.

Definition 0.5. Let M be an R-module. A *quadratic form* on M is a function $q : M \to R$ such that

1. $q(ax) = a^2q(x)\,\forall a \in R, x \in M$
2. The form $\beta_q : M \times M \to R$ defined by $\beta_q(x,y) = q(x+y) - q(x) - q(y)$ is bilinear

β_q is called the associated symmetric bilinear form.

The quadratic form $q : M \to R$ is called regular if β_q is regular.

Let $(M,q),(M',q')$ be two quadratic forms modules. An isometry from M to M' is an R-linear isomorphism $f : M \to M'$ such that $q(x) = q'(f(X))\,\forall x \in M$.

Remark. If β is a (symmetric) bilinear form then $q_\beta(x) = \beta(x,x)$ is a quadratic form because $q_\beta(ax) = \beta(ax,ax) = a^2\beta(x,x) = a^2q_\beta(x)$ and $\beta_{q_\beta}(x,y) = q_\beta(x+y) - q_\beta(x) - q_\beta(y) = \beta(x+y,x+y) - \beta(x,x) - \beta(y,y) = \beta(x,y)+\beta(y,x)$ is bilinear.

If β is symmetric then $\beta_{q_\beta} = 2\beta$

Corollary 0.6. *If $\frac{1}{2} \in R$ (i.e. $2 \in R$ is a unit) and M is an R-module then $\{$quadratic forms on $M\} \to \{$symetric bilinear forms on $M\}$ by $q \mapsto \beta_q$ is a bijection with inverse $\{$symetric bilinear forms on $M\} \to \{$quadratic forms on $M\}$ defined by $\beta \mapsto \frac{1}{2}q_\beta$*

Proof. Exercise ☐

Remark. If $\frac{1}{2} \in R$ then the theory of quadratic forms is the same as the theory of symmetric bilinear forms.

But if $\frac{1}{2} \notin R$ then the two theories may differ:

Example. The symmetric bilinear form $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $x, y \mapsto xy$ does not come from a quadratic forms on $\mathbb{Z}$ because if $q : \mathbb{Z} \to \mathbb{Z}$ is a quadratic form then $q(a) = q(a \cdot 1) = a^2 q(1)$ and $\beta_q(x, y) = q(x + y) - q(x) - q(y) = (x + y)^2 q(1) - x^2 q(1) - y^2 q(1) = 2xyq(1) \neq xy$

Objective of this course: Understand classification of quadratic forms (or symmetric bilinear forms) up to isometry:
How many quadratic forms exists (up to isometry)?
Given two quadratic forms how can I decide when they are isometric

A few applications of quadratic forms:

- Algebra (quaternion algebras)
- Manifold theory (as products pairing)
- Number theory
- Lattice theory (sphere packing)

1 Quadratic forms and homogeneous polynomial of degree 2

Definition 1.1. A polynomial $f = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \in R[x_1, \ldots, x_n]$ is called *homogenous* of degree m if all occurring monomials $x_1^{i_1} \ldots x_n^{i_n}$ $(a_{i_1,\ldots i_n} \neq 0)$ has degree $i_1 + \ldots + i_n = m$

Example. $x^3 + x^2 y + z^3$ is homogeneous of degree 3
$x^3 + x^2 + zy^2$ is not homogeneous.

Every homogeneous degree 2 polynomial $f \in R[x_1, \ldots, x_n]$ has the form $f = \sum_{i=1}^n a_i x_i^2 + \sum_{i<j} b_{ij} x_i x_j$. To every polynomial $f \in R[x_1, \ldots, x_n]$ one can associate a (polynomial) function $\bar{f} : R^n \to R$ by $(r_1, \ldots, r_n) \mapsto f(r_1, \ldots, r_n)$

Remark. In general $R[x_1, \ldots, x_n] \to$ Funtions (R^n, R) which maps to $f \mapsto \bar{f}$ is not injective. (find examples!)

But homogenous polynomials in n-variables of degree $m \to$ Functions (R^n, R) is injective

Claim. If $f \in R[x_1, \ldots, x_n]$ is homogeneous of degree 2 then $\bar{f} : R^n \to R$ is a quadratic from

Proof. Note: If q_1, q_2 are quadratic forms on M then $q_1 + q_2$ and aq_1 are all quadratic forms $\forall a \in R$. Thus can assume $f = x_i x_j$. Then $\bar{f}(r_1, \ldots, r_n) = r_i r_j$ so

1. $\bar{f}(ar) = a^2 \bar{f}(r) \, \forall a \in R_1, r \in R^n$
2. $\bar{f}(r + s) - \bar{f}(r) - \bar{f}(s) = (r_i + s_i)(r_j + s_j) - r_i r_j - s_i s_j = r_i s_j + s_i r_j$ is bilinear in $r, s \in R^n$

☐

Lemma 1.2. *For any (commutative!) ring R, the map*

$$\left\{\begin{matrix}\textit{homoegenous polynomials of degree} \\ \textit{2 in n variables}\end{matrix}\right\} \to \{\textit{quadratic forms } R^n\}$$

defined by $f \mapsto \bar{f}$ is bijective

Proof. Exercise ☐

If $\underset{e_j \mapsto \sum_{i=1}^n a_{ij} e_i}{R^n \to R^n}$ is an R-linear map given by a matrix $A = (a_{ij}) \in M_n(R)$ we can define a ring homomorphism $A_* : R[x_1, ..., x_n] \to R[x_1, ..., x_n]$ by $x_j \mapsto A_*(x_j) = \sum_{j=1}^n a_{ij} x_j$ which sends homogenous polynomials of degree m to homogenous polynomials of the degree m.

Definition 1.3. Two homogenous polynomials of degree 2 $f, g \in R[x_1, ..., x_n]$ are (linearly) equivalent if $\exists A \in M_n(R)$ invertible with $A_*(f) = g$

Lemma 1.4. *The map*

$$\left\{\begin{matrix} \text{homoegenous polynomials of degree} \\ 2 \text{ in } n \text{ variables} \\ \end{matrix}\right\} / \text{linear equivalence} \to \{\text{quadratic forms on } R^n\}/\text{isometry}$$

is bijective

Proof. Exercise ◻

1.1 Free bilinear form modules

Definition 1.5. A bilinear R-module (M, β) is called *free of rank n* ($n \in \mathbb{N}$) if $M \cong R^n$

If (M, β) is free of rank n then M has a basis $e_1, ..., e_n$ and we can defined an associated bilinear form matrix $B = (\beta(e_i, e_j))$. Note that $B = (\beta(e_i, e_j))$ determines β since if $x, y \in M$ have coordinates (with respect to $e_1, ..., e_n$) $x_1, ..., x_n, y_1, ..., y_n \in R$ i.e. $x = \sum x_i e_i, y = \sum y_i e_i$ then $\beta(x, y) = \beta(\sum x_i e_i, \sum y_j e_j) = \sum x_i \beta(e_i, e_j) y_j = (x_1, ..., x_n) B (y_1, ..., y_n)^T$

Example. Standard scalar product on $\mathbb{R}^n$ has bilinear form matrix with respect to standard basis
$$B = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Lemma 1.6. *Let (M, β) be a free bilinear form module of rank n with basis $e_1, \ldots, e_n$, then β is non-degenerate $\iff$ the associated bilinear form matrix $B = (\beta(e_i, e_j)) \in M_n(R)$ is invertible*

Proof. Recall that β is non degenerate if and only if $r, l : M \to \mathrm{Hom}_R(M, R)$ defined by

$$\begin{aligned} x &\mapsto r(x) = \beta(x, -),\ r(x)(y) = \beta(x, y) \\ &\mapsto l(x) = \beta(-, x),\ l(x)(y) = \beta(y, x) \end{aligned}$$

are bijective. M has basis $e_1, \ldots, e_n$. Then $\mathrm{Hom}_R(M, R)$ has basis $e_1^\#, ..., e_n^\#$ where $e_i^\# e_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$ i.e. $e_i^\# (\sum x_j e_j) = x_i$. Let (r_{ij}) receptively (l_{ij}) be the $n \times n$ of r, l with respect to basis $e_1, ..., e_n$of M and $e_1^\#, ..., e_n^\#$of $\mathrm{Hom}_R(M, R)$ i.e. $\sum_{k=1}^n r_{kj} e_k^\# = r(e_j)$ and $\sum_{k=1}^n l_{kj} e_k^\# = l(e_j)$ so $\beta(e_j, e_i) r(e_j)(e_i) = \sum_{k=1}^n r_{kj} e_k^\#(e_i) = r_{ij}\, \forall i, j \Rightarrow (r_{ij}) = B^T =$ transpose of B. Similarly for $(e_{ij}) = B$. So, β non degenerated $\iff$ r, l are R-linear isomorphism $\iff$ (r_{ij}) and (l_{ij}) are invertible $\iff$ B^T, B are invertible $\iff$ B is invertible ◻

Lemma 1.7. *Let $(M, \beta), (M', \beta')$ be two free bilinear form modules over R of rank n with basis $e_1, ..., e_n$ for M and $e_1', ..., e_n'$ for M' then (M, β) and (M', β') are isometric $\iff$ associated bilinear form matrices $B = (\beta(e_i, e_j))$ and $B' = (\beta'(e_i', e_j'))$ are congruent. i.e. $\exists A \in M_n(R)$ invertible such that $B = A^T B' A$*

Proof. " $\Rightarrow$ ": Let $f : M \to M'$ be an isometry. Let (f_{ij}) be the associated matrix with respect to the basis $e_1, ..., e_n$ and $e_1', .., e_n'$ i.e. $f(e_j) = \sum_{k=1}^n f_{kj} e_k'$. Then f isometry $\Rightarrow$ f isomorphism $\Rightarrow (f_{ij})$ invertible and $\beta(e_i, e_j) = \beta'(f(e_i), f(e_j)) = \beta'\left(\sum_{k=1}^n f_{ki} e_k', \sum_{l=1}^n f_{lj} e_l'\right) = \sum f_{ki} \beta'(e_k', e_l') f_{lj} = (A^T B' A)_{ij}$. Hence $B = A^T B' A$

" $\Leftarrow$ ": $A = (f_{ij}) \in M_n(R)$ defines an isomorphism $f : M \to M'$ by $f(e_j) = \sum f_{kj} e_k'$ such that $\beta(e_i, e_j) = \beta'(f(e_i), f(e_j))$ (Calculation as above). Hence $f : M \to M'$ is an isometry ◻

Definition 1.8. Let $B \in M_n(R)$ we let $\langle B \rangle$ stand for the bilinear form module (R^n, β), $\beta : R^n \times R^n \to R$ defined by

$$\underset{\begin{pmatrix} x_1 \\ \\ x_n \end{pmatrix}}{x} \;,\; \underset{\begin{pmatrix} y_1 \\ \\ y_n \end{pmatrix}}{y} \mapsto \beta(x, y) = x^T B y$$

This is a free bilinear form module with basis $e_1, \ldots, e_n$ with e_i has an 1 in the i-th position and associated bilinear form matrix B. Note $\beta(e_i, e_j) = e_i^T B e_j = B_{ij}$

Remark. $\langle B \rangle \cong \langle B' \rangle$ for $B, B' \in M_n(R) \iff \exists A \in M_n(R)$ invertible such that $B' = A^T B A$

Definition 1.9. The *determinant* of a non-degenerate free bilinear form module $M = (M, \beta)$ with basis $e_1, \ldots, e_n$ is the determinant $\det M = \det(\beta(e_i, e_j))_{i,j=1,\ldots,n} \in R^*/R^{2*}$. Here $R^{2*} \subset R^*$ is the set of units which are squares. Note that $\det M \in R^*/R^{2*}$ does not depend on the choice of basis because if $e_1', \ldots, e_n'$ is another basis, then $(\beta(e_i', e_j')) = A^T(\beta(e_i, e_j)A \Rightarrow \det(\beta(e_1', e_j') = (\det(A))^2 \det(\beta(e_i, e_j))$

Example. Recall $\langle a \rangle$ is $R \times R \to R$ defined by $x, y \mapsto axy$.

- If $\langle 1 \rangle = \langle 2 \rangle \Rightarrow \underbrace{\det\langle 1 \rangle}_{=1} = \underbrace{\det\langle 2 \rangle}_{=2} \in R^*/R^{2*} \Rightarrow 2$ is a square $\Rightarrow \langle 1 \rangle \not\cong \langle 2 \rangle$ over $\mathbb{Q}$
- If $\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \Rightarrow 1 = -1 \in R^*/R^{2*} \Rightarrow (-1)$ is a square $\Rightarrow \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \not\cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ but $\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ over $\mathbb{C}$ (see below)

Remark. if (M, β) is a free of rank n with basis $e_1, \ldots, e_n$ and bilinear form matrix B then

- (M, β) is non-degenerate $\iff \det B \in R^*$.
- (M, β) is symmetric $\iff B = B^T$
- (M, β) is skew-symmetric $\iff B^T = -B$
- (M, β) is symplectic $\iff B^T = -B$ and all diagonal entries of B are 0

Proof. Exercise. □

Lemma 1.10. *Let R be (commutative!) ring and $f : R^n \to R^l$ is a surjective R-module homomorphism. Then $n \geq l$. In particular, $R^n \cong R^l \Rightarrow n = l$*

Proof. Let $m \subset R$ be a maximal ideal. Then $R/m = k$ is a field. Reducing $f \mod m$ yields a surjective map $f : (R/m)^n \to (R/m)^l$ of finite dimensional k-vector space $\Rightarrow n = \dim_k(R/m)^n \geq \dim_k(R/m)^l = l$ □

Remark. Lemma does not hold for non-commutative ring in general. For example let V be a k-vector space of ∞ dimension and $A = \mathrm{End}_k(V)$ then $A \oplus A \cong A$ as A module

2 Orthogonal sum

Definition 2.1. Let (M, β) and (M', β') be two bilinear form modules. Their *orthogonal sum* $(M, \beta) \perp (M', \beta')$ has underlying module $M \oplus M'$ and bilinear form $(M \oplus M') \times (M \oplus M') \to R$ defined by $(x, u), (y, v) \mapsto \beta(x, y) + \beta'(u, v)$.

Remark.

- $B \in M_n(R), B' \in M_m(R)$ then $\langle B \rangle \perp \langle B' \rangle = \left\langle \begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix} \right\rangle$
- If (M, β) and (M', β') are regular (symmetric,skew-symmetric,symplectic) then so is $(M, \beta) \perp (M', \beta')$

Definition 2.2. Let (M, β) be a symmetric or skew-symmetric bilinear form (so $\beta(x, y) = 0 \Rightarrow \beta(y, x) = 0$). Let $N \subset M$ be a sub-module. The *orthogonal complement* of N (in M) is the sub-module $N^\perp = \{x \in M | \beta(x, y) = 0 \, \forall y \in N\}$

Lemma 2.3. *Let (M,β) be symmetric or skew-symmetric and $N \subset M$ a sub-module such that (N,β_N) is non degenerate. Then $M = N \perp N^\perp$*

Proof. Have to check that $N \cap N^\perp = 0$. If $x \in N \cap N^\perp$ then $\beta(x,y) = 0\,\forall y \in N$ (as $x \in N^\perp$). But since $x \in N$ and β_N is non degenerate we have $x = 0$. So $M \supset N + N^\perp = N \oplus N^\perp$.

We next need to check $N + N^\perp = M$. Let $x \in M$ then $\beta(x,-)|_N \in \mathrm{Hom}_R(N,R) \underset{\beta_N \text{ non-degenrate}}{\Rightarrow}$ $\exists x_0 \in N :\ \beta(x,y) = \beta(x_0,y)\,\forall y \in N$ then $\beta(x-x_0,y) = 0\,\forall y \in N \Rightarrow x - x_0 \in N^\perp \Rightarrow x = \underbrace{x_0}_{\in N} + \underbrace{x - x_0}_{\in N^\perp}$.

Thus $N + N^\perp = M \Rightarrow N \oplus N^\perp = M$

Lastly we need to check that $(N,\beta_N) \perp (N^\perp, \beta_N^\perp) = (M,\beta)$. If $x,y \in N, u,v \in N^\perp$ then $\beta(x+u,y+v) = \beta(x,y) + \underbrace{\beta(x,v)}_{=0} + \underbrace{\beta(v,y)}_{=0} + \beta(u,v) = \beta_N(x,y) + \beta_N^\perp(u,v)$ □

Corollary 2.4. *If (M,β) is a finitely generated symmetric bilinear form module. Then $M = \langle u_1\rangle \perp \langle u_2\rangle \perp \cdots \perp \langle u_k\rangle \perp N$ where $u_i \in R^*$ and $\beta(x,x) \in R \setminus R^*\,\forall x \in N$*

Proof. Set $M_0 = M$ and if $\beta(x,x) =\in R \setminus R^*\,\forall x \in M_0 = M$ then take $N = M_0 = M$ and we are done. So assume $\exists x \in M_0 : \beta(x,x) \in R^*$ then $ax \neq 0 \in M\,\forall a \in R \setminus \{0\}$ (if $ax = 0 \Rightarrow \beta(ax,x) = a\beta(x,x) \Rightarrow a = 0$). So $Rx \subset M$ is a free module of rank 1 with basis x. Rx has bilinear form matrix $(\beta(x,x)) \in R^*$ invertible. So, $\beta|_{Rx}$ is non degenerate. $\Rightarrow M = \underbrace{Rx}_{\langle u_1\rangle} \perp \underbrace{(Rx)^\perp}_{=:M_1}$ with $u_1 = \beta(x,x) \in R^*$ contradicting Lemma 1.10

Repeat with M_1in place of M_0 to obtain $M = \langle u_1\rangle \perp \cdots \perp \langle u_k\rangle \perp M_k$. We can repeats as long as $\exists x \in M_K : \beta(x,x) \in R^*$. But the procedure stops because $K > n$ impossible otherwise there exists a surjective map $R^n \twoheadrightarrow M = \underbrace{\langle u_1\rangle \perp \cdots \perp \langle u_n\rangle}_{R^k} \perp M_k \twoheadrightarrow R^k \Rightarrow n \geq k$ □

Remark. If $\beta(x,x) \in R \setminus R^*\ \forall x \in N \neq 0$ and β is non-degenerate then (N,β) cannot has an orthogonal basis

Proof. If $N = \langle u_1\rangle \perp \cdots \perp \langle u_n\rangle$ and if N is non-degenerate with respect to base $e_1,\ldots,e_n$ then $\langle u_i\rangle$ are non-degenerate $\Rightarrow u_i \in R^*$. $\beta(e_i,e_j) = \begin{cases} u_i & i = j \\ 0 & i \neq j \end{cases}$ in particular $\beta(e_1,e_1) = u_1 \in R^*$ □

Theorem 2.5 (Existence of orthogonal basis over fields of char $\neq 2$)**.** *Let k be a field of char $\neq 2$ and (M,β) a finite dimensional symmetric bilinear form. Then $M = \langle u_1\rangle \perp \cdots \perp \langle u_l\rangle \perp N$ such that $\beta|_N = 0$ ($\beta(x,y) = 0\,\forall x,y \in N$). In particular (M,β) has an orthogonal basis, $e_1,\ldots,e_l,e_{l+1},\ldots e_n$ such that* $\beta(e_i,e_j) = \begin{cases} u_i & j = i = 1,\ldots l \\ 0 & j = i = l+1,\ldots n \\ 0 & j \neq i \end{cases}$

Proof. From corollary we have $(R = k)$ $M = \langle u_1\rangle \perp \cdots \perp \langle u_l\rangle \perp N$ with $u_i \in R^*, \beta(x,x) \in \underset{k\setminus k^* = 0}{R \setminus R^*}\forall x \in N$. Need to show $\beta|_N = 0$. $\beta(x,x) = 0\,\forall x \in N \Rightarrow$ associated quadratic form $q(x) = \beta(x,x) = 0 \underset{\text{char}\neq 2}{\Rightarrow}$ $\beta(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = 0$ □

Want to generalize theorem on existence of orthogonal basis to rings.

Definition 2.6. A ring R is called *local* if it has a unique maximal ideal m.

Note that R/m is a field as $m \subset R$ is a maximal ideal.

Notation. (R,m,k) is a local ring if $k = R/m, m \subset R$ is the maximal ideal

Remark. In a local ring (R,m,k) we have $R^* = R \setminus m$

Proof. Need to show $m = R \setminus R^*$.

- We see that $m \cap R^* = \emptyset$ because $m \subsetneq R \Rightarrow m \subset R \setminus R^*$.

- If $a \in R \setminus R^*$, then $(a) = Ra \subsetneq R$ (proper ideal because $Ra = R \Rightarrow \exists b : ba = 1$ contradicting $a \notin R^*$) Every proper ideal is contained in a maximal ideal $\Rightarrow Ra \subset m \Rightarrow a \in m \Rightarrow R \setminus R^* \subset m$

$\square$

(R, m, k) local then $A \in M_n(R)$ is invertible if and only if $A \mod m \in M_n(k)$ is invertible because $A \in M_n(R)$ invertible $\iff \det A \in R^* = R \setminus m \iff \det(A \mod m) \neq 0 \in k = R/m \iff A \mod m \in M_n(k)$ is invertible.

Example.

- Fields are local rings with $m = 0$
- $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$ where $p \in \mathbb{Z}$ is prime. This is a local ring with maximal ideal $m = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b, p \mid a\}$. Then $\mathbb{Z}_{(p)}/m = \mathbb{F}_p$
- k field $k[T]/T^n$ is a local ring with maximal ideal (T)

Definition 2.7. A finitely generated R-module P is called *projective* if it is a direct factor of some $R^n, n \in \mathbb{N}$ i.e. $\exists R$-module $N : M \oplus N \cong R^n$

Theorem 2.8. *Let (R, m, k) be a local ring and M a finitely generated projective R-module, then $M \cong R^l$ for some $l \in \mathbb{N}$*

Proof. M projective so $\exists N : M \oplus N \underset{\leftarrow}{\overset{f}{\cong}} R^n$. Let $p : R^n \to R^n$ be the linear map $R^n \xrightarrow{f} M \oplus N \underset{x,y \mapsto (x,0)}{\overset{q}{\to}} M \oplus N \xrightarrow{f^{-1}} R^n$ and let p be the composition of all these maps. Note that $p^2 = (f^{-1}qf)^2 = f^{-1}qff^{-1}qf = f^{-1}\underbrace{q^2}_{=q}f = p$ and $\operatorname{im} p \underset{\underset{g}{\leftarrow}}{\overset{\overset{f}{\to}}{\cong}} M$

Claim. $\exists$ basis of R^n with respect to which p has the form $\begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix}$ i.e. $\exists U \in M_n(R)$ such that $p = U \begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix} U^{-1}$.

Note that claim implies theorem because $\operatorname{im} p \underset{U}{\overset{\cong}{\leftarrow}} \operatorname{im} \begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix} = R^l$

Claim is true over a field (i.e. $\mod m$). M/mM and N/mN are finite dimensional k-vector spaces so $k^l \underset{\underset{g_1}{\to}}{\cong} M/mM$, $k^r \underset{\underset{g_2}{\to}}{\cong} N/mN$

$$\begin{tikzcd}
k^l \oplus k^r \arrow[r, "\begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix}"] \arrow[d, "g_1 \oplus g_2"] & k^l \oplus k^r \\
M/mM \oplus N/mN \arrow[r, "q"] \arrow[d, "f \mod m"', "\cong"] & M/m \oplus N/mN \arrow[u, "g_1^{-1} \oplus g_2^{-1}"'] \\
(R/m)^n \arrow[r, "p"] & (R/m)^n \arrow[u, "f^{-1}"']
\end{tikzcd}$$

Then we get $\begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix} = A^{-1}p\underbrace{f(g_1 \oplus g_2)}_{A \in M_n(k)}$, $p \mod m = A \begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix} A^{-1}$, now lift all entries of A to entries of R (under the surjective $R/m \to k$) to obtain a matrix $S \in M_n(R)$ such that $A = S \mod m$. $A \in M_n(k)$ invertible $\Rightarrow S \in M_n(R)$ invertible. $S^{-1}pS \mod m = \begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix} \mod m$ so $S^{-1}pS = \begin{pmatrix} T & B \\ C & D \end{pmatrix}$ with $T = 1_l \mod m$ and $B, C, D = 0 \mod m$. $\Rightarrow$ after base change (given by S) p becomes $\begin{pmatrix} T & B \\ C & D \end{pmatrix}$ as above. Idea: "Want to perform row and column operation to make

$\begin{pmatrix} T & B \\ C & D \end{pmatrix}$ into $\begin{pmatrix} 1_l & 0 \\ 0 & 0 \end{pmatrix}$ after base changes". Now, $T = 1 \mod m \Rightarrow T \in M_n(R)$ invertible. $p^2 = p \Rightarrow \begin{pmatrix} T & B \\ C & D \end{pmatrix} = \begin{pmatrix} T & B \\ C & D \end{pmatrix}\begin{pmatrix} T & B \\ C & D \end{pmatrix} = \begin{pmatrix} T^2+BC & * \\ * & * \end{pmatrix}$. $T = T^2 + BC \Rightarrow 1 = T + T^{-1}BC$. $\underbrace{\begin{pmatrix} 1 & T^{-1}B \\ 0 & 1 \end{pmatrix}}_{X}\begin{pmatrix} T & B \\ C & D \end{pmatrix}\underbrace{\begin{pmatrix} 1 & -T^{-1}B \\ 0 & 1 \end{pmatrix}}_{X^{-1}} = \begin{pmatrix} 1 & * \\ * & * \end{pmatrix}$$\Rightarrow$after bases change p becomes $\begin{pmatrix} 1 & B \\ C & D \end{pmatrix}$, $B, C, D = 0 \mod m$. $p^2 = p \Rightarrow \begin{pmatrix} 1 & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1 & B \\ C & D \end{pmatrix}\begin{pmatrix} 1 & B \\ C & D \end{pmatrix} \Rightarrow BC = 0, BD = 0, DC = 0, D = CB + D^2$. $\Rightarrow D^2 = \underbrace{DCB}_{0} + D^3 \Rightarrow D^2 = D^3 \Rightarrow D^2(1-D) = 0 \Rightarrow D^2 = 0 \Rightarrow D = CB$. The second to last implication is because $1 - D$ is invertible as $D \equiv 0 \mod m$. $\underbrace{\begin{pmatrix} 1 & 0 \\ -C & 1 \end{pmatrix}}_{Y^{-1}}\begin{pmatrix} 1 & B \\ C & CB \end{pmatrix}\underbrace{\begin{pmatrix} 1 & 0 \\ C & 1 \end{pmatrix}}_{Y} = \begin{pmatrix} 1 & B \\ 0 & 0 \end{pmatrix}$Then an other base change gives $\underbrace{\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix}}_{Z}\begin{pmatrix} 1 & B \\ 0 & 0 \end{pmatrix}\underbrace{\begin{pmatrix} 1 & -B \\ 0 & 1 \end{pmatrix}}_{Z^{-1}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ □

Remark. If R is a Euclidean domain (e.g. $R = \mathbb{Z}$) then every finitely projective R-module is free.

Example. $R = \mathbb{Z}$ every finitely generated $\mathbb{Z}$-module is isomorphic to $\mathbb{Z}^n \oplus$finite abelian group. If P is finitely generated projective over $\mathbb{Z}$ then $P \subseteq \mathbb{Z}^m \Rightarrow P$ has no element of finite order. $\Rightarrow P = Z^n \oplus$ / finite

Remark. For a general commutative ring, projective R-modules may not be free

Example. $R = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[T]/(T^2+5)$. Fact: R is a Dedekind domain, every ideal $I \subset R$ of a Dedekind domain is a projective R-module. Let $I = (2, 1+\sqrt{-5}) \subset R$. From the fact I is projective. If I was free then $I \cong R^n$, $n \neq 0$ because $I \neq 0$. Let's compute R/I:

$$\begin{aligned} R/I &= \mathbb{Z}[T]/(T^2+5, 2, 1+T) \\ &= \mathbb{F}_2[T]/(T^2+5, T+1) \\ &= \mathbb{F}_2[T]/(T^2+1, T+1) \\ &= \mathbb{F}_2[T]/((T+1)^2, T+1) \\ &= \mathbb{F}_2[T]/(T+1) \\ &\cong \mathbb{F}_2 \end{aligned}$$

Assume $n = 1$ then $I = Rt$ for some $t \in R$. Now t is not a unit because otherwise $0 = R/Rt$ contradicting $R/I = \mathbb{F}_2$. If $t \notin R^* : I = Rt \Rightarrow 2 = at \underset{2\text{ irreducible}}{\Rightarrow} a \in R^* \Rightarrow I = Rt = R\frac{1}{a}2 = R \cdot 2$ and

$$\begin{aligned} R/I &= \frac{\mathbb{Z}[T]}{T^2+5} / \underbrace{I}_{2R} \\ &= \mathbb{Z}[T]/(T^2+5, 2) \\ &= \mathbb{F}_2[T]/(T^2+1) \\ &= \mathbb{F}_2[T]/(T+1)^2 \\ &\neq \mathbb{F}_2 \end{aligned}$$

$\Rightarrow I \cong R^n \Rightarrow n \geq 2$. So $R^n \cong I \subset R$, let $F =$ field of fraction of R. Then $I \hookrightarrow I \otimes_R F$ and $R \hookrightarrow F = R \otimes_R F$ so we get $F^n = I \otimes_R F \subset F = R \otimes_R F$ (since F is a localization of R) $\Rightarrow F^n \subset F$ contradiction so $n \ngeq 2$.

Definition 2.9. An *inner product space* is a non-degenerate bilinear form module (M, β) where M is finitely generated and projective.

Remark. Over a local ring any inner product space is free

Definition 2.10. Let R be a ring. The *hyperbolic plane* $\mathbb{H}$is the symmetric inner product space $\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ i.e. $\mathbb{H} = (R^2, \beta)$.

$\mathbb{H}$ has basis e_1, e_2 with respect to which we have $\beta(e_i, e_j) = \begin{cases} 0 & i = j \\ 1 & i \neq j \end{cases}$. $\mathbb{H}$ is a symmetric space because $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, it is non-degenerate because $\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1 \in R^*$. Does $\mathbb{H}$ have an orthogonal basis? If $\frac{1}{2} \in R$ (i.e. $2 \in R^*$) then $\mathbb{H} \cong \langle 1 \rangle \perp \langle -1 \rangle$ because $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & -\frac{1}{2} \\ 1 & \frac{1}{2} \end{pmatrix}}_{A^T} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}}_{=A}$ and $\det A = 1$ and thus A is invertible. If $\frac{1}{2} \notin R$ ($2 \notin R^*$) then $\mathbb{H}$ has no orthogonal basis. In $\mathbb{H} \ni \begin{pmatrix} x \\ y \end{pmatrix}$ then $\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2xy \notin R^* \, \forall x, y \in \mathbb{H}$ since $2 \notin R^*$. If $(\mathbb{H}, \beta)$ had an orthogonal basis e_1, e_2 then $\beta(e_i, e_i) \in R^* \Rightarrow \mathbb{H}$ has not orthogonal basis.

Example. If (R, m, k) is a local ring with char$k = 2$ then for all $a, b \in m$ $\left\langle \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix} \right\rangle$has no orthogonal basis (otherwise, any orthogonal basis would yield an orthogonal basis mod m but $\left\langle \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix} \right\rangle$ mod $m = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle = \mathbb{H}$ has no orthogonal basis.

Theorem 2.11. *Let (R, m, k) be a local ring and $M = (M, \beta)$ a symmetric inner product space.*

- *If char$(k) \neq 2$ then M has an orthogonal basis*
- *If char$(k) = 2$ then $M = \langle u_1 \rangle \perp \cdots \perp \langle u_l \rangle \perp N_1 \perp \cdots \perp N_r$ where $u_i \in R^*$ and $N_i = \left\langle \begin{pmatrix} a_i & 1 \\ 1 & b_i \end{pmatrix} \right\rangle, a_i, b_i \in m$*

Proof. Recall M finitely generated, β is symmetric $\Rightarrow M = \langle u_1 \rangle \perp \cdots \perp \langle u_l \rangle \perp N$ such that $u_i \in R^*$ and $\beta(x, x) \in R \setminus R^* = m \, \forall x \in N$.

Recall R local and M finitely generated projective $\Rightarrow M \cong R^{n+l}$, same for N so $N \cong R^n$

If $n = 0$ done. So assume $n \geq 1$.Then β non-degenerate $\Rightarrow$ for $\varphi : \underset{(x_1, \ldots, x_n) \mapsto x_1}{R^n = N \to R}$ linear, $\exists x_0 \in N : \beta(x_0, y) = \varphi(y) \; \forall y \in N \Rightarrow \exists x, y \in N : \beta(x, y) = 1 \; (y = e_1, x = x_0)$.

If char$(k) \neq 2$ ($2 \notin m = R \setminus R^* \Rightarrow 2 \in R^*$). If $N \neq 0 \Rightarrow \exists x, y \in N, \beta(x, y) = 1$. Then $x + y \in N$ so $\underbrace{\beta(x + y, x + y)}_{\in m} = \underbrace{\beta(x, x)}_{\in m} + \underbrace{2\beta(x, y)}_{=2} + \underbrace{\beta(y, y)}_{\in m} \Rightarrow 2 \in m \Rightarrow N = 0$ (due to the contradiction of char$(k) \neq 2$)

Now assume that char$(k) = 2$. We are going to prove that $N = N_1 \perp \cdots \perp N_r$ with N_i as in the theorem by induction on n ($N \cong R^n$). $n = 0 \Rightarrow N = 0$ and we are done. $n = 1 \Rightarrow N \cong R$ then $\beta|_N$ is a non-degenerate symmetric form on R but any rank 1 inner product space is $\cong \langle u \rangle$ for $u \in R^*$ because $\beta : R \times R \to R, \beta(x, y) = xy \cdot \beta(1, 1)$ and β non-degenerated $\Rightarrow \beta(1, 1) \in R^*$. This contradict our assumption that $\beta(x, x) \in m \forall x \in N$. So assume $n \geq 2$: Since $\beta|_N$ is non degenerate and N free (of rank n) $\Rightarrow \exists x, y \in N : \beta(x, y) = 1$ (because $N \cong R^n, \varphi : R^n \to R$ by $x_1, \ldots, x_n \mapsto x_1 \underset{\beta \text{ non-deg}}{\Rightarrow} \exists x : \varphi(y) = \beta(x, y) \forall y \in R^n$ so in particular $\exists x \in N \, 1 = \varphi(e_1) = \beta(x, e_1)$)
The subspace $Rx + Ry \subset N$ has bilinear form matrix with respect to $\{x, y\}$

$$\begin{pmatrix} \beta(x, x) & \beta(x, y) \\ \beta(y, x) & \beta(y, y) \end{pmatrix} = \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix}$$

and by assumption $a, b \in m$ because $\beta(z, z) \in \forall z \in N$. This has determinant $\underbrace{\underbrace{ab}_{\in m} - \underbrace{1}_{\notin m}}_{\notin m} \in R^* \Rightarrow x, y$

linearly independent and $N_1 := Rx + Ry \subset N$ is isometric to $\left\langle \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix} \right\rangle \Rightarrow N = N_1 \perp N_1^\perp$ and apply induction hypothesis to $N_1^\perp$ and we are done $\square$

Example. $(M, \beta) = \left\langle \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \right\rangle$ over $\mathbb{Z}_{(2)} = \{\frac{p}{q} \in \mathbb{Q} | 2 \nmid q\}$. $\det \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = 3$ and $3 \in (\mathbb{Z}_{(2)})^*$, hence M is non-degenerate. But M has no orthogonal basis because $\mathbb{Z}_{(2)}/2 = \mathbb{F}_2$ and any orthogonal basis over $\mathbb{Z}_{(2)}$ induces a orthogonal basis over $\mathbb{Z}_{(2)}/2$ but $M = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ over $\mathbb{F}_2$ which we have seen has no orthogonal basis.

Over $R = \mathbb{Z}_{(p)}$ where $p \in \mathbb{Z}$ is prime, $p \neq 3$ (otherwise M is degenerate as $3 \notin (\mathbb{Z}_{(3)})^*$). Then M is non-degenerate since $\det M = 3 \in (\mathbb{Z}_{(p)})^*$. If furthermore $p \neq 2$ then by theorem M has an orthogonal basis: For instance $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ then $\beta(x,x) = 2 \in (\mathbb{Z}_{(p)})^*$ $(p \neq 2) \Rightarrow Rx \subset M$ non-degenerate subspace so $M = Rx \perp (Rx)^\perp$. Now $(Rx)^\perp = \{y \in M : \beta(x,y) = 0\} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in R^2 | \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = 0 \right\} = R \begin{pmatrix} 1 \\ -2 \end{pmatrix} \Rightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right\}$ is an orthogonal basis of M if $R = \mathbb{Z}_{(p)}$ $p \neq 2, 3$ (Also works for $\mathbb{Q}, \mathbb{R}, \mathbb{C}$)

Definition 2.12. Let (M, β) be a symplectic inner product space (β symplectic if $\beta(x,x) = 0 \, \forall x \in M$). A symplectic basis of M is a basis $x_1, y_2, x_2, y_x, \dots, x_n, y_n$ such that $M = (Rx_1 + Ry_1) \perp \cdots \perp (Rx_n + Ry_n)$ and $\beta(x_i, y_i) = 1 \, \forall i$ $(\Rightarrow \beta(y_i, x_i) = -1)$ i.e. the bilinear form matrix of β with respect to the basis $x_1, y_1, ..., x_n, y_n$ is

$$\begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & 0 \\ & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & \\ & & \ddots & \\ 0 & & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \end{pmatrix}$$

Theorem 2.13. *Let (R, m, k) be a local ring and (M, β) a symplectic inner product space. Then (M, β) has a symplectic basis*

Proof. (M, β) inner product space $\Rightarrow \beta$ non-degenerate, M projective $\Rightarrow$ free (since R local) $\Rightarrow \exists x, y \in M : \beta(x,y) = 1$. So the inner product matrix of β with respect to $\{x, y\}$ is $\begin{pmatrix} \beta(x,x) & \beta(x,y) \\ \beta(x,y) & \beta(y,y) \end{pmatrix} \underset{\beta \text{ sympletic}}{=} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Thus set $N_1 = Rx + Ry \subset M$ is a non-degenerate free submodule of rank 2 with symplectic basis $\{x, y\}$. $(N_1, \beta|_{N_1})$ non-degenerate $\Rightarrow M = \underbrace{N_1}_{\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle} + N_1^\perp$ repeating the same argument with $N_1^\perp$ instead of M we obtain $M = N_1 \perp N_2 \perp \cdots \perp N_n$ where $N_i = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$ $\square$

Corollary 2.14. *Over a local ring any symplectic inner product space has even dimension. Furthermore any two symplectic inner product spaces are isometric if and only if they have the same rank.*

2.1 Witt Cancellation

Motivation: Let V_1, V_2 be finite dimensional vector spaces over k, If $V_1 \oplus W \cong V_2 \oplus W$ for some finite dimensional vector space W then $V_1 \cong V_2$ because $\dim V_1 = \dim V_1 \oplus W - \dim W = \dim V_2 \oplus W - \dim W = \dim V_2$. The same is true for free modules of finite rank (over a commutative ring), and also over finitely generated projective modules over local rings.

Question: If V_1, V_2, W are symmetric inner product spaces does $V_1 \perp W \cong V_2 \perp W \Rightarrow V_1 \cong V_2$?

Example. $R = \mathbb{F}_2$ (or R local with $\frac{1}{2} \notin R$) then $\langle -1 \rangle \perp \langle -1 \rangle \perp \langle -1 \rangle \cong \langle -1 \rangle \perp \mathbb{H}$, that is, $\left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$ but $\langle -1 \rangle \perp \langle -1 \rangle \not\cong \mathbb{H}$ because $\mathbb{H}$ has no orthogonal basis over $\mathbb{F}_2$. For the isometry see the example below.

Definition 2.15. We say *Witt cancellation* holds for a ring R if $\forall M, N, P$ symmetric inner product spaces over R $M \perp P \cong N \perp P \Rightarrow M \cong N$

Example. Witt cancellation does not hold over fields of char2 (or for local rings R where $2 \notin R^*$).

Note. $\left\langle \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} -1 & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \right\rangle (*)$, because $\beta = \left\langle \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \right\rangle$ has orthogonal basis e_1, e_2, e_3 with $\beta(e_i, e_j) = 0$ for $i \neq j$ and $\beta(e_i, e_i) = \begin{cases} -1 & i = 1, 2 \\ 1 & i = 3 \end{cases}$. In the basis $e_1 + e_2 + e_3, e_1 + e_3, e_2 + e_3$, the inner product β has inner product matrix $\left\langle \begin{pmatrix} -1 & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \right\rangle \Rightarrow (*)$. So If Witt cancellation holds then $\langle -1 \rangle \perp \langle -1 \rangle \cong \mathbb{H}$ but this is not the case for field char2 (or local rings R with $2 \notin R^*$)

Definition 2.16. Let M be an symmetric inner product space and $N \subseteq M$ a non-degenerate subspace then $M = N \perp N^\perp$ and *the reflection of M at N* is the isometry

$$r_N : M = N \perp N^\perp \to N \perp N^\perp$$

$$(x, y) \mapsto (x, -y), \qquad x \in N, y \in N^\perp$$

Remark. r_N is R-linear, an isomorphism ($r_N \circ r_N = \mathrm{id}$) and preserves inner product hence r_N is an isometry

Lemma 2.17. *Let (M, β) be a symmetric inner product space and $x, y \in M$ such that $\beta(x, x) = \beta(y, y) \in R^*$. If R is local with $\frac{1}{2} \in R$ then there is a reflection r of M such that $r(x) = y$*

Proof. Consider $u = x + y, v = x - y \in M$ then $x = \frac{1}{2}(u + v), y = \frac{1}{2}(u - v)$

- $u \perp v$: $\beta(u, v) = \beta(x + y, x - y) = \beta(x, x) - \beta(y, y) = 0$ (Since by assumption $\beta(x, x) = \beta(y, y)$)
- $\beta(u, u)$ or $\beta(v, v) \in R^*$: $4\beta(x, x) = \beta(2x, 2x) = \beta(u + v, u + v) \in R^*$ (since $\beta(x, x) \in R^*$ and $2 \in R^*$). By the first point $\beta(u + v, u + v) = \beta(u, u) + \beta(v, v)$. If $\beta(u, u), \beta(v, v) \in m =$ maximal ideal of $R \Rightarrow \beta(u, u) + \beta(v, v) \in m$. Contradiction hence $\beta(u, u)$ or $\beta(v, v) \in R^*$
- If $\beta(u, u) \in R^*$ then $Ru \subseteq M$ non-degenerate subspace $r_{Ru}(x) = r_{Ru}(\frac{u+v}{2}) = \frac{1}{2} r_{Ru}(u+v) \underset{v \in (Ru)^\perp}{=} \frac{1}{2}(u - v) = y$
  If $\beta(v, v) \in R^*$ then $Rv \subseteq M$ non-degenerate subspace $r_{(Rv)^\perp}(x) = \frac{1}{2} r_{(Rv)^\perp}(u + v) \underset{\substack{u \in (Rv)^\perp \\ v \in ((Rv)^\perp)^\perp = Rv}}{=} \frac{1}{2}(u - v) = y$

$\square$

Theorem 2.18. *Let (R, m, k) be a local ring with $2 \in R^*$. Then Witt cancellation holds for R. That is $\forall M, N, P$ symmetric inner product space over R we have $M \perp P \cong N \perp P \Rightarrow M \cong N$.*

Proof. Let M, N, P be symmetric inner product spaces over R such that $M \perp P \cong N \perp P$. By our assumption R local and $2 \in R^* \Rightarrow P = \langle u_1 \rangle \perp \cdots \perp \langle u_r \rangle$ for $u_i \in R^*$. Thus it suffices to show $M \perp \langle u \rangle \cong N \perp \langle u \rangle \Rightarrow M \cong N$. Let $f : M \perp \langle u \rangle \xrightarrow{\cong} N \perp \langle u \rangle$ be an isometry and let $x \in M \perp \langle u \rangle$ and $y \in N \perp \langle u \rangle$ be a generator for $\langle u \rangle$ i.e. $M \perp \langle u \rangle = M \perp Rx$ and $N \perp \langle u \rangle = N \perp Ry$. $\beta(x, x)_{M \perp \langle u \rangle} = u = \beta(y, y)_{N \perp \langle u \rangle}$. f isometry: $\beta(f(x), f(x))_{N \perp \langle u \rangle} = \beta(x, x)_{M \perp \langle u \rangle} = u = \beta(y, y)_{N \perp \langle u \rangle} \Rightarrow f(x), y \in N \perp \langle u \rangle$ satisfy hypotheses of lemma 2.17 $\Rightarrow \exists$ reflection $r : N \perp \langle u \rangle \to N \perp$

$\langle u \rangle$ such that $r(f(x)) = y \Rightarrow r \circ f : M \perp \langle u \rangle \to N \perp \langle u \rangle$ is an isometry such that $r \circ f : Rx \underset{x \mapsto y}{\overset{\cong}{\to}} Ry$.
$\Rightarrow r \circ f : \underbrace{(Rx)^\perp}_{M} \overset{\cong}{\to} \underbrace{(Ry)^\perp}_{N} \Rightarrow M \underset{r \circ f}{\overset{\cong}{\to}} N$ $\square$

2.2 Symmetric Inner Product space over $\mathbb{R}$

Any symmetric inner product space M over $\mathbb{R}$ has an orthogonal basis $M = \langle u_1 \rangle \perp \dots \langle u_n \rangle, n = \dim_{\mathbb{R}}(M), u_i \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$. If $u > 0$ then $u = a^2$ for some $a \in \mathbb{R}, \langle u \rangle \underset{\leftarrow a}{\cong} \langle 1 \rangle$. If $u < 0$ then $u = -a^2$and $\langle u \rangle \underset{\leftarrow a}{\cong} \langle -1 \rangle$. So $M = r \langle 1 \rangle \perp s \langle -1 \rangle$ (and $r + s = \dim_{\mathbb{R}}(M)$)

Proposition 2.19 (Inertia Theorem)**.** *Over $\mathbb{R}$ we have $r \langle 1 \rangle \perp s \langle -1 \rangle \cong m \langle 1 \rangle \perp n \langle -1 \rangle \Rightarrow r = m$ and $s = n$*

Proof. The equation implies that $r + s = \dim_{\mathbb{R}}(M) = n + m$. Assume without loss of generality that $r \le m$ then $n \le s$. Witt cancellation tells us that $(s - n) \langle -1 \rangle \cong (m - r) \langle 1 \rangle$. Note that if $m - r = s - n \ne 0$ then $\forall x \ne 0 \in (s - n) \langle -1 \rangle$ we have $\beta(x, x) = -\sum x_i^2 < 0$. However $\forall x \ne 0 \in (m - r) \langle 1 \rangle$ we have $\beta(x, x) = \sum x_i^2 > 0$. Contradiction. Hence $s - n = m - r = 0$ $\square$

Corollary 2.20. *The numbers r, s in $M \cong r \langle 1 \rangle + s \langle -1 \rangle$ do not depend on the choice of an orthogonal basis for M*

Definition 2.21. If $M \cong r \langle 1 \rangle \perp s \langle -1 \rangle$ over $\mathbb{R}$ then $r = i^+ M$ is called the *positive index of M*. $s = i^- M$ is called the *negative index of M* and $i^+ M - i^- M = r - s = \operatorname{sgn}(M)$ is called the *signature of M*

We have showed that if (over $\mathbb{R}$) $M \cong N$ then $i^+ N = i^+ M, i^- N = i^- M$ and $\operatorname{sgn}(N) = \operatorname{sgn}(M)$

Corollary 2.22. *Two symmetric inner product-spaces M, N over $\mathbb{R}$ are isometric $M \cong N \iff i^+ M = i^+ N, i^- M = i^- N \iff$ rank $M =$ rank $N, \operatorname{sgn} M = \operatorname{sgn} N$*

2.3 Witt chain equivalence theorem

Notation. Let $u_1, \dots, u_l \in R^*$ write $\langle u_1, \dots, u_l \rangle$ for $\langle u_1 \rangle \perp \cdots \perp \langle u_l \rangle = \left\langle \begin{pmatrix} u_1 & & 0 \\ & \ddots & \\ 0 & & u_l \end{pmatrix} \right\rangle$. We say $\langle u_1, \dots, u_l \rangle$ is a diagonal form

Definition 2.23. We say (M, β) represent $a \in R$ if $\exists x \in M$ such that $\beta(x, x) = a$

Example. A diagonal form $\langle u_1, \dots, u_l \rangle$ represents $u_1, \dots, u_l, u_1 + u_2, \dots$. The equation $a = u_1 x_1^2 + \cdots + u_l x_l^2$ has a solution $x_1, \dots, x_l \in R \iff a$ is represented by $\langle u_1, \dots, u_l \rangle$

Lemma 2.24. *Let R be a local ring (or a ring in which every direct summand of a finitely generated free module is free) Let $\langle a, b \rangle$ and $\langle c, d \rangle$ be non-degenerate diagonal forms ($a, b, c, d \in R^*$). Then $\langle a, b \rangle \cong \langle c, d \rangle \iff ab = cd \in R^*/(R^*)^2$ and $\exists e \in R^*$ which represent $\langle a, b \rangle$ and $\langle c, d \rangle$*

Proof. "$\Rightarrow$": We've already done. (They obviously need the same determinant modulo squares, and need to represent the same numbers)

"$\Leftarrow$": $e \in R^*$ represents $\langle a, b \rangle$ and $\langle c, d \rangle \Rightarrow \exists x, y \in R^2$ such that $\beta(x, x)_{\langle a, b \rangle} = e = \beta(y, y)_{\langle c, d \rangle} \Rightarrow \langle a, b \rangle = \underbrace{\underbrace{Rx}_{\text{non-degenerat}} \perp \underbrace{(Rx)^\perp}_{\text{rank1}}}_{\langle e \rangle \perp \langle u_1 \rangle}$ and $\langle c, d \rangle = \underbrace{\underbrace{Ry}_{\text{non-degenerat}} \perp \underbrace{(Ry)^\perp}_{\text{rank1}}}_{\langle e \rangle \perp \langle u_2 \rangle}$ with $u_1, u_2 \in R^*$. Now $e \cdot u_1 = \det(\langle e \rangle \perp \langle u_1 \rangle) = \det \langle a, b \rangle = \det \langle c, d \rangle = \det \langle e, u_2 \rangle = eu_2 \in R^*/(R^*)^2 \Rightarrow eu_1 = eu_2 g^2$ for some $g \in R^* \Rightarrow u_1 = u_2 g^2$ for some $g \in R^*$, $\langle u_1 \rangle \cong \langle u_2 \rangle \Rightarrow \langle a, b \rangle \cong \langle e, u_1 \rangle \cong \langle e, u_2 \rangle \cong \langle c, d \rangle$ $\square$

Definition 2.25. Two non-degenerate diagonal forms $\langle a_1, \dots, a_n \rangle$ and $\langle b_1, \dots, b_n \rangle$ (of the same rank n) are called *simply (chain) equivalent* (with notation $\approx_s$) if either

- $n \geq 2$ and $\exists 1 \leq i < j \leq n$ such that $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$ and $a_l = b_l \, \forall l \neq i, j$
- or $n = 1$ $\langle a_1 \rangle \cong \langle b_1 \rangle$

Two non-degenerate diagonal forms $\langle a_1, \ldots, a_n \rangle$ and $\langle b_1, \ldots, b_n \rangle$ are *chain equivalent (with notation* $\approx$) if $\exists M_1, \ldots, M_r$ non degenerated diagonal forms of rank n such that $M_1 = \langle a_1, \ldots, a_n \rangle, M_r = \langle b_1, \ldots, b_n \rangle$ and $M_1 \approx_s M_2 \approx_s \cdots \approx_s M_r$

Remark. $\langle a_1, \ldots, a_n \rangle \approx \langle b_1, ..., b_n \rangle \Rightarrow \langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$

Example. $\sigma \in \sum_n$ = permutation group on n letters. $\langle a_1, \ldots, a_n \rangle \approx \left\langle a_{\sigma(1)}, \ldots a_{\sigma(n)} \right\rangle$ because true for transpositions because $\underbrace{\left\langle \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} \right\rangle}_{\langle a \rangle \perp \langle b \rangle \cong \langle b \rangle \perp \langle a \rangle}$ $\Rightarrow$ true for all $\sigma \in \sum_n$ because $\sum_n$ is generated by transpositions.

Witt's Chain Equivalence Theorem. *Let $\langle a_1, \ldots, a_n \rangle$ and $\langle b_1, \ldots, b_n \rangle$ be non-degenerate diagonal forms over a local ring R with $2 \in R^*$ then $\langle a_1, \ldots a_n \rangle \approx \langle b_1, \ldots, b_n \rangle \iff \langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$*

Proof. "$\Rightarrow$": We seen this in the remark

"$\Leftarrow$": We use induction on n. For $n = 0$ there is nothing to say. $n = 1, n = 2$ is true by definition of chain equivalence.

Assume $n \geq 3$ and $\langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$

Claim: $\exists$ non-degenerate diagonal form $\langle c_1, \ldots, c_n \rangle \approx \langle a_1, \ldots, a_n \rangle$ with $c_1 = b_1$.

Note that the claim implies the theorem because $\langle a_1, \ldots, a_n \rangle \approx \langle c_1, \ldots, c_n \rangle, \langle c_1, \ldots, c_n \rangle = \langle b_1, c_2, \ldots, c_n \rangle \cong \langle b_1, \ldots, b_n \rangle \underset{\text{Witt cancellation}}{\Rightarrow} \langle c_2, \ldots, c_n \rangle \cong \langle b_2, \ldots b_n \rangle$. So by hypothesis $\Rightarrow \langle c_2, \ldots, c_n \rangle \approx \langle b_2, \ldots, b_n \rangle$ hence $\langle a_1, \ldots, a_n \rangle \approx \left\langle \underbrace{c_1}_{b_1}, c_2, \ldots, c_n \right\rangle \approx \langle b_1, \ldots, b_n \rangle$.

Proof of claim: Let $P = \{(c, p) | c = \langle c_1, \ldots, c_n \rangle, 1 \leq p \leq n$ such that $\langle c_1, \ldots, c_p \rangle$ represents $b_1\}$. Note that $(\langle a_1, \ldots, a_n \rangle, n) \in P$ so $P \neq \emptyset$. Let $p = \min\{l | \exists (c, l) \in P\}$ well defined and $1 \leq p \leq n$ because $P \neq \emptyset$. Choose (c, p) with p minimal as above. $c = \langle c_1, \ldots, c_n \rangle$ has property that $\langle c_1, \ldots, c_p \rangle$ represent $b_1 \Rightarrow \exists x_1, \ldots x_p \in R$ such that $b_1 = c_1 x_1^2 + \cdots + c_p x_p^2 \in R^*$. Assume that $p \geq 2$. If $\forall i \neq j$ $c_i x_i^2 + c_j x_j^2 \in m = R \setminus R^*$ then $\underbrace{(c_1 x_1^2 + c_2 x_2^x)}_{\in m} + \underbrace{(c_2 x_2^2 + c_3 x_3^2)}_{\in m} + \cdots + \underbrace{(c_p x_p^2 + c_1 x_1^2)}_{\in m} = 2b_1$ which is a contradiction as $2 \in R^*$ and $b_1 \in R^* \Rightarrow \exists i < j$ such that $c_i x_i^2 + c_j x_j^2 \in R^*$. Since $\langle c_1, \ldots, c_p \rangle \approx \left\langle c_{\sigma(1)}, \ldots, c_{\sigma(p)} \right\rangle \forall \sigma \in \sum_p$ we can assume $d = c_1 x_1^2 + c_2 x_2^2 \in R^*$. Then $\langle c_1, c_2 \rangle \cong \langle d, dc_1 c_2 \rangle$ because both represent $d \in R^*$ and both have the same determinant (in R^*/R^{2*}), $\Rightarrow \langle c_1, \ldots, c_p \rangle \approx \langle d, dc_1 c_2, c_3, \ldots, c_p \rangle \approx \langle d, c_3, \ldots, c_p, dc_1 c_2 \rangle$ but $\langle d, c_3, \ldots, c_p \rangle$represent b_1 because $b_1 = \underbrace{c_1 x_1^2 + c_2 x_2^2}_{d \cdot 1^2} + \cdots + c_p x_p^2 \Rightarrow (\langle d, c_1, \ldots, c_p, dc_1 c_2, c_{p+1}, \ldots, c_n \rangle, p - 1) \in P$ which contradicts minimality of $p \Rightarrow p = 1 \Rightarrow \exists \langle c_1, \ldots, c_p \rangle \approx \langle a_1, \ldots, a_n \rangle$and $\langle c_1 \rangle$ represents b_1, i.e., $b_1 = c_1 x^2 \Rightarrow \langle b_1 \rangle \cong \langle c_1 \rangle \Rightarrow \exists \langle b_1, c_2, \ldots, c_p \rangle \approx \langle a_1, \ldots, a_n \rangle$ □

2.4 Witt Groups:

Goal: Define $W(R)$ = abelian group to be {isometry classes of symmetric inner product space over R}/metabolic forms (=hyperbolic if $\frac{1}{2} \in R$) with group operation given by $\perp$

Definition 2.26. A symmetric inner product space (M, β) is called *metabolic* (or split) if $\exists$ direct summand $N \subseteq M$ such that $N = N^\perp$. Such a direct summand N is called *Lagrangian.*

Remark. $N \subseteq M$ is a direct summand if $\exists P \subseteq M$ such that $N \oplus P = M$ (i.e. $N + P = M$ and $N \cap P = 0$)

Example.

- $\mathbb{H} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ is metabolic with Lagrangian $\begin{pmatrix} 1 \\ 0 \end{pmatrix} : R \to R^2$ defined by $x \mapsto \begin{pmatrix} x \\ 0 \end{pmatrix}$.
i.e. $L = \{(x, 0) \in R^2 | x \in R\} \subset \mathbb{H}$ is a Lagrangian. Because

- L is a direct summand with complement $P = \{(0,y)|y \in R\} \subseteq \mathbb{H}$,
- $L^\perp = \{(x,y) \in R^2 | \underbrace{\underbrace{(z,0)}_{\in L} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0}_{zy=0\,\forall z \iff y=0} \forall z \in R\} = \{(x,y) \in R^2 | y = 0\} = L$

- I_n is the identity matrix in $M_n(R)$. $A \in M_n(R)$ then $\left\langle \begin{pmatrix} 0 & I_n \\ I_n & A_n \end{pmatrix} \right\rangle$ is metabolic with Lagrangian the image of the map $R^n \xrightarrow{\begin{pmatrix} I_n \\ 0 \end{pmatrix}} R^n \oplus R^n$ (proof is the same as above)
-

Lemma 2.27. *Let (M, β) be a symmetric inner product space then $(M, \beta) \perp (M, -\beta)$ is metabolic.*

Proof. The submodule $L = \{(x,x) \in M \oplus M | x \in M\} \subseteq M \perp M$ is a Lagrangian for $(M.\beta) \perp (M, -\beta)$ because

- L is a direct summand with complement $P = \{(y, 0) \in M^2 | y \in M\}$ as $L \cap P = 0$ and every element $(a,b) \in M^2$ is $(a,b) = \underbrace{(b,b)}_{\in L} + \underbrace{(a-b,0)}_{\in P}$ so $L \oplus P = L + P = M^2$
- $L = L^\perp$ because let $\begin{pmatrix} a \\ b \end{pmatrix} \in L^\perp \subseteq M^2 \iff \beta(a,x) - \beta(b,x) = 0 \,\forall x \in M \iff \beta(a-b, x) = 0 \,\forall x \in M \underset{\beta \text{ non degenerate}}{\iff} a - b = 0 \Rightarrow a = b \Rightarrow \begin{pmatrix} a \\ b \end{pmatrix} \in L$. Hence $L^\perp = L$

□

Definition 2.28. A free symmetric inner product space is called *hyperbolic* if it is isometric to $\mathbb{H}^n$

Note. M, N are metabolic (or hyperbolic) then so is $M \perp N$. If M, N are metabolic with Lagrangian $L_1 \subseteq M, L_2 \subseteq N$ then $M \perp N$ has Lagrangian $L_1 \perp L_2 \subseteq M \oplus N$.

$\left\langle \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \right\rangle \cong \mathbb{H}^n$ (by change of basis). Let the basis of the first one to be $e_1, \ldots, e_n, e_{n+1}, \ldots, e_{2n}$ then the basis of the second one is $(e_1, e_{n+1}), (e_2, e_{n+2}), \ldots (e_n, e_{2n})$ where each pairs gives a copy of $\mathbb{H}$

Lemma 2.29. *If $2 \in R^*$ then for all $A \in M_n(R)$, $\left\langle \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \right\rangle \cong \mathbb{H}^n$*

Proof. We need to find a base change, that is $\exists X \in M_n(R)$ which is invertible such that $X \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} X^T = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$. Take $X = \begin{pmatrix} I_n & 0 \\ -\frac{1}{2}A & I_n \end{pmatrix}$ which is invertible with inverse $X^{-1} = \begin{pmatrix} I_n & 0 \\ \frac{1}{2}A & I_n \end{pmatrix}$ □

Lemma 2.30. *Let R be a ring for which all finitely generated projective R-module are free (e.g.., R local or $R = \mathbb{Z}$) then any metabolic inner product space (M, β) is isometric to $\left\langle \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} \right\rangle$ for some $n \in \mathbb{N}$, and $A \in M_n(R)$. If moreover, $2 \in R^*$ then every metabolic space is hyperbolic.*

Proof. Let (M, β) be metabolic with Lagrangian $L \subseteq M$. $L \subseteq M$ being a direct summand $\Rightarrow P \subseteq M$ such that $L \cap P = 0$ and $L + P = M$. By assumption M projective $\Rightarrow P, L$ projective $\underset{\text{assumption on } R}{\Rightarrow} P, L$ are free. In a basis for L, and P, the inner product space β has inner product matrix $\begin{pmatrix} 0 & B \\ B^T & C \end{pmatrix}$, with $C = C^T$. The upper left corner is 0 because $L = L^\perp$ we have $\beta(x,x) = 0 \,\forall x \in L$.

Claim: The matrix B is invertible.

Proof of claim: B is the matrix of the linear map $P \underset{x \mapsto \beta(x,-)}{\to} L^* = \mathrm{Hom}_R(L, R)$ with respect to the basis of P and the dual basis of L. Need to show $P \to L^*$ defined by $x \mapsto \beta(x, -)$ is an isomorphism.

Injectivitiy: $x \in P : \beta(x,y) = 0 \,\forall y \in L \Rightarrow x \in L^\perp = L \Rightarrow x \in L \cap P = 0 \Rightarrow x = 0$

Surjectivity: Let $\phi \in L^*, \phi : L \to R$. Define $\bar{\phi} : M = L \oplus P \to P$ by $(x,y) \mapsto \phi(x)$. Now β is non-degenerate $\Rightarrow \exists \underset{\in L}{a}, \underset{\in P}{b} \in M = L \oplus P$ such that $\bar{\phi}(x,y) = \beta(a+b, x+y) \forall x \in L, y \in P \Rightarrow \phi(x) = \bar{\phi}(x,0) = \beta(a+b,x) = \underbrace{\beta(a,x)}_{=0 \text{ since } a,x \in L = L^\perp} + \beta(b,x) = \beta(b,x) \forall x \in L$. So $b \in P$ is sent to ϕ under the map $P \to L^*$. This shows surjectivity.

Notice that $\begin{pmatrix} 0 & I_n \\ I_n & (B^T)^{-1}CB^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & (B^T)^{-1} \end{pmatrix} \begin{pmatrix} 0 & B \\ B^T & C \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & B^{-1} \end{pmatrix} \Rightarrow M \cong \left\langle \begin{pmatrix} 0 & B \\ B^T & C \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} \right\rangle$. For $A = (B^T)^{-1}CB^{-1}$ □

Note. If $2 \in R^*$ then $\left\langle \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} \right\rangle \cong \mathbb{H}^n$

Corollary 2.31. *Over a local ring R, every metabolic space has even dimension and if $2 \in R^*$, R local, then every metabolic space is hyperbolic*

Definition 2.32. Let M, N be symmetric inner product spaces over R then M are N are called *Witt Equivalent* ($M \sim N$) if $\exists$ metabolic spaces P, Q such that $M \perp P \cong N \perp Q$. Denote by $W(R)$ be the set of Witt equivalence classes $[M]$ of symmetric inner product spaces M over R

Lemma 2.33 (**Definition**)**.** *Orthogonal sum $\perp$ makes $W(R)$ into an abelian group with $0 = [0], [M] + [N] = [M \perp N]$ and $-[M, \beta] = [M, -\beta]$. $W(R)$ is called the* Witt group of R.

Proof.
- "$+$" is well defined because if $M \sim M', N \sim N'$ then $\exists P, P', Q, Q'$ metabolic such that $M \perp P \cong M' \perp P', N \perp Q \cong N' \perp Q'$. Then $(M \perp N) \perp \underbrace{(P \perp Q)}_{\text{metabolic}} \cong (M' \perp N') \perp \underbrace{(P' \perp Q')}_{\text{metabolic}} \Rightarrow M \perp N \sim M' \perp N'$
- We have $[M] + [N] = [M \perp N] = [N \perp M] = [N] + [M]$ (since $M \perp N \cong N \perp M$) and the group law is commutative
- $[0] + [M] = [0 + M] = [M]$ because $0 \perp M \cong M$
- $[M, \beta] + [M, -\beta] = [(M, \beta) \perp (M, -\beta)] = 0$ because $(M, \beta) \perp (M, -\beta)$ is metabolic for any inner product space (M, β).

□

Remark. W : (commutative) rings $\to$ abelian groups, defined by $R \mapsto W(R)$ is a functor. For $f : R \to S$ a ring homomorphism, we define a map of abelian groups $W(f) : W(R) \to W(S)$ by $[M, \beta] \mapsto [M_S, \beta_S]$ where $M_S = S \otimes_R M$ and $\beta_S : M_S \times M_S \to S$ is defined $s_1 \otimes x_1, s_2 \otimes x_2 \mapsto s_1 s_2 \beta(x_1, x_2)$. Note that if (M, β) is non-degenerate then so is (M_S, β_S) : if M is free choose an R-basis of M, say $x_1, \dots, x_n \in M$ then M_S is free with S-basis $1 \otimes x_1, \dots, 1 \otimes x_n$. Then (M, β) non-degenerate $\iff$ $(\beta(x_i, x_j)) \in M_n(R)$ is invertible $\underset{f : R^* \to S^*}{\Rightarrow}$ $(f(\beta(x_i, x_j)) = (\beta_S(1 \otimes x_i, 1 \otimes x_j)) \in M_n(S)$ is invertible $\iff$ (M_S, β_S) is non-degenerate. In the case (M, β) is projective do it as an exercise

For $R \xrightarrow{g} S \xrightarrow{f} T$ ring homomorphism, note that $W(f) \circ W(g) = W(f \circ g)$ because $T \otimes_S (S \otimes_R M) \cong \underbrace{(T \otimes_S S)}_{\substack{\cong T \\ x \otimes y \mapsto x f(y)}} \otimes_R M \cong T \otimes_R M$

Proposition 2.34. *Let R be a local ring with $2 \in R^*$. Then two symmetric inner product spaces M, N are isometric if and only if rank M = rank N and $[M] = [N] \in W(R)$*

Proof. "$\Rightarrow$": Obvious

"$\Leftarrow$": $[M] = [N] \in W(R) \Rightarrow M \sim N \Rightarrow \exists$ metabolic P, Q such that $M \perp P \cong N \perp Q$. R local, $2 \in R^* \Rightarrow$ metabolic = hyperbolic so $P \cong \mathbb{H}^p, Q \cong \mathbb{H}^q$. Now rank M = rank N and rank $M \perp P$ = rank $N \perp Q \Rightarrow p = q \Rightarrow M \perp \mathbb{H}^p \cong N \perp \mathbb{H}^p$ so by Witt cancellation $\Rightarrow M \cong N$. □

Definition 2.35. Let R be a local ring. The rank homomorphism $\operatorname{rk}: W(R) \to \mathbb{Z}/2\mathbb{Z}$ is defined by $[M] \mapsto \operatorname{rank} M$. Note this map is well defined as $M \sim 0 \iff \exists P$ metabolic such that $M \perp P$ is metabolic$\Rightarrow M \perp P$ and P have even rank $\Rightarrow \operatorname{rk} M = 0 \in \mathbb{Z}/2\mathbb{Z}$. The rank map is surjective because $\operatorname{rk}(\langle 1 \rangle) = 1$.

Let $I(R) = \ker(\operatorname{rk})$ =set of equivalence classes of even rank inner product spaces

The *discriminant* is the homomorphism disc: $I(R) \to R^*/R^{2*}$ defined by $[M] \mapsto (-1)^{\frac{\operatorname{rk} M}{2}} \det M$ which is well defined because disc $P = 1$ for P metabolic as $\det \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} = (-1)^n$

Note that disc map is surjective because $\operatorname{disc}(\langle u, -1 \rangle) = u \, \forall u \in R^*$

Proposition 2.36. *Let F be a field in which every element is a square (e.g. F algebraic closed, or char $F = 2$ and F perfect, e.g., finite and char $F = 2$) then $\operatorname{rk}: W(F) \overset{\cong}{\to} \mathbb{Z}/2\mathbb{Z}$ is an isomorphism.*

Proof. $\operatorname{rk}: W(F) \to \mathbb{Z}/2\mathbb{Z}$ is surjective (for any commutative ring) since $\langle 1 \rangle \mapsto 1$. Recall that every symmetric inner product space over F a field is isometric to $\langle u_1 \rangle \perp \cdots \perp \langle u_l \rangle \perp N_1 \perp \cdots \perp N_r$ with $N_i = \mathbb{H}$ (in the case of a field). So $W(F)$ is generated by $\langle u \rangle, u \in F^*/F^{2*}$ as an abelian group. Consider the map $\mathbb{Z} \to W(F)$ defined by $1 \mapsto \langle 1 \rangle$. Since $\langle 1 \rangle + \langle 1 \rangle = \langle 1 \rangle + \langle -1 \rangle$ (as $-1 \in F^{2*}$), we have $\langle 1 \rangle + \langle 1 \rangle = 0 \Rightarrow$ This map factors as $\mathbb{Z}/2\mathbb{Z} \to W(F)$ with $1 \mapsto \langle 1 \rangle$. As $W(F)$ is generated by $\langle u \rangle, u \in F^*/F^{2*} = \{1\}$ this means that the map $\mathbb{Z}/2\mathbb{Z} \to W(F)$ is surjective and it is injective as $\mathbb{Z}/2\mathbb{Z} \twoheadrightarrow W(F) \overset{\operatorname{rk}}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z}$ sends $\underbrace{1 \mapsto \langle 1 \rangle \mapsto 1}_{\text{id}} \Rightarrow \mathbb{Z}/\mathbb{Z}2 \overset{\cong}{\to} W(F) \Rightarrow W(F) \underset{\cong}{\overset{\operatorname{rk}}{\to}} \mathbb{Z}/2\mathbb{Z}$ $\square$

Corollary 2.37. *$W(\mathbb{F}_q) = \mathbb{Z}/2\mathbb{Z}$ for q even,* $\operatorname{rk}: W(\mathbb{C}) \overset{\cong}{\to} \mathbb{Z}/2\mathbb{Z}$

Example. $W(\mathbb{R}) \to \mathbb{Z}$ defined by $[M] \mapsto \operatorname{sgn} M$ is well defined because $\operatorname{sgn}(\mathbb{H}) = 0$

Claim: $\operatorname{sgn}: W(\mathbb{R}) \overset{\cong}{\to} \mathbb{Z}$ is an isomorphism

Surjective: $\operatorname{sgn}(n \langle 1 \rangle) = n \operatorname{sgn}(\langle 1 \rangle) = n \cdot 1 = n$

Injectivitiy: Every symmetric inner product space over $\mathbb{R}$ is $M \cong n \langle 1 \rangle + m \langle -1 \rangle$. If $\operatorname{sgn} M = \operatorname{sgn}(n \langle 1 \rangle + m \langle -1 \rangle) = n - m$ then $n = m \Rightarrow M = n(\langle 1 \rangle + \langle -1 \rangle) = 0 \in W(\mathbb{R})$

Recall:

- $I(F) = \ker(W(F) \overset{\operatorname{rk}}{\to} \mathbb{Z}/2\mathbb{Z}) =$ "*fundamental ideal*"
- $I(F) \overset{\text{disc}}{\to} F^*/F^{2*}$ map of abelian groups defined by $M \mapsto (-1)^{\frac{\operatorname{rk} M}{2}} \det M$

Note. The disc map extends to all of $W(F)$ by $W(F) \to F^*/F^{2*}$ defined by $M \mapsto (-1)^{\frac{r(r-1)}{2}} \det M$, where $r = \operatorname{rk} M$, but, in general, this is not a map of abelian groups so we don't often use this.

Proposition 2.38. *Let F be a finite field. Then the discriminant map is an isomorphism: $I(F) \overset{\cong}{\to} F^*/F^{2*}$*

Proof. If char $F = 2$ this is true because both sides are equal to 0. (Since F finite and char $F = 2 \Rightarrow F^*/F^{2*} = 0$)

So assume char F is odd. We have to prove the following special case

Claim: $\langle a, b \rangle \cong \langle ab, 1 \rangle$

The claim implies the proposition: define the map $\rho: F^*/F^{2*} \to I(F)$ by $a \mapsto \langle a, -1 \rangle$ this is easily seen to be a well defined map of <u>sets</u>. This is a map of abelian groups because $\rho(ab) = \langle ab, -1 \rangle = \langle ab \rangle + \langle -1 \rangle = \langle ab \rangle + \langle 1 \rangle + \overline{\langle -1 \rangle + \langle -1 \rangle} = \langle ab, 1 \rangle + \langle -1 \rangle + \langle -1 \rangle \underset{\text{claim}}{=} \langle a, b \rangle + 2 \langle -1 \rangle = \langle a, -1 \rangle + \langle b, -1 \rangle = \rho(a) + \rho(b)$. The maps is surjective because every $\langle a_1, \ldots, a_{2n} \rangle \in I(F)$ is $\langle a_1, \ldots, a_{2n} \rangle = \langle a_1 \ldots a_{2n}, 1, 1, \ldots, 1 \rangle \underset{\text{claim}}{=} \langle a_1 \ldots a_{2n}, -1 \rangle + 2n \langle 1 \rangle = \rho(a_1 \ldots a_{2n}) + n\rho(-1)$ because $\rho(-1) = \langle -1, -1 \rangle \underset{\text{claim}}{=} \langle 1, 1 \rangle$. The map ρ is injective because $F^*/F^{2*} \overset{\rho}{\to} I(F) \overset{\text{disc}}{\to} F^*/F^{2*}$ defined by $\underbrace{a \mapsto \langle a, -1 \rangle \mapsto a}_{\text{id}}$, hence we are done.

Proof of claim: Recall: $\langle a, b \rangle \cong \langle c, d \rangle \iff ab = cd \in F^*/F^{2*}$ and $\exists e \in F$ such that e is represented by both forms. Obviously $\langle a, b \rangle \cong \langle ab, 1 \rangle$ has the same determinant, so the claim is equivalence to the fact, since $\langle ab, 1 \rangle$represent 1, that $\langle a, b \rangle$ represent 1, i.e., $\exists x, y \in F$ such that $1 = ax^2 + by^2$. This follows from the following lemma

Lemma 2.39. *Let F be a finite field of order q =odd. Then $\forall a, b \in F^*$ the equation $1 = ax^2 + by^2$ has a solution $x, y \in F$*

Proof. Need to find x, y such that $1 - by^2 = ax^2$. We use the pigeon hole principle.

Let $\varphi : F^* \to F^* : x \mapsto x^2$ hence $F^{2*} = \operatorname{im}\varphi = F^*/\ker(\varphi) = F^*/\{\pm 1\}$ (The last equality holds since char $F \neq 2$)$\Rightarrow |(F^{2*})| = \frac{|F^*|}{2} = \frac{q-1}{2} \Rightarrow$ number of square in $F = |F^{2*}|+1$ (for zero) $= \frac{q+1}{2}$. Hence $n_1 = |\{ax^2 | x \in F\}| = |\{x^2 | x \in F\} = \frac{q+1}{2}$. Similarly $n_2 = |\{1 - by^2 | y \in F\}| = |\{y^2 | y \in F\} = \frac{q+1}{2}$. Hence $n_1 + n_2 = q + 1 > |F| \Rightarrow \{ax^2 | x \in F\} \cap \{1 - by^2 | y \in F\} \neq \emptyset \Rightarrow 1 - by^2 = ax^2$ has a solution. □

□

Theorem 2.40. *Let F be a finite field with q elements then*

$$W(F) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & \textit{char } F = 2 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & q \equiv 1 \mod 4 \ (\iff -1 \in F^{2*}) \\ \mathbb{Z}/4\mathbb{Z} & q \equiv 3 \mod 4 \ (\iff -1 \notin F^{2*}) \end{cases}$$

Proof. char $F = 2$ we have already done (in this case $\operatorname{rk} : W(F) \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z}$)

Assume char F odd, so q odd. We have an exact sequence

$$0 \to \underbrace{I(F)}_{\cong F^*/F^{2*}} \to W(F) \xrightarrow{\mathrm{rk}} \mathbb{Z}/2\mathbb{Z} \to 0$$

Since q is odd we have $|F^*/F^{2*}| = 2$ because $F^{2*} = \operatorname{im}(F^* \underset{x \mapsto x^2}{\overset{\cdot^2}{\to}} F^*)$ and $\ker(F^* \overset{\cdot^2}{\to} F^*) = \{\pm 1\}$. $\Rightarrow |W(F)| = 4 \Rightarrow$(by the structure theorem of finite groups) $W(F) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $W(F) = \mathbb{Z}/4\mathbb{Z}$.

If $-1 \in F^{2*}, (-1 = a^2), \Rightarrow 2\langle u \rangle = \langle u \rangle + \langle u \rangle = \langle u \rangle + \langle a^2 u \rangle = \langle u \rangle + \langle -u \rangle = 0 \in W(F) \, \forall u \in F^*$. $W(F)$ generated as an abelian group by $\langle u \rangle, u \in F^* \Rightarrow$ every element in $W(F)$ has order ≤ 2. $\Rightarrow W(F) \neq \mathbb{Z}/4\mathbb{Z} \Rightarrow W(F) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

If $-1 \notin F^{2*} \Rightarrow$ if $2\langle 1 \rangle = 0 \in W(F)$ then $\langle 1 \rangle + \langle 1 \rangle = \langle 1 \rangle + \langle -1 \rangle \in W(F) \underset{\text{char } F \text{ odd}}{\Rightarrow} \langle 1 \rangle + \langle 1 \rangle \cong \langle 1 \rangle + \langle -1 \rangle \underset{\text{Witt Cancellation}}{\Rightarrow} \langle 1 \rangle \cong \langle -1 \rangle \Rightarrow 1 = \det\langle 1 \rangle = \det\langle -1 \rangle = -1 \in F^*/F^{2*} \Rightarrow -1 \in F^{2*}$ which is a contradiction to the assumption $-1 \notin F^{*2} \Rightarrow 2\langle 1 \rangle \neq 0 \Rightarrow W(F) \neq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \Rightarrow W(F) = \mathbb{Z}/4\mathbb{Z}$. (Then the theorem follows from the following lemma) □

Lemma 2.41. *Let F be a finite field of odd characteristic, with $q = |F|$ elements. Then $-1 \in F^{2*} \iff q \equiv 1 \mod 4$.*

Proof. $-1 \in F^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$ is the only element of order 2. $\Rightarrow -1 \in F^{2*} \iff F^* = \mathbb{Z}/(q-1)\mathbb{Z}$ has an element of order 4 $\iff 4|(q-1) \iff q \equiv 1 \mod 4$. □

Remark. $p \in \mathbb{Z}$ is an odd prime, then p can be written as $p = a^2 + b^2$ with $a, b \in \mathbb{Z} \iff -1$ is a square in $\mathbb{F}_p$ ($\iff p \equiv 1 \mod 4$)

To see this: $a^2 + b^2 = (a + ib)(a - ib) \in \mathbb{Z}[i]$. Recall that $\mathbb{Z}[i]$ is a Euclidean domain, hence a UFD (unique factorization domain) and thus, irreducible elements and prime elements are the same. If $a^2 + b^2 = (a + ib)(a - ib) \in \mathbb{Z}[i]$, we have $p = a^2 + b^2 \Rightarrow p$ not prime in $\mathbb{Z}[i]$. The converse also holds: if p is not a prime in $\mathbb{Z}[i]$ then $p = xy \in \mathbb{Z}[i]$ for non-units $x, y \in \mathbb{Z}[i]$. But then (if $x = a + ib$) $N(x) = a^2 + b^2$ has the properties $N(xy) = N(x)N(y), N(x) = 1 \iff x$ unit. So $p = xy \Rightarrow \underbrace{N(p)}_{=p^2} = N(x)N(y) \Rightarrow N(x) = p = N(y) \Rightarrow a^2 + b^2 = N(x) = p$. So p can be written as $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$ $\iff p$ is not a prime in $\mathbb{Z}[i]$. But p is a prime in $\mathbb{Z}[i] \iff \mathbb{Z}[i]/p$ is a domain. But $\mathbb{Z}[i] = \mathbb{Z}[t]/(t^2 + 1)$ so $\mathbb{Z}[i]/p = \mathbb{Z}[t]/(t^2 + 1, p) = \frac{\mathbb{Z}}{p}[t]/(t^2 + 1) = \mathbb{F}_p[t]/(t^2 + 1)$. Now $\mathbb{F}_p[t]/(t^2 + 1)$ is a field $\iff t^2 + 1$ irreducible $\iff t^2 + 1$ has no solution in $\mathbb{F}_p \iff -1 \notin \mathbb{F}_p^{2*}$. On the other hand $t^2 + 1$ reducible $\iff -1 \in \mathbb{F}_p^{2*}, -1 = a^2, t^2 + 1 = (t + a)(t - a)$. Then $\mathbb{F}[t]/(t^2 + 1) = \mathbb{F}_p[t]/((t - a)(t + a)) \underset{\text{CRT}}{=} \mathbb{F}_p[t]/(t + a) \times \mathbb{F}_p[t]/(t - a) = \mathbb{F}_p \times \mathbb{F}_p$ not a domain.

Hence $p = a^2 + b^2 \iff p$ not a prime in $\mathbb{Z}[i] \iff \mathbb{Z}[i]/p = \mathbb{F}_q[t]/(t^2 + 1)$ not a domain $\iff -1 \in \mathbb{F}_p^{2*} \iff p \equiv 1 \mod 4$ □

Corollary 2.42 (of Theorem 2.40). *Two symmetric inner product spaces over a finite field of odd characteristic are isometric if and only if they have the same rank and the same determinant* ($\in F^*/F^{2*}$).

Theorem 2.43. *Let F be a field then $W(F)$ is generated as an abelian group by $\langle u\rangle, u \in F^*$ subject to the relations:*

1. $\langle u\rangle = \langle a^2u\rangle \; \forall a, u \in F^*$
2. $\langle u\rangle + \langle -u\rangle = 0 \, \forall u \in F^*$
3. $\langle u\rangle + \langle v\rangle = \langle u+v\rangle + \langle uv(u+v)\rangle \; \forall u, v \in F^*, u+v \in F^*$

Remark. The theorem asserts that

$$\frac{\bigoplus_{a\in F^*} \overbrace{\mathbb{Z}\{a\}}^{\text{rank 1 free abelian group with basis } \{a\}}}{\{u\} - \{a^2u\}, \{u\} + \{-u\}, \{u\} + \{v\} - \{u+v\} - \{uv(u+v)\}} \overset{\cong}{\to} W(F)$$

defined by $\{a\} \mapsto \langle a\rangle$ is an isomorphism. (Here $\mathbb{Z}\{a\} \cong \mathbb{Z}$ denotes the free $\mathbb{Z}$-module of rank 1 with basis $\{a\}$.)

Proof. We already know that $W(F)$ is generated by $\langle u\rangle, u \in F^*$ and that $1, 2, 3$ holds in $W(F) \Rightarrow$

$$\rho : \frac{\bigoplus_{a\in F^*} \overbrace{\mathbb{Z}\{a\}}^{\text{rank 1 f.a.g.w/ basis } \{a\}}}{\{u\} - \{a^2u\}, \{u\} + \{-u\}, \{u\} + \{v\} - \{u+v\} - \{uv(u+v)\}} \to W(F)$$

is a well defined surjective map of abelian groups. So we need to check that ρ is injective. Will give a proof when char $F \neq 2$ (the char $F = 2$ case needs a different, longer proof)

Using relation 2. ($\{u\} = -\{-u\}$) we can write every element in LHS as $\sum_{i=1}^n \{u_i\}$. Given $U = \sum_{i=1}^n \{u_i\}$ and $V = \sum_{j=1}^m \{v_j\}$ in the LHS such that $\rho(U) = \rho(V) \in W(F) \Rightarrow n = \text{rk}\ \rho(u) = \text{rk}\ \rho(V) = m \in \mathbb{Z}/2\mathbb{Z}$. So $m \equiv n \mod 2$ and without loss of generality say $m \geq n$ so $m - n = 2k, k \geq 0$. Then $U = U + k\underbrace{(\{1\} + \{-1\})}_{=0 \text{ by } 2.} \in$ LHS. Replacing $U \in$ LHS with $U + k(\{1\}+\{-1\})$ we can assume that $m = n$. Then $\rho(U) = \rho(V) \in W(F)$ and $\text{rk}\,\rho(U) = \text{rk}\,\rho(V)$. $\underset{\frac{1}{2}\in F^*}{\Rightarrow}$ $\langle u_1, \ldots, u_n\rangle \cong \langle v_1, \ldots, v_n\rangle \underset{\text{chain equivalence thm}}{\Rightarrow}$ $\langle u_1, \ldots, u_n\rangle \approx \langle v_1, \ldots, v_n\rangle \Rightarrow \exists$ diagonal forms $c_1, \ldots, c_l$ such that $\langle u_1, \ldots u_n\rangle \approx_S c_1 \approx_S \cdots \approx_S c_l \approx_S \langle v_1, \ldots, v_n\rangle \Rightarrow$ it suffices to show that $\{u_1\} + \cdots + \{u_n\} = \{v_1\} + \cdots + \{v_n\}$ in the case $\langle u_1, \ldots, u_n\rangle, \langle v_1, \ldots, v_n\rangle$ are simply chain equivalence (i.e., they differ in two places). So, we can assume $n = 2$, we need to show that $\langle u_1, u_2\rangle \cong \langle v_1, v_2\rangle$ then $\{u_1\} + \{u_2\} = \{v_1\} + \{v_2\}$ in LHS. Assume $\langle u_1, u_2\rangle \cong \langle v_1, v_2\rangle \Rightarrow u_1u_2 = v_1v_2a^2$ for some $a \in F^*$ and $u_1 = v_1x^2 + v_2y^2$ for some $x, y \in F$. If $x, y \neq 0$ then $\{v_1\} + \{v_2\} \underset{1.}{=} \{v_1x^2\} + \{v_2y^2\} \underset{3.}{=} \{v_1x^2 + v_2y^2\} + \{v_1v_2x^2y^2(v_1x^2 + v_2y^2)\} = \{u_1\} + \{\frac{1}{a^2}u_1u_2x^2y^2u_1\} \underset{1}{=} \{u_1\} + \{u_2\} \in$ LHS. If x or $y = 0$, say $x = 0$ then $y \neq 0$ since $u_1 \in F^*$, then we get $u_1 = v_2y^2$ and $v_1v_2a^2 = v_2y^2u_2 \Rightarrow v_1(\frac{a}{y})^2 = u_2$. Then $\{u_1\}+\{u_2\} = \{v_2y^2\}+\{v_1(\frac{a}{y})^2\} \underset{1.}{=} \{v_2\}+\{v_1\} \in$ LHS.

So $\rho(U) = \rho(V) \in W(F) \Rightarrow U = V \in$ LHS$\Rightarrow \rho$ injective □

2.5 Second Residue Homomorphism

For a DVR (*Discrete valuation ring*) R with field of fraction F, residue field $k = R/m$ and uniformizing element $\pi \in R$, we will construct maps $\partial_\pi : W(F) \to W(k)$ which will help compute $W(\mathbb{Q}), W(\mathbb{Z}), W(\mathbb{Q}_p) \ldots$

Definition 2.44. A *discrete valuation ring* (DVR) is a local ring (R, m, k) which is:

- Noetherian
- A domain ($ab = 0 \in R \Rightarrow a = 0$ or $b = 0$)

- $m \neq 0$ is a principal ideal ($m = \pi R$ for some $\pi \in R$)

There are other (equivalent) characterizations of DVR (which we won't need):

- R is a DVR $\iff$ local 1-dimensional integrally closed noetherian domain
- $\iff$ Local 1-dimensional noetherian regular domain
- $\iff$ Local PID
- $\iff$ Local domain with principal m such that $\cap_{n \geq 0} m^n = 0$
- $\iff$ valuation ring of a discrete valuation on a field

Example (Of DVR).

- $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} | p \nmid a\}$, $p \in \mathbb{Z}$ prime. $m = p\mathbb{Z}_{(p)}, k = \mathbb{F}_p$. Fraction field $\mathbb{Q}$.
- The p-adic integers $\mathbb{Z}_p = \lim\limits_{\substack{\leftarrow \\ n \to \infty}} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n \in \mathbb{N}_{\geq 1}}, x_n \in \mathbb{Z}/p^n\mathbb{Z} : x_{n+1} = x_n \mod p^n\}$, $m = p\mathbb{Z}_p, k = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ and field of fractions $\mathbb{Z}_p = \mathbb{Q}_p$
- $D =$ Dedekind domain, $p \subset D$ a prime ideal then $D_p = \{\frac{a}{b} \in \mathrm{Frac} D | b \notin p\}$, $m = pD_p, k = D/p$
- K is a field, $f \in K[T]$ is irreducible. $K[T]_{(f)} = \{\frac{a}{b} \in \mathrm{Frac}(K[T]) = K(T) | f \nmid b\}$, $m = fK[T]_{(f)}, k = K[T]/f$.
- R is a UFD, $f \in R$ an irreducible element (=prime element) $R_{(f)} = \{\frac{a}{b} \in \mathrm{Frac}\ R | f \nmid b\}$

Definition 2.45. Let (R, m, k) be a DVR, a *uniformizing element* of R is a choice $\pi \in m \subset R$ generating m, i.e. $\pi R = m$

Lemma 2.46. *Let R be a DVR with uniformizing element $\pi \in R$, then every element $a \in R, a \neq 0$ can be written uniquely as $a = \pi^n u$ for some $n \in \mathbb{N}$ and $u \in R^*$*

Proof. Uniqueness :Assume $\pi^n u = \pi^m v$ with $u, v \in R^*$. Without loss of generality assume $m \geq n$. R domain $\Rightarrow \pi^{m-n} = vu^{-1} \in R$. If $m \neq n \Rightarrow \pi^{n-m} \in \pi R = m$ but $vu^{-1} \in R^* = R \setminus m$ which is a contradiction $\Rightarrow n = m \Rightarrow 1 = vu^{-1} \Rightarrow u = v$

Existence :Let $a \in R$, $a \neq 0$. If $a \in \cap_{n \geq 0} m^n = \cap_{n \geq 0} \pi^m R$ then $a = \pi^n b_n \, \forall n$. $\underset{R\,\text{domain}}{\Rightarrow}$ $b_n = \pi b_{n+1} \Rightarrow (b_n) \subset (b_{n+1}) \subset (b_{n+2}) \subset \ldots R$, is an ascending chain of ideals which has to stop because R is noetherian. $\exists n$ such that $(b_n) = (b_{n+1})$ in particular $b_{n+1} \in (b_n) \Rightarrow b_{n+1} = cb_n$ but $b_n = \pi b_{n+1}$ $\underset{R\,\text{domain}}{\Rightarrow}$ $1 = c\pi \Rightarrow \pi \in R^* = R \setminus m$ which contradicts the fact that $\pi \in m$. Hence $a = 0 \Rightarrow \cap_{n \geq 0} \pi^n R = 0$. Hence $\exists n$ such that $a \in \pi^n R$ but $a \notin \pi^{n+1} R \Rightarrow a = \pi^n u, u \notin \pi R = m$ hence $u \in R^*$. ☐

Remark. $\cap_{n \geq 0} \pi^n R = \cap_{n \geq 0} m^n$. For all Noetherian $R : \cap_{n \geq 0} m^n = 0$

Corollary 2.47. *Let R be a DVR with uniformizing element π and F its field of fractions, then every $a \in F, a \neq 0$ can be written uniquely as $a = \pi^n u$ where $u \in R^*$.*

So we can define a function $\nu : F^* \to \mathbb{Z}$ defined by $a = \pi^n u \mapsto n = \nu(a)$ (with $u \in R^*$) with the properties

1. $\nu(ab) = \nu(a) + \nu(b)$
2. $\nu(a + b) \geq \min(\nu(a), \nu(a))$
3. Setting $\nu(0) = \infty$ we have $R = \{a \in F : \nu(a) \geq 0\}$, $R^* = \{a \in F | \nu(a) = 0\}$, $m = \{a \in F | \nu(a) > 0\}$

Definition 2.48. A *discrete valuation* on a field F is a function $\nu : F^* \to \mathbb{Z}$ satisfying 1., 2. above.
The valuation ring of ν is the ring $R = \{a \in F | \nu(a) \geq 0\}$ where $\nu(0) = \infty$.

Definition 2.49. Let (F, ν) be a discrete valuation on a field F with associated DVR R and choice of uniformizing element $\pi \in R$. The *second residue homomorphism* is the map $\partial_\pi : W(F) \to W(R/\pi)$ defined by

$$\langle a \rangle \mapsto \begin{cases} \langle \underline{u} \rangle & n = \nu(a)\,\text{odd} \\ 0 & n = \nu(a)\,\text{even} \end{cases}$$

where $a \in F^*$, $a = \pi^n u, n = \nu(a), u \in R^*, \underline{u} = u \mod m = \pi R$, $u \in R/\pi$

Note. ∂ depends on the choice of the uniformizing element π.

Lemma 2.50. *The second residue homomorphism is well defined*

Proof. Recall that $W(F)$ is generated by $\langle a\rangle$, $a \in F^*$ subject to:

1. $\langle u\rangle = \langle x^2 u\rangle$, $u, x \in F^*$
2. $\langle u\rangle + \langle -u\rangle = 0$
3. $\langle u\rangle + \langle v\rangle = \langle u+v\rangle + \langle uv(u+v)\rangle$, $u, v, u+v \in F^*$

We need to check that ∂_π preserves these relations. First define $\epsilon_i = \begin{cases} 0 & i \text{ even} \\ 1 & i \text{ odd} \end{cases}$, so that we can write $\partial\langle u\rangle = \epsilon_{\nu(u)}\langle \underline{\phi}\rangle$ where $u = \pi^{\nu(u)}\phi, \phi \in R^*, \underline{\phi} = \phi \mod \pi R$. Then:

1. Let $u = \pi^n\phi, x = \pi^m\psi$ where $\phi, \psi \in R^*$. Then $x^2u = \pi^{2m+n}\phi\psi^2$ so $\partial\langle x^2u\rangle = \epsilon_{2m+n}\langle \underline{\phi\psi^2}\rangle = \epsilon_n\langle\underline{\phi}\rangle \in W(R/\pi)$ as required $\partial\langle u\rangle = \epsilon_n\langle\underline{\phi}\rangle$.
2. Let $u = \pi^n\phi, -u = \pi^n(-\phi)$ with $\phi \in R^*$. Then $\partial\langle u\rangle + \partial\langle -u\rangle = \epsilon_n\langle\underline{\phi}\rangle + \epsilon_n\langle\underline{-\phi}\rangle = \epsilon_n(\underbrace{\langle\underline{\phi}\rangle + \langle\underline{-\phi}\rangle}_{=0}) = 0 \in W(R/\pi)$
3. Let $u = \pi^n\phi, v = \pi^m\psi$, without loss of generality assume $n \geq m$. $u+v = \pi^n\phi + \pi^m\psi = \pi^m(\pi^{n-m}\phi + \psi)$

   Case 1. $n > m$: Then $n - m > 0 \Rightarrow t = \underbrace{\pi^{n-m}\phi}_{\in m} + \underbrace{\psi}_{\notin m} \in R^*, u+v = \pi^m t$, note that $t \equiv \psi \mod \pi R$. Now $uv(u+v) = \pi^{n+2m}\underbrace{\phi\psi t}_{\in R^*}$. So $\partial\langle u+v\rangle + \partial\langle uv(u+v)\rangle = \epsilon_m\langle\underline{t}\rangle + \epsilon_{n+2m}\langle\underline{\phi\psi t}\rangle = \epsilon_m\langle\underline{\psi}\rangle + \epsilon_n\langle\underline{\phi\psi^2}\rangle = \partial\langle v\rangle + \partial\langle u\rangle$

   Case 2. $n = m$: Now $u+v = \pi^n(\phi+\psi)$ and $\phi + \psi = \pi^l t$ where $t \in R^*$.

   Case i. $l = 0$: $\phi + \psi = t \in R^*$. Now $u + v = \pi^n t$ and $uv(u+v) = \pi^{3n}\underbrace{\phi\psi t}_{\in R^*}$. Then $\partial\langle u+v\rangle + \partial\langle uv(u+v)\rangle = \epsilon_n\langle\underline{t}\rangle + \epsilon_{3n}\langle\underline{\phi\psi t}\rangle = \epsilon_n\langle\underline{\phi} + \underline{\psi}\rangle + \epsilon_n\langle\underline{\phi\psi}(\underline{\phi}+\underline{\psi})\rangle = \epsilon_n(\langle\underline{\psi}\rangle + \langle\underline{\phi}\rangle) \in W(R/\pi)$ which is what we wanted.

   Case ii. $l > 0$: $u + v = \pi^{l+n}t \in \pi R$. In particular $\underline{\psi} + \underline{\phi} = 0$ so $\underline{\psi} = -\underline{\phi} \in R/\pi R$. So $uv(u+v) = \pi^{3n+l}\phi\psi t$. Then $\partial\langle u+v\rangle + \partial\langle uv(u+v)\rangle = \epsilon_{n+l}\langle\underline{t}\rangle + \epsilon_{3n+l}\langle\underline{\phi\psi t}\rangle = \epsilon_{n+t}\langle\underline{t}\rangle + \epsilon_{n+l}\partial\langle -\underline{\psi}^2\underline{t}\rangle = \epsilon_{n+l}(\langle\underline{t}\rangle + \langle\underline{-t}\rangle) = 0 = \epsilon_n(\langle -\underline{\psi}\rangle + \langle\underline{\psi}\rangle) = \epsilon_n\langle\underline{\phi}\rangle + \epsilon_n\langle\underline{\psi}\rangle = \partial\langle u\rangle + \partial\langle v\rangle$

□

Theorem 2.51. *Let D be a Dedekind domain with field of fractions F. Then the sequence of abelian group*

$$0 \longrightarrow W(D) \longrightarrow W(F) \overset{\oplus\partial_\wp}{\longrightarrow} \bigoplus_{\substack{\wp \subset D \\ \text{max. ideal}}} W(D/\wp)$$

is exact.

We will prove the above theorem in the special cases: $D = \mathbb{Z}$, DVR, $k[T]$.

Lemma 2.52. *Let (R, m, k) be a DVR with field of fraction k and uniformizing element $\pi \in m \subset R$. Then the composition*

$$W(R) \longrightarrow W(F) \xrightarrow{\partial_\pi} W(R/\pi)$$

is zero

Proof. R local $\Rightarrow W(R)$ is generated by $\langle u\rangle, u \in R^*$ and $\left\langle\begin{pmatrix} a & 1 \\ 1 & b\end{pmatrix}\right\rangle, a, b \in m$. We have $\partial\langle u\rangle = 0$ by definition of ∂: $\partial\langle u\rangle = \begin{cases} 0 & \nu(u)\,\text{even} \\ \langle \underline{v}\rangle & \nu(u)\,\text{odd}\end{cases}$ where $u = \pi^{\nu(u)}v, v \in R^*$.

If $a = 0$ then $\left\langle\begin{pmatrix} 0 & 1 \\ 1 & b\end{pmatrix}\right\rangle$ is metabolic so, $W(F) \ni \left\langle\begin{pmatrix} a & 1 \\ 1 & b\end{pmatrix}\right\rangle = 0 \Rightarrow \partial\left\langle\begin{pmatrix} a & 1 \\ 1 & b\end{pmatrix}\right\rangle = 0$

If $a \neq 0$ then $a \in F^*$ so $\left\langle\begin{pmatrix} a & 1 \\ 1 & b\end{pmatrix}\right\rangle = \langle a\rangle + \langle a(ab-1)\rangle, a = \pi^{\nu(a)}v, v \in F^*, a(ab-1) = \pi^{\nu(a)}v\underbrace{(ab-1)}_{\in R^*}, ab \in m \Rightarrow \partial\left\langle\begin{pmatrix} a & 1 \\ 1 & b\end{pmatrix}\right\rangle = \partial\langle a\rangle + \partial\langle a(ab-1)\rangle = \epsilon_{\nu(a)}\langle\underline{v}\rangle + \epsilon_{\nu(a)}\left\langle \underline{v}\,\underbrace{\underline{(ab-1)}}_{-1 \mod m}\right\rangle = \epsilon_{\nu(a)}(\langle\underline{v}\rangle + \langle -\underline{v}\rangle) = 0$ $\square$

Corollary 2.53. *The composition $W(\mathbb{Z}) \to W(\mathbb{Q}) \xrightarrow{\partial_p} \oplus_{p\in\mathbb{Z}} W(\mathbb{Z}/p\mathbb{Z})$ (p prime) is zero, where $W(\mathbb{Q}) \xrightarrow{\partial_p} W(\mathbb{Z}/p\mathbb{Z})$ is the 2nd residue homomorphism associated with the p-adic valuation on $\mathbb{Q}$ which has valuation ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} | p \nmid b\}$*

Proof. We have defined

$$\begin{tikzcd} W(\mathbb{Q}) \arrow[r, "\prod \partial_p"] \arrow[dr, dashed, "?"'] & \prod W(\mathbb{Z}/p\mathbb{Z}) \\ & \oplus W(\mathbb{Z}/p\mathbb{Z}) \arrow[u, hook] \end{tikzcd}$$

Need to see that $\prod \partial_p$ has image in $\oplus_p W(\mathbb{Z}/p\mathbb{Z})$. This is the case because if $\langle u\rangle \in W(\mathbb{Q}), u \in \mathbb{Q}^*$ then $u = \frac{a}{b}$ and $\{p \in \mathbb{Z}\text{ prime } | \nu(u) \neq 0\} \subset \{\text{primes in the factorization of } a, b\}$ finite $\Rightarrow \forall \xi \in W(\mathbb{Q}), \partial_p\xi = 0$ for all but finitely many $p \in \mathbb{Z}$ prime. For the composition to be zero, it suffices to check that the composition $W(\mathbb{Z}) \to W(\mathbb{Q}) \xrightarrow{\partial_p} W(\mathbb{Z}/p\mathbb{Z})$ is zero for all p. The composition is zero because it factors as $W(\mathbb{Z}) \to \underbrace{W(\mathbb{Z}_{(p)}) \to W(\mathbb{Q}) \xrightarrow{\partial_p} W(\mathbb{Z}/p\mathbb{Z})}_{0}$ $\square$

Definition 2.54. *A principal ideal domain (PID)* is a commutative ring R which is a domain ($ab = 0 \Rightarrow a$ or $b = 0$) and for which every ideal is a principal ideal ($I \subset R \Rightarrow I = Rx$ for some $x \in I$)

Example. $\mathbb{Z}, k[T]$ (k a field) are PIDs (Euclidean domain$\Rightarrow$PID)

A DVR R is a PID: Let π be a uniformizing element, so $m = \pi R$ and let $I \subset R$ be any ideal. $I = 0$ is principal, so assume $I \neq 0$. Let $n = \min\{\nu(a) | a \in I, a \neq 0\} \in \mathbb{N}_{\geq 0}$. Then $I = \pi^n R$ because $I \subset \pi^n R$ since if $a \in I, a \neq 0, a = \pi^{\nu(a)}u = \pi^n(\underbrace{\pi^{\overbrace{\nu(a)-n}^{\geq 0}}u}_{\in R}) \in \pi^n R$, and $\pi^n R \subset I$ since $\exists a \in I, a \neq 0$, $\nu(a) = n$ so $a = \pi^n u, u \in R^*, a \in I \Rightarrow \pi^n R = \pi^n u R = aR \subset I$. Hence $I = \pi^n R$ is principal.

Remark. A PID is noetherian

Proof. Let R be a PID, $I_1 \subset I_2 \subset \cdots \subset I_2 \subset \cdots \subset R$ be an ascending chain of ideals. Then $I = \cup I_n \subset R$ is an ideal $\Rightarrow I = xR$ for some $x \in I \Rightarrow x \in I_n$ for some $n \Rightarrow I = Rx \subset I_n \subset I \Rightarrow I_n = I_m = I\,\forall m \geq n$ $\square$

Definition 2.55. An R-module M is called *cyclic* if $M \cong R/I$ for some ideal $I \subset R$.

Fact. *Every finitely generated module M over a PID R is a finite direct sum of cyclic R-modules, that is, $M \cong \oplus_{i=1}^n R/a_i$ for some non-units $a_1, \ldots, a_n \in R$*

Corollary 2.56. *Let R be a PID with field of fractions F*

1. *Every submodule M of a finitely generated free R-module is free*
2. *Every finitely generated R-submodule $M \subset F^n$ is also free*

Proof. R is a PID then R is noetherian, $M \subset R^n \Rightarrow M$ is finitely generated so in 1 and 2 the module M is finitely generated $\Rightarrow M = \oplus_{i=1}^n R/a_i$ for some non-unit a_i. But $R/a \subset R^n$ or $R/a \subset F^n \Rightarrow a = 0$ because:

If $a \neq 0$ and $a \notin R^*$ then the composition $R/a \subset R \overset{a}{\hookrightarrow} R$ is injective and $R/a \overset{a=0}{\to} R/a \hookrightarrow R$ zero at the same time (a contradiction). Similarly the composition $R/a \subset F^n \overset{a}{\to} F^n$ is injective (if $a \neq 0, a \notin R^*$) and equals $R/a \overset{a=0}{\to} R/a \hookrightarrow F^n$ zero, again a contradiction $\square$

Corollary 2.57. *Every inner product space over a PID is free*

Lemma 2.58. *Let R be a PID with field of fractions F then the map $W(R) \to W(F)$ defined by $[M, \beta] \mapsto (M_F, \beta_F)$ is injective, where $M_F = M \otimes_R F$ and $\beta_F(x \otimes a, y \otimes b) = ab\beta(x, y)$ for $a, b \in F, x, y \in M$.*

Proof. Assume $[M_F, \beta_F] = 0 \in W(F)$ then $(M_F, \beta_F) \sim 0 \Rightarrow \exists$ metabolic $V = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & A \end{pmatrix} \right\rangle$ with $A \in M_n(F), A^T = A$ such that $(M_F, \beta_F) \perp V$ is metabolic. There exist $d \in R$ such that $dA \in M_n(R)$. Then

$$\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & A \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & d^2A \end{pmatrix} \Rightarrow \left\langle \begin{pmatrix} 0 & 1 \\ 1 & A \end{pmatrix} \right\rangle \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & d^2A \end{pmatrix} \right\rangle \Rightarrow (M, \beta) \perp \underbrace{\left\langle \begin{pmatrix} 0 & 1 \\ 1 & d^2A \end{pmatrix} \right\rangle}_{\text{metabolic over } R}$$

is metabolic over F. Hence can assume (M, β) to be metabolic over F.

Let (M, β) be a symmetric inner product space over R such that $(M, \beta)_F = (M_F, \beta_F)$ is metabolic over F. $M_F = M \otimes_R F$, $\beta_F(x \otimes a, y \otimes b) = ab\beta(x, y)$, $x, y \in M, a, b \in F$. Note $M \subset M_F$ (as $R \subset F, M \cong R^n, M_F \cong F^n$). Now (M_F, β_F) metabolic$\Rightarrow \exists N \subset M_F$ Lagrangian

Claim: $M \cap N \subset M$ is a Lagrangian for (M, β)

$M \cap N$ is a direct summand of M because $M/M \cap N \subset M_F/N \cong F^m$ is a finitely generated R-submodule of $F^m \underset{\text{PID}}{\Rightarrow} M/M \cap N$ is finitely generated free R-module, so $M/M \cap N \cong R^l$. Any section $s : M/M \cap N \to M$ of $g : M \to M/M \cap N \cong R^l$ (that is $gs = 1$) yields a direct sum decomposition $(M \cap N) \oplus \operatorname{im}(s) = M \Rightarrow M \cap N \subset M$ is a direct summand. We now need to check that $(M \cap N)^\perp = M \cap N$. Let $x \in M$, then $x \in (M \cap N)^\perp \iff \beta(x, y) = 0\, \forall y \in M \cap N \iff \beta(x, y) = 0\, \forall y \in N$ (because $\forall t \in M_F = M \otimes_R F\ \exists a \in R, a \neq 0$ such that $at \in M$, in particular $\forall y \in N, \exists a \in R, a \neq 0, ay \in M \cap N$, $\beta(x, y) = 0 \iff \beta(x, ay) \underset{a \neq 0}{=} 0$). But $\beta(x, y) = 0\, \forall y \in N \underset{N = N^\perp}{\iff} x \in N^\perp = N \underset{x \in M}{\iff} x \in M \cap N$. Hence $M \cap N \subset M$ is a Lagrangian $\Rightarrow (M, \beta)$ is metabolic $\Rightarrow [M, \beta] = 0 \in W(R)$

To finish the proof, take $[M, \beta] \in W(R)$ such that $(M, \beta)_F = 0 \in W(F) \Rightarrow \exists V$ metabolic symmetric inner product space over R such that $(M \perp V)_F$ is metabolic over $F \Rightarrow M \perp V$ metabolic over $R \Rightarrow [M] = [M] + [V] = [M \perp V] = 0 \in W(R)$. $\square$

Theorem 2.59. *The sequence of abelian group*

$$0 \to W(\mathbb{Z}) \to W(\mathbb{Q}) \overset{\oplus_p \partial_p}{\longrightarrow} \bigoplus_{p \in \mathbb{Z}_{\geq 2} \text{prime}} W(\mathbb{F}_p) \to 0$$

is exact and the map $W(\mathbb{Z}) \to W(\mathbb{R})$ defined by $M \mapsto M \otimes_{\mathbb{Z}} \mathbb{R}$ is an isomorphism

Proof. We have already proved that $W(\mathbb{Z}) \to W(\mathbb{Q})$ is injective since $\mathbb{Z}$ is a PID and the composition $W(\mathbb{Z}) \to W(\mathbb{Q}) \to \oplus_p W(\mathbb{F}_p)$ is zero.

For $n \in \mathbb{Z}_{\geq 1}$, let $\mathscr{P}_n$ be the set $\mathscr{P}_n = \{a \in \mathbb{Z} \setminus \{0\} | \forall \text{ prime } p : p | a \Rightarrow p \leq n\}$ (e.g. $\mathscr{P}_1 = \{+1, -1\}, \mathscr{P}_2 = \{+2^n, -2^n\}, \mathscr{P}_n \subset \mathscr{P}_{n+1}$). Note that $\mathscr{P}_{n-1} = \mathscr{P}_n$ unless n is prime. Let $L_n \subset W(\mathbb{Q})$ be the subgroup generated by $\langle a \rangle$ with $a \in \mathscr{P}_n$. So $L_{n-1} \subset L_n$ and $L_{n-1} = L_n$ unless n is prime. The composition $L_{p-1} \subset L_p \overset{\partial_p}{\to} W(\mathbb{F}_p)$ is zero because, for $a \in \mathscr{P}_{p-1}, \nu_p(a) = 0$ so $\partial_p(a) = 0$. Hence we get a map of abelian groups $L_p/L_{p-1} \overset{\partial_p}{\to} W(\mathbb{F}_p)$.

Claim: $L_p/L_{p-1} \overset{\partial_p}{\to} W(\mathbb{F}_p)$ is an isomorphism for all primes $p \in \mathbb{Z}_{\geq 2}$.

The claim will follow from:

Lemma 2.60. *If $0 < |n|, |n_1|, \ldots, |n_k| < p$, and $n \equiv n_1 \ldots n_k \mod p$, then $\langle pn \rangle = \langle pn_1 \ldots n_k \rangle \in L_p/L_{p-1}$*

Proof. We use induction on k. The case $k = 1$ follows from $k = 2$ with $n_2 = 1$.

Assume $k \geq 2$: Write $n_1 n_2 = pl + r, 0 \neq |r| < p$. $|pl| = |n_1 n_2 - r| \leq |n_1||n_2| + |r| \leq (p-1)(p-1) + p - 1 = p^2 - p \leq p^2 \Rightarrow |l| < p$. We will show that $\langle pn_1 \dots n_k \rangle = \langle prn_3 \dots n_k \rangle \in L_p/L_{p-1}$. This is clear for $l = 0$ as then both sides are the same. Assume $l \neq 0$ and write $m = n_3 \dots n_k$.

$$\begin{aligned}
\langle pn_1 \dots n_k \rangle - \langle prn_3 \dots n_k \rangle &= \langle pn_1 n_2 m \rangle - \langle prm \rangle \\
&= \langle pn_1 n_2 m \rangle - \langle lm \rangle - \langle prm \rangle \mod L_{p-1} \\
&= \langle pn_1 n_2 m \rangle - \left\langle \underbrace{p^2 lm}_{=:v} \right\rangle - \left\langle \underbrace{prm}_{=:u} \right\rangle \mod L_{p-1} \\
&= \langle pn_1 n_2 m \rangle - \langle u + v \rangle - \langle uv(u+v) \rangle \\
&= \langle pn_1 n_2 m \rangle - \langle pm(pl + r) \rangle - \left\langle p^4 m^3 lr(pl + r) \right\rangle \\
&= \langle pn_1 n_2 m \rangle - \langle pmn_1 n_2 \rangle - \left\langle p^4 m^3 lrn_1 n_2 \right\rangle \\
&= -\langle mlrn_1 n_2 \rangle = 0 \mod L_{p-1}
\end{aligned}$$

Hence $\langle pn_1 n_2 \dots n_k \rangle = \langle prn_3 \dots n_k \rangle$ where $n_1 n_2 = pl+r, |r| < p$. This proves the case $k = 2$ (and hence $k = 1$). Now, the product $rn_3, ..., n_k$ has $k-1$ factors, and we can apply the induction hypothesis. $\square$

We now construct an inverse of the map in the claim. We define the map $\phi : \oplus_{u \in \mathbb{F}_p^*} \mathbb{Z}\{u\} \to L_p/L_{p-1}$ by $\{u\} \mapsto \langle pn \rangle$ where $n \in \mathbb{Z} \setminus \{0\}$, $|n| < p, u \equiv n \mod p$. Note that ϕ is well defined by the lemma, that is our choice of n does not matter. Need to check that ϕ preserves the three relations for $W(\mathbb{F}_p)$

1. $\langle u \rangle = \left\langle a^2 u \right\rangle, a, u \in \mathbb{F}_p^*$. Choose $a_0, u_0, n_o \in \mathbb{Z} \setminus \{0\}$ such that $a_0 = a, u_0 = u, n_0 = a^2 u \in \mathbb{F}_p, |a_0|, |u_0|, |n_0| < p$. Then $\{u\} - \{a^2 u\} \overset{\phi}{\mapsto} \langle pu_0 \rangle - \langle pn_0 \rangle \underset{\text{lemma}}{=} \langle pu_0 \rangle - \left\langle pa_0^2 u_0 \right\rangle = 0 \in L_p/L_{p-1}$
2. $\langle u \rangle + \langle -u \rangle = 0 \in W(\mathbb{F}_p)$. Choose $u_0 \in \mathbb{Z} \setminus \{0\}$, $|u_0| < p, u_0 = u \in \mathbb{F}_p$. Then $\{u\} + \{-u\} \overset{\phi}{\mapsto} \langle pu_0 \rangle + \langle -pu_0 \rangle = 0 \in L_p/L_{p-1}$
3. $\langle u \rangle + \langle v \rangle = \langle u + v \rangle + \langle uv(u+v) \rangle \in W(\mathbb{F}_p), u, v, u+v \in \mathbb{F}_p^*$. Choose $-p < u_0 < 0 < v_0 < p$, (then $|u_0+v_0| < p, |n_0| < p$), $|n_0| < p$ such that $u_0, v_0, n_0 \in \mathbb{Z} \setminus \{0\}$, $u_0 = u, v_0 = v, n_0 = uv(u+v) \in \mathbb{F}_p$. Then $\{u\} + \{v\} - \{u+v\} - \{uv(u+v)\} \overset{\phi}{\mapsto} \langle pu_0 \rangle + \langle pv_0 \rangle - \langle p(u_0 + v_0) \rangle - \langle pn_0 \rangle \underset{\text{lemma}}{=} \langle pu_0 \rangle + \langle pv_0 \rangle - \langle pu_0 + pv_0 \rangle - \langle pu_0 pv_0 (pu_0 + pv_0) \rangle = 0 \in L_p/L_{p-1}$

From this it follows that ϕ induces a well defined map of abelian groups $\bar{\phi} : W(\mathbb{F}_p) \to L_p/L_{p-1}$. The map $\bar{\phi}$ is surjective because L_p/L_{p-1} generated by $\langle pm \rangle$, all prime divisors q of m are $q < p$. By the lemma $\langle pm \rangle \in \mathrm{im}(\bar{\phi})$. It is injective because $\underset{\langle u \rangle \mapsto \langle pn \rangle \mapsto \langle \underline{n} \rangle = \langle u \rangle}{W(\mathbb{F}_p) \to L_p/L_{p-1} \overset{\partial_p}{\to} W(\mathbb{F}_p)}$ is the identity $(*)$. Hence $\bar{\phi}$ is an isomorphism $\underset{(*)}{\Rightarrow}$ $\partial_p : L_p/L_{p-1} \overset{\cong}{\to} W(\mathbb{F}_p)$ is an isomorphism. This finishes the claim.

We prove by induction on $n \geq 1$ that $L_n/L_1 \to \oplus_{p \leq n} W(\mathbb{F}_p)$ is an isomorphism.

The case $n = 1$ is clear as both sides are 0

The case $n = 2$ is true by the claim

$n-1$ to n: If n is not a prime then $\text{LHS}_n = \text{LHS}_{n-1} = \text{RHS}_{n-1} = \text{RHS}_n$

If n is a prime, we have a map of short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & L_{n-1}/L_1 \arrow[r] \arrow[d, "\cong \text{ by induction}"] & L_n/L_1 \arrow[r] \arrow[d] & L_n/L_{n-1} \arrow[r] \arrow[d, "\cong \text{ by claim}"] & 0 \\
0 \arrow[r] & \oplus_{p \leq n-1} W(\mathbb{F}_p) \arrow[r] & \oplus_{p \leq n} W(\mathbb{F}_p) \arrow[r] & W(\mathbb{F}_n) \arrow[r] & 0
\end{tikzcd}$$

By the five lemma we have that $L_n/L_1 \overset{\partial_p}{\to} \oplus_{p \leq n} W(\mathbb{F}_p)$ is also an isomorphism.

Hence $W(\mathbb{Q})/L_1 = \cup_{n \geq 1} L_n/L_1 \overset{\cong}{\to} \cup_{n \geq 1} \oplus_{p \leq n} W(\mathbb{F}_p) = \oplus_{p \geq 1, \text{prime}} W(\mathbb{F}_p)$. So we get the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & L_1 \arrow[r] & W(\mathbb{Q}) \arrow[r] & \oplus_{p \in \mathbb{Z}_{\geq 2} \text{ prime}} W(\mathbb{F}_p) \arrow[r] & 0 \\
& W(\mathbb{Z}) \arrow[ur, hook] \arrow[urr, "0"'] & & &
\end{tikzcd}$$

Since $W(\mathbb{Z}) \subset W(\mathbb{Q})$ and $(\oplus\partial_p)W(\mathbb{Z}) = 0 \Rightarrow W(\mathbb{Z}) \subset L_1$. But $L_1 \subset W(\mathbb{Z})$ because L_1 is generated by $\langle 1\rangle, \langle -1\rangle \Rightarrow W(\mathbb{Z}) = L_1$, and we have exactness of $0 \to W(\mathbb{Z}) \to W(\mathbb{Q}) \to \oplus_p W(\mathbb{F}_p) \to 0$. Finally the map $W(\mathbb{Z}) \to W(\mathbb{R}) \underset{\mathrm{sgn}}{\cong} \mathbb{Z}$ is an isomorphism. This is due to the fact it is surjective since if $U \in W(\mathbb{R})$ then $U = n\langle 1\rangle + m\langle -1\rangle$ but $n\langle 1\rangle + m\langle -1\rangle \in W(\mathbb{Z})$. It is also injective since $W(\mathbb{Z}) = L_1$ is generated by $\langle 1\rangle, \langle -1\rangle$, so every element V of $W(\mathbb{Z})$ has the form $V = n\langle 1\rangle + m\langle -1\rangle$ which is zero in $W(\mathbb{R}) \iff n - m = \mathrm{sgn}(n\langle 1\rangle + m\langle -1\rangle) = 0 \in \mathbb{Z} \iff n = m \iff V = n\langle 1\rangle + n\langle -1\rangle = n(\langle 1\rangle + \langle -1\rangle) = 0 \in W(\mathbb{Z})$. Hence $W(\mathbb{Z}) \to W(\mathbb{R})$ is an isomorphism □

Corollary 2.61. *The map*

$$W(\mathbb{Q}) \to W(\mathbb{R}) \oplus \bigoplus_{p\in\mathbb{Z}_{\geq 2}\text{ prime}} W(\mathbb{F}_p)$$

defined by $M \mapsto (M \otimes_{\mathbb{Q}} \mathbb{R}, \sum_p \partial_p M)$ is an isomorphism.

Proof. This follows from the exact sequence $0 \to W(\mathbb{Z}) \to W(\mathbb{Q}) \to \oplus_p W(\mathbb{F}_p) \to 0$, which is split exact via

$$\begin{tikzcd} W(\mathbb{Z}) \arrow[r, hook] \arrow[dr, "\cong"'] & W(\mathbb{Q}) \arrow[d] \\ & W(\mathbb{R}) \end{tikzcd}$$

□

Corollary 2.62. *Two symmetric inner product spaces M, N over $\mathbb{Q}$ are isometric $\iff$ $\mathrm{sgn}\, M = \mathrm{sgn}\, N, \mathrm{rk}\, M = \mathrm{rk}\, N$, $\partial_p M = \partial_p N \in W(\mathbb{F}_p)\, \forall p \in \mathbb{Z}$ prime. (In terms of quadratic forms, any two regular quadratic forms are equivalent over $\mathbb{Q}$ if and only if the previous condition are fulfilled)*

Proof. $M \cong N \iff \mathrm{rk}\, M = \mathrm{rk}\, N$ and $[M] = [N] \in W(\mathbb{Q}) \iff \mathrm{rk}\, M = \mathrm{rk}\, N$ and $\underbrace{[M] = [N] \in W(\mathbb{R})}_{\mathrm{sgn}\, M = \mathrm{sgn}\, N}$ and $\partial_p M = \partial_p N$ □

Corollary 2.63 (Weak Hasse Principle)**.** *The map*[1]

$$W(\mathbb{Q}) \hookrightarrow W(\mathbb{R}) \oplus \prod_{\mathbb{Z}\ni p\text{ prime}} W(\mathbb{Q}_p)$$

is injective. In particular two inner product spaces M, N over $\mathbb{Q}$ are isometric over $\mathbb{Q}$ if and only if M and N are isometric over $\mathbb{R}$ and $\mathbb{Q}_p$ for all $p \in \mathbb{Z}$ prime.

Proof. We have the following commutative diagram by definition of ∂_p

$$\begin{tikzcd} W(\mathbb{Q}) \arrow[r, "\cong", "(a)"'] \arrow[d, "(b)"'] & W(\mathbb{R}) \oplus \bigoplus_{p\text{ prime}} W(\mathbb{F}_p) \arrow[d, "(c)"] \\ W(\mathbb{R}) \oplus \prod_{p\text{ prime}} W(\mathbb{Q}_p) \arrow[r, "\mathrm{id}_{W(\mathbb{R})} \oplus \prod \partial_p"'] & W(\mathbb{R}) \oplus \prod_{p\text{ prime}} W(\mathbb{F}_p) \end{tikzcd}$$

Now (a) isomorphism and (c) injective implies (b) injective.

$M \cong_{\mathbb{Q}} N \Rightarrow M \cong_{\mathbb{R}} N$ and $M \cong_{\mathbb{Q}_p} N$ for all $p \in \mathbb{Z}$ prime.

Assume $M \cong_{\mathbb{R}} N$ and $M \cong_{\mathbb{Q}_p} N$ for all $p \in \mathbb{Z}$ prime. Then $\mathrm{rk}\, M = \mathrm{rk}\, N$ and $[M] = [N] \in W(\mathbb{R})$ and $[M] = [N] \in W(\mathbb{Q}_p)$ for all p. But (b) injective $\Rightarrow \mathrm{rk}\, M = \mathrm{rk}\, N, [M] = [N] \in W(\mathbb{Q}) \underset{\mathrm{char}\,\mathbb{Q}\neq 2}{\iff} M \cong N$ □

[1] In the lectures I carelessly wrote $\bigoplus_p$ instead of $\prod_p$ but the image of $W(\mathbb{Q})$ does not lie in $\bigoplus_p$, otherwise, what is the image of $\langle 1\rangle$ which is $\neq 0 \in W(F)$ for any field F?

Example. We start with two side remarks: The quadratic form $q = \sum_{i=1}^n a_i x_i^2 + \sum_{i<j} a_{ij} x_i x_j$ has associated form matrix $B = (\beta_{ij})$ (with respect to $e_1, e_2, e_3, \ldots, e_n$) where $\beta_{ij} = q(e_i + e_j) - q(e_i) - q(e_j) = \begin{cases} a_{ij} & i<j \\ a_{ij} & j<i \\ 2a_i & i=j \end{cases}$

That is, $B = \begin{pmatrix} 2a_1 & a_{12} & \ldots & a_{1n} \\ a_{12} & 2a_2 & & \\ \vdots & & \ddots & \\ a_{1n} & & & 2a_n \end{pmatrix}$.

The diagonalisation of a symmetric matrix $B = \begin{pmatrix} a_1 & a_{12} & \ldots & a_{1n} \\ a_{12} & a_2 & & \\ \vdots & & \ddots & \\ a_{1n} & & & a_n \end{pmatrix}$ is $\langle B \rangle = \left\langle d_1, \frac{d_2}{d_1}, \ldots, \frac{d_n}{d_{n-1}} \right\rangle$ where $d_i =$ determinant of the upper left corner of size $i \times i$ of B, provided $d_1, \ldots, d_{n-1} \neq 0$.

1. Does $15 = x^2 + 2xy + 3y^2 - 4yz$ have a solution $x, y, z \in \mathbb{Q}$?

   Solution: Let $q = x^2 + 2xy + 3y^2 - 4yz$. Does q represent 15? The associated symmetric bilinear form $\beta(u,v) = q(u+v) - q(u) - q(v)$, $u, v \in \mathbb{Q}^3$ has form matrix

   $$B = \begin{pmatrix} 2 & 2 & 0 \\ 2 & 6 & -4 \\ 0 & -4 & 0 \end{pmatrix}$$

   which has determinant -32 hence it is non-degenerate. It has diagonalisation $\langle B \rangle \cong \left\langle 2, \frac{8}{2}, \frac{-32}{8} \right\rangle \cong \left\langle 2, \underbrace{1, -1}_{\mathbb{H}} \right\rangle \underset{\text{exercise}}{\Rightarrow} q$ isotropic and represent any rational number. In particular there exists x, y, z such that $q(x,y,z) = 15$

   Note that $\langle B \rangle \cong \langle 2, 4, -4 \rangle \Rightarrow q \cong x^2 + 2y^2 - 2z^2 \cong x^2 + yz$

2. Does $15 = x^2 + 4xy - 2xz + 7y^2 - 4yz + z^2 =: q$ has a solution $x, y, z \in \mathbb{Q}$.

   Solution: The associated bilinear form β of q has matrix form

   $$B = \begin{pmatrix} 2 & 4 & -2 \\ 4 & 14 & -4 \\ -2 & -4 & 2 \end{pmatrix}$$

   with determinant $= 0$ (since $Be_3 = -Be_1$). So q is degenerate, and we can eliminate a variable as follows: The inner product space $\langle B \rangle$ has diagonalisation $\langle B \rangle \cong \underbrace{(\mathbb{Q}e_1 + \mathbb{Q}e_2)}_{\text{non-degenrate as } \det\left(\begin{smallmatrix} 2 & 4 \\ 4 & 14 \end{smallmatrix}\right) = 12 \neq 0} + \underbrace{(\mathbb{Q}e_1 + \mathbb{Q}e_2)^\perp}_{\text{dim}=1,\text{degenerate as } \det B = 0} \cong \left\langle \begin{pmatrix} 2 & 4 \\ 4 & 14 \end{pmatrix} \right\rangle \perp \langle 0 \rangle \cong \left\langle 2, \frac{12}{2} \right\rangle \perp \langle 0 \rangle \cong \langle 2, 6 \rangle \perp \langle 0 \rangle$. This means that $q \cong x^2 + 3y^2$, so does this represent 15? This is equivalent to asking $\langle 2, 6 \rangle \cong \langle 30, a \rangle$ for some $a \in \mathbb{Q}^*$. Then det LHS = det RHS modulo square units $\iff \langle 1, 3 \rangle \cong \langle 15, 5 \rangle \iff \langle 1, 3 \rangle = \langle 15, 5 \rangle \in W(\mathbb{Q})$ (because $\langle 1, 3 \rangle$ and $\langle 15, 5 \rangle$ have the same rank) $\iff \langle 1, 3 \rangle \cong \langle 15, 5 \rangle \in W(\mathbb{R})$ and $\partial_p \langle 1, 3 \rangle \cong \partial_p \langle 15, 5 \rangle \in W(\mathbb{F}_p)$ for all p prime.

   - If $p \neq 3$ or 5 then $\partial_p \langle 1, 3 \rangle = 0 = \partial_p \langle 15, 5 \rangle$
   - if $p = 3$ then $\partial_3 \langle 1, 3 \rangle = \partial_3 \langle 1 \rangle + \partial_3 \langle 3 \rangle = 0 + \langle 1 \rangle$, and $\partial_3 \langle 15, 5 \rangle = \partial_3 \langle 15 \rangle + \partial_3 \langle 5 \rangle = \langle 5 \rangle + 0 = \langle -1 \rangle$. Do they agree in $W(\mathbb{F}_3)$? No because $\langle 1 \rangle \neq \langle -1 \rangle \in W(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$ generated by $\langle 1 \rangle \Rightarrow \langle 1 \rangle - \langle -1 \rangle = 2 \langle 1 \rangle \neq 0 \in W(\mathbb{F}_3)$

   We have showed that $\langle 1, 3 \rangle \neq \langle 15, 5 \rangle \in W(\mathbb{Q}) \Rightarrow q$ does not represent 15 and the equation has no solution in $x, y, z \in \mathbb{Q}$

2.6 The Brauer Group and the Hasse Invariant

Recall from MA377 (Rings and Modules):

Definition 2.64. Let k be a field, a k-algebra A is called:

- *central:* if $k \xrightarrow{\cong} Z(A)$, where $Z(A)$ denotes the center of A
- *simple:* if $A \neq 0$ and the only ideals of A are 0 and A
- *finite dimensional*: if $\dim_k A < \infty$

Fact. *Let A, B be finite dimensional central simple k-algebras. Then:*

1. *$A = M_n(D)$ where D is a finite dimensional division k-algebra*
2. *$A \otimes_k B$ is also a finite dimensional central simple k-algebra*
3. *$A \otimes_k A^{op} \cong M_n(k)$ where $n = \dim_k A$*

Definition 2.65. Let F be a field. The *Brauer group, $Br(F)$,* is the set of Brauer equivalence classes $[A]$ of finite dimensional central simple F-algebras A, where $A \sim B$ (A is *Brauer equivalent* to B) if $M_m(A) \cong M_n(B)$ as F-algebras for some $m, n \in \mathbb{N}_{\geq 1}$.

$\mathrm{Br}(F)$ is a group with group law: $[A][B] := [A \otimes_F B]$, with $1 = [F]$ and $[A]^{-1} = [A^{op}]$. Indeed $\mathrm{Br}(F)$ is an abelian group: $[A][B] = [A \otimes_F B] = [B \otimes_F A] = [B][A]$, $1[A] = [F][A] = [F \otimes_F A] = [A]$, $[A][A^{op}] = [A \otimes_F A^{op}] \underset{\text{Fact}}{=} [M_n(F)] = [F] = 1$

Example. (From MA377)

- $\mathrm{Br}(\mathbb{C}) = \mathrm{Br}(F) = \{F\} = 0$ where $F = \bar{F}$ is algebraically closed
- $\mathrm{Br}(F) = 0$ if F is a finite field
- $\mathrm{Br}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\} = \mathbb{Z}/2$

Definition 2.66. Let F be a field with char $F \neq 2$ and $a, b \in F^*$. Let $(\frac{a,b}{F})$ be the 4-dimensional F-algebra with basis, $1, i, j, k$ such that $i^2 = a, j^2 = b, k = ij = -ji$

Note. $k^2 = ij(-ji) = -ab$

Fact. *For $a, b \in F^*$, $(\frac{a,b}{F})$ is a 4-dimensional central simple F-algebra.*

Definition 2.67. An F-algebra which is F-algebra isomorphic to $(\frac{a,b}{F})$ for some $a, b \in F^*$ is called (generalized) *quaternion algebra* (over F)

Structure theorem for Quaternion algebras. *Let F be a field with char $F \neq 2$. Then* $(\frac{a,b}{F}) \cong (\frac{c,d}{F}) \iff \langle a, b, -ab\rangle = \langle c, d, -cd\rangle \in W(F)$

Remark. Let A, B be finite dimensional central simple F-algebras. Then $A \cong B \iff \dim_F A = \dim_F B$ and $[A] = [B] \in \mathrm{Br}(F)$.

In particular $[(\frac{a,b}{F})] = [(\frac{c,d}{F})] \in \mathrm{Br}(F) \iff \langle a, b, -ab\rangle = \langle c, d, -cd\rangle \in W(F)$

Example. $(\frac{1,1}{F}) \cong M_2(F)$ by $i \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, j \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$(\frac{-1,-1}{\mathbb{R}})$ = Real quaternion algebra.

$M_2(\mathbb{R}) = (\frac{1,1}{\mathbb{R}}) \not\cong (\frac{-1,-1}{\mathbb{R}})$ because $\underbrace{\langle 1, 1, -1\rangle}_{\text{sgn}=1} \neq \underbrace{\langle -1, -1, -1\rangle}_{\text{sgn}=-3} \in W(\mathbb{R})$

Remark. $(\frac{a,b}{F})$ is a division algebra $\iff (\frac{a,b}{F}) \not\cong M_2(F) \iff \langle a, b, -ab\rangle \not\cong \langle 1, 1, -1\rangle \iff \langle a, b, -ab\rangle$ is an isotropic (i.e., does not represent 0)

Remark. $(\frac{a,b}{F}) \cong (\frac{a,b}{F})^{op}$ by $1 \mapsto 1, i \mapsto -i, j \mapsto -j, k \mapsto -k$. This means that $[(\frac{a,b}{2})]$ has order 2 in $\mathrm{Br}(F)$ because $(\frac{a,b}{F}) \otimes_F (\frac{a,b}{F}) \cong (\frac{a,b}{F}) \otimes_F (\frac{a,b}{F})^{op} \cong M_4(F) \Rightarrow [(\frac{a,b}{F})][(\frac{a,b}{F})] = [M_4(F)] = [F] = 1 \in \mathrm{Br}(F)$. Hence $[(\frac{a,b}{F})] \in {}_2\mathrm{Br}(F)$, where for an abelian group G we denote ${}_2G = \{x \in G | x^2 = 1\}$

Lemma 2.68. *Let F be a field with char $F \neq 2$. Then:*

1. $(\frac{a,b}{F}) \cong (\frac{a,-ab}{F}) \cong (\frac{b,-ab}{F})$

2. $(\frac{a,b}{F}) \otimes_F (\frac{a,c}{F}) \cong (\frac{a,bc}{F}) \otimes_F M_2(F)$

Proof. 1. $(\frac{a,b}{F}) \cong (\frac{a,-ab}{F})$ because $\langle a,b,-ab\rangle \cong \langle a,-ab,a^2b\rangle$

2. Let $A = (\frac{a,b}{F}), B = (\frac{a,c}{F})$ have basis $\mathscr{B}_A = \{1, i_A, j_A, k_A\}$ and $\mathscr{B}_B = \{1, i_B, j_B, k_B\}$ respectively. Then $A \otimes_F B$ has basis $\{u \otimes v | u \in \mathscr{B}_A, v \in \mathscr{B}_B\}$. Let $\Sigma_A = \{1\otimes 1, i_A \otimes 1, j_A \otimes j_B, k_A \otimes j_B\} \subset A \otimes_F B$ and $\Sigma_B = \{1\otimes 1, 1 \otimes j_B, i_A \otimes k_B, -ci_A \otimes i_B\}$. Then $\Sigma_A, \Sigma_B$are the basis of $A', B' \subset A \otimes_F B$-subalgebras with $A' \cong (\frac{a,bc}{F})$ and $B' \cong (\frac{c,-a^2c}{F})$ because

   - $(i_A \otimes 1)^2 = i_A^2 \otimes 1 = a(1 \otimes 1) = a$
   - $(j_A \otimes j_B)^2 = j_A^2 \otimes j_B^2 = b \otimes c = bc(1 \otimes 1) = bc$
   - $(1_A \otimes 1)(j_A \otimes j_B) = k_A \otimes j_B = -(j_A \otimes j_B)(i_A \otimes 1)$

   and

   - $(1 \otimes j_B)^2 = 1 \otimes j_B^2 = c$
   - $(i_A \otimes k_B)^2 = i_A^2 \otimes k_B^2 = a \cdot (-ac) = -a^2c$
   - $(1 \otimes j_B)(i_A \otimes k_B) = -(i_A \otimes k_B)(1 \otimes j_B) = i_A \otimes -ci_B = -ci_A \otimes i_B$

   But $(\frac{c,-a^2c}{F}) \cong (\frac{1,1}{F}) = M_2(F)$ because $\langle c, -a^2c, a^2c^2\rangle \cong \langle c,-c,1\rangle \cong \langle 1,1,-1\rangle$. Every element of A' commutes with every element of B' (one checks that Σ_A commutes with Σ_B)$\Rightarrow$ The map $\phi : A' \otimes_F B' \to A \otimes_F B$ defined by $x \otimes y \mapsto xy$ is a well defined map of F-algebras. The elements $\{xy | x \in \Sigma_A, y \in \Sigma_B\}$ are linearly independent in $A \otimes_F B$ (check!) $\Rightarrow \phi$ is injective. Since $\dim_F A' \otimes_F B' = 8 = \dim_F A \otimes_F B$, this means that ϕ is an isomorphism $\Rightarrow (\frac{a,bc}{F}) \otimes_F M_2(F) \cong A' \otimes_F B' \cong A \otimes_F B \cong (\frac{a,b}{F}) \otimes_F (\frac{a,c}{F})$

□

Definition 2.69. Let F be a field with char $F \neq 2$, and V be a symmetric inner product space over F with diagonalisation $V \cong \langle a_1, \dots, a_n\rangle$. The *Hasse invariant* of V is the algebra

$$\mathrm{Hasse}(V) = \prod_{1 \leq i < j \leq n} \left(\frac{a_i, a_j}{F}\right) \in {}_2\,\mathrm{Br}(F)$$

Lemma 2.70. $\mathrm{Hasse}(V) \in_2 \mathrm{Br}(F)$ *does not depend on diagonalisation* $\langle a_1, \dots, a_n\rangle$ *of* V *used to define* $\mathrm{Hasse}(V)$

Proof. 1. $\mathrm{Hasse}(\langle a_1, \dots a_i, a_{i+1}, \dots, a_n\rangle) = \mathrm{Hasse}(\langle a_1, \dots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \dots, a_n\rangle)$. This is because

$$\begin{aligned} \mathrm{LHS} &= \left(\prod_{r<s, \{r,s\} \neq \{i,i+1\}} \left(\frac{a_r, a_s}{F}\right)\right)\left(\frac{a_i, a_{i+1}}{F}\right) \\ \mathrm{RHS} &= \left(\prod_{r<s, \{r,s\} \neq \{i,i+1\}} \left(\frac{a_r, a_s}{F}\right)\right)\left(\frac{a_{i+1}, a_i}{F}\right) \end{aligned}$$

   Since $(\frac{a,b}{F}) \cong \left(\frac{b,a}{F}\right) \Rightarrow \mathrm{LHS} = \mathrm{RHS}$. Hence for all $\sigma \in \Sigma_n =$ permutation group, we have $\mathrm{Hasse}(\langle a_1, \dots, a_n\rangle) = \mathrm{Hasse}(\langle a_{\sigma(1)}, \dots, a_{\sigma(n)}\rangle)$

2. char $\neq 2$, if $\langle a_1, \dots, a_n\rangle$ and $\langle b_1, \dots, b_n\rangle$ are diagonalisation of V then $\langle a_1, \dots, a_n\rangle \approx \langle b_1, \dots, b_n\rangle$ (Chain equivalence Theorem on page 13). Hence it suffices to show that $\mathrm{Hasse}(\langle a_1, \dots, a_n\rangle) = \mathrm{Hasse}(\langle b_1, \dots, b_n\rangle)$ for $\langle a_1, \dots, a_n\rangle \approx_s \langle b_1, \dots, b_n\rangle$ simply chain equivalent. By 1. it suffices

to show $\mathrm{Hasse}(\langle a,b,e_1,\dots,e_n\rangle) = \mathrm{Hasse}(\langle c,d,e_1,\dots,e_n\rangle)$ where $\langle a,b\rangle \cong \langle c,d\rangle$. Recall that $\langle a,b\rangle \cong \langle c,d\rangle \iff ab = cd\cdot x^2, a = cy^2+dz^2$ for some $x,y,z\in F$. Now

$$\begin{aligned} \mathrm{LHS} &= \left(\frac{a,b}{F}\right)\prod_{i=1}^{n}\left(\frac{a,e_i}{F}\right)\left(\frac{b,e_i}{F}\right)\mathrm{Hasse}(\langle e_1,\dots,e_n\rangle) \\ \mathrm{RHS} &= \left(\frac{c,d}{F}\right)\prod_{i=1}^{n}\left(\frac{c,e_i}{F}\right)\left(\frac{d,e_i}{F}\right)\mathrm{Hasse}(\langle e_1,\dots,e_n\rangle) \end{aligned}$$

Note that

$$\begin{aligned} \left(\frac{a,e}{F}\right)\left(\frac{b,e}{F}\right) &= \left(\frac{ab,e}{F}\right) \in \mathrm{Br}(F) \\ &= \left(\frac{cd,e}{F}\right) \text{ since } ab = cdx^2 \\ &= \left(\frac{c,e}{F}\right)\left(\frac{d,e}{F}\right) \end{aligned}$$

and $(\frac{a,b}{F}) \cong (\frac{c,d}{F})$ because $\langle a,b,-ab\rangle = \langle a,b\rangle + \langle -ab\rangle = \langle c,d\rangle + \langle -cd\rangle = \langle c,d,-cd\rangle$

□

Lemma 2.71. $\mathrm{Hasse}(V\perp W) = \mathrm{Hasse}(V)\,\mathrm{Hasse}(W)\cdot(\frac{\det V,\det W}{F})$

Proof. Exercise □

So $\mathrm{Hasse}(-)$ does not define a group homomorphism $W(F)\to {}_2\mathrm{Br}(F)$. $\mathrm{Hasse}(\mathbb{H}) = \mathrm{Hasse}(\langle 1,-1\rangle) = (\frac{1,-1}{F}) \cong (\frac{1,1}{F}) = M_2(F)$ because $\langle 1,-1,1\rangle \cong \langle 1,1,-1\rangle$. But $\mathrm{Hasse}(\mathbb{H}^2) = \mathrm{Hasse}(\mathbb{H})\,\mathrm{Hasse}(\mathbb{H})\cdot(\frac{\det\mathbb{H},\det\mathbb{H}}{F}) = (\frac{-1,-1}{F}) \neq (\frac{1,1}{F}) = M_2(F) = F\in\mathrm{Br}$ in general.

2.7 Tensor Product of Inner Product Spaces

Definition 2.72. Let $(M,\beta),(B,\gamma)$ be symmetric bilinear forms over R. We define $(M\otimes_R N, \beta\otimes_R\gamma)$ to be the bilinear form $\beta\otimes\gamma : M\otimes_R N\times M\otimes_R N\to R$ defined by $(x\otimes u, y\otimes v)\mapsto \beta(x,y)\cdot\gamma(u,v)$, which is symmetric: $\beta\otimes\gamma(x\otimes u,y\otimes v) = \beta(x,y)\gamma(u,v) = \beta(y,x)\gamma(v,u) = \beta\otimes\gamma(y\otimes v,x\otimes u)$

Lemma 2.73. *Let P,Q be finitely generated R-module then the following map $\phi : \mathrm{Hom}_R(P,R)\otimes_R \mathrm{Hom}_R(Q,R)\to\mathrm{Hom}_R(P\otimes_R Q,R)$ defined by $f\otimes g\mapsto f\cdot g$ where $(f\cdot g)(x\otimes u) = f(x)g(u)$, is an isomorphism*

Proof. ϕ is an isomorphism for $(P,Q) = (R,R)$.

If ϕ is an isomorphism for (P_1,Q) and (P_2,Q) then ϕ is an isomorphism for $(P_1\oplus P_2,Q)$ because $(P_1\oplus P_2)\otimes Q = P_1\otimes Q\oplus P_2\otimes Q$, $\mathrm{Hom}(P_1\oplus P_2,R) = \mathrm{Hom}(P_1,R)\oplus\mathrm{Hom}(P_2,R)$ and $\phi_1\oplus\phi_2$ is an isomorphism if and only if ϕ_1 and ϕ_2 are isomorphisms. $\Rightarrow \phi$ is isomorphism for $(P,Q) = (R^m,R^n)$ $m,n\in\mathbb{Z}_{\geq 0}$.

A finitely generated projective module is a direct factor of R^n for some n. If ϕ_1 is a direct summand of a map ϕ which is an isomorphism then ϕ_1 is an isomorphism $\Rightarrow \phi$ is an isomorphism for P,Q finitely generated projective modules. □

Lemma 2.74. *Let $(M,\beta),(N,\gamma)$ be symmetric inner product spaces over R. Then $(M\otimes_R N,\beta\otimes\gamma)$ is an inner product space over R*

Proof. M,N is finitely generated projective $\Rightarrow M\otimes_R N$ is finitely generated projective. We need to show $\beta\otimes\gamma$ is non-degenerate. Now β,γ non-degenerated $\iff$ $M\to\mathrm{Hom}_R(M,R)$ defined by $x\mapsto\beta(x,-)$ and $N\to\mathrm{Hom}_R(N,R)$ defined by $y\mapsto\gamma(y,-)$ are isomorphisms. $\beta\otimes\gamma$ is non-degenerate $\iff$ $M\otimes_R N\to\mathrm{Hom}_R(M\otimes_R N,R)$ defined by $x\otimes y\mapsto\beta(x,-)\gamma(y,-)$ is an isomorphism, but this map is the composition of the following two maps

$$M\otimes_R N\xrightarrow{\cong}\mathrm{Hom}_R(M,R)\otimes\mathrm{Hom}_R(N,R)\xrightarrow[\text{Lemma}]{\cong}\mathrm{Hom}_R(M\otimes_R N,R)$$

$$x\otimes y\mapsto\beta(x,-)\otimes\gamma(y,-)\mapsto\beta(x,-)\cdot\gamma(y,-)$$

□

Lemma 2.75 (Definition). *The Wilt group $W(R)$ of a a commutative ring R is a commutative ring with multiplication $[M,\beta]\cdot[N,\gamma]=[(M,\beta)\otimes_R(N,\gamma)]$ and unit $\langle 1\rangle$. $W(R)$ is called the* Witt ring of *R.*

Proof. We need to show that if (M,β) is metabolic and (N,γ) arbitrary then $(M,\beta)\otimes(N,\gamma)$ is metabolic. But a Lagrangian $L\subset M$ of (M,β) defines a Lagrangian $L\otimes N\subset M\otimes N$ of $(M\otimes N,\beta\otimes\gamma)$ (exercise) $\square$

Remark. $\langle u\rangle\cdot\langle v\rangle=\langle uv\rangle\in W(R)$

Definition 2.76. Let R be a local ring then the rank map $W(R)\to\mathbb{Z}/2$ defined by $M\mapsto \operatorname{rk} M$ is a ring homomorphism. The kernel ker(rk) is an ideal $I(R)$ which is called *the fundamental ideal.*

Remark. $I(F)$ is generated by even dimensional forms, hence additively generated by 2 dimensional forms $\langle a,b\rangle=\langle a,1\rangle-\langle -b,1\rangle\Rightarrow I(F)$ is additively generated by $\langle a,1\rangle, a\in F^*\Rightarrow I^2(F)$ is additively generated by $\langle a,1\rangle\otimes\langle b,1\rangle=\langle ab,a,b,1\rangle$, the discriminant map, disc : $I(F)\to F^*/F^{2*}$ defined by $V\mapsto(-1)^{\frac{\dim V}{2}}\det V$, in our case we have $\langle ab,a,b,1\rangle\mapsto a^2b^2=1\in F^*/F^{2*}$ hence $\operatorname{disc}(I^2)=0$ and $I(F)/I^2(F)\to F^*/F^{2*}$ well defined surjective map of abelian groups

Theorem 2.77 (Pfister)**.** *The map $I(F)/I^2(F)\to F^*/F^{2*}$ is an isomorphism for all fields F.*

Proof. The map is surjective because $I(F)\overset{\text{disc}}{\to}F^*/F^{2*}$ sends $\langle a,-1\rangle$ to a for $a\in F^*$.

In $W(F)/I^2$ we have:

1. $\langle a\rangle+\langle b\rangle=\langle -ab\rangle+\langle -1\rangle$ because $\langle ab,a,b,1\rangle\in I^2$
2. $3\langle -1\rangle=\langle 1\rangle$ because $\langle 1,1,1,1\rangle=\langle 1,1\rangle\otimes\langle 1,1\rangle\in I^2$, hence $4\langle -1\rangle=0$.

If $\xi=\langle u_1,\dots,u_n\rangle\in I/I^2$ then $n=2m$. For $u=\text{dics}\xi$ we have

$$\begin{aligned}\xi=\langle u_1,\dots,u_{2m}\rangle &\underset{1.}{=} \langle -(-1)^m u,\underbrace{-1,\dots,-1}_{2m-1}\rangle \text{ in } I/I^2\\ &\underset{2.}{=}\begin{cases}\langle u,-1,-1,-1\rangle & m \text{ even}\\ \langle u,-1\rangle & m\text{ odd}\end{cases}\\ &= \langle -u,1\rangle\end{aligned}$$

where the last equation follows from 2 when m is even, and when m is odd we have $\langle u,-1\rangle=\langle -u,1\rangle$ because $\langle u,u,-1,-1\rangle=\langle -u^2,-1,-1,-1\rangle=\langle -1,-1,-1,-1\rangle=0\in I/I^2$, by 1 and 2. Thus, if ξ is in the kernel of the discriminant map then $1=\operatorname{disc}(\xi)=\operatorname{disc}(-u,1)=u\Rightarrow u=1\in F^*/F^{2*}\Rightarrow\xi=\langle -u,1\rangle=\langle -1,1\rangle=0\in I/I^2\Rightarrow\xi=0\in I/I^2$ and the map $I/I^2\to F^*/F^{2*}$ is injective. $\square$

Example.

- $I^2(\mathbb{F}_q)=0$ because disc : $I(\mathbb{F}_q)\overset{\cong}{\to}\mathbb{F}_q^*/\mathbb{F}_q^{2*}$ is an isomorphism.
- $I^2(F)=I(F)=0$ for any algebraically closed field F because rk : $W(F)\overset{\cong}{\to}\mathbb{Z}/2\mathbb{Z}$
- $$\begin{tikzcd} I(\mathbb{R}) \arrow[r, hook] \arrow[d, equal] & W(\mathbb{R}) \arrow[r, "\text{rk}"] \arrow[d, equal, "\text{sgn}"'] & \mathbb{Z}/2\mathbb{Z} \\ 2\mathbb{Z}\subset & \mathbb{Z} \arrow[ur, "\text{reduction mod 2}"'] & \end{tikzcd}$$
- We'll see later: $I^2(\mathbb{Q}_p)=\mathbb{Z}/2\mathbb{Z}$

Definition 2.78. Let V be a $4k$-dimensional symmetric inner product space over F with disc$V$ $(=\det V)=1$. *The Signed Hasse Invariant* is $s(V)=(\frac{-1,-1}{F})^k\,\text{Hasse}(V)=(\frac{(-1)^k-1}{F})\,\text{Hasse}(V)$

Note. If V, W have dimension divisible by 4 and disc$V$ = disc$W = 1$ then

$$\begin{aligned}
s(V\perp W) &= (\frac{-1,-1}{F})^{\frac{\dim V+\dim W}{4}} \operatorname{Hasse}(V\perp W)\\
&= \left(\frac{-1,-1}{F}\right)^{\frac{\dim V}{4}}\left(\frac{-1,-1}{F}\right)^{\frac{\dim W}{4}} \operatorname{Hasse}(V)\operatorname{Hasse}(W)\underbrace{\left(\frac{\det V,\det W}{F}\right)}_{(\frac{1,1}{F})}\\
&= s(V)s(W)
\end{aligned}$$

and $s(\mathbb{H}^2) = (\frac{-1,-1}{2})\operatorname{Hasse}(\mathbb{H}^2) = (\frac{-1,-1}{F})(\frac{-1,-1}{F}) = [F] \in \operatorname{Br}(F) \Rightarrow s(\mathbb{H}^{2k}) = [F] \in \operatorname{Br}(F)$. Hence $s : I^2(F) \to {}_2\operatorname{Br}(F)$ is a well defined map of abelian groups. (as I^2 is generated by 4-dimesional spaces)

Lemma 2.79. *$s(I^3F) = 0$ for every field F of char $\neq 2$*

Proof. I is generated by $\langle 1,a\rangle \Rightarrow I^3$ is generated by $\langle 1,a\rangle\otimes\langle 1,b\rangle\otimes\langle 1,c\rangle = \langle 1,a,b,c,ab,ac,bc,abc\rangle = \langle a_1,\dots,a_8\rangle$. So,

$$\begin{aligned}
s(\langle a_1,\dots,a_8\rangle &= (-1)^{\frac{8}{4}}\operatorname{Hasse}(\langle a_1,\dots,a_8\rangle)\\
&= \prod_{i\le i<j\le 8}\left(\frac{a_i,a_j}{F}\right)\\
&= \prod_{1\le i\le 7}\left(\frac{a_i\prod_{i<j\le 8}a_j}{F}\right) \quad \text{by Lemma 2.68}\\
&= \left(\frac{1,a^4b^4c^4}{F}\right)\left(\frac{a,a^3b^4c^4}{F}\right)\left(\frac{b,a^3b^3c^4}{F}\right)\left(\frac{c,a^3b^3c^3}{F}\right)\left(\frac{ab,a^2b^2c^3}{F}\right)\left(\frac{ac,ab^2c^2}{F}\right)\left(\frac{bc,abc}{F}\right)\\
&= \left(\frac{1,1}{F}\right)\left(\frac{a,a}{F}\right)\left(\frac{b,ab}{F}\right)\left(\frac{c,abc}{F}\right)\left(\frac{ab,c}{F}\right)\left(\frac{ac,a}{F}\right)\left(\frac{bc,abc}{F}\right) \quad \text{removing powers of 2}\\
&= \left(\frac{a,a}{F}\right)\left(\frac{b,-a}{F}\right)\left(\frac{c,-ab}{F}\right)\left(\frac{ab,c}{F}\right)\left(\frac{a,-c}{F}\right)\left(\frac{bc,-a}{F}\right) \quad \text{by using the relation } \left(\frac{a,b}{F}\right) = \left(\frac{a,-ab}{F}\right)\\
&= \left(\frac{a,a}{F}\right)\left(\frac{a,-c}{F}\right)\left(\frac{b,-a}{F}\right)\left(\frac{bc,-a}{F}\right)\left(\frac{c,-ab}{F}\right)\left(\frac{c,ab}{F}\right) \quad \text{by rearranging}\\
&= \left(\frac{a,-ac}{F}\right)\left(\frac{c,-a}{F}\right)\left(\frac{c,-1}{F}\right) \text{pairing off and Lemma 2.68}\\
&= \left(\frac{a,-ac}{F}\right)\left(\frac{c,a}{F}\right) \quad \text{Lemma 2.68 on the last two pairs}\\
&= \left(\frac{a,-ac^2}{F}\right) \quad \text{Lemma 2.68}\\
&= \left(\frac{a,-a}{F}\right) \quad \text{removing powers of 2}\\
&= \left(\frac{1,1}{F}\right) \quad \text{because } \langle a,-a,a^2\rangle = \langle 1,1,-1\rangle\\
&= 0
\end{aligned}$$

□

Corollary 2.80. *The signed Hasse invariant gives a well defined map of abelian groups $I^2(F)/I^3(F) \to {}_2\operatorname{Br}(F)$*

Theorem 2.81 (Merkurev, 1981)**.** *The map $I^2F/I^3F \xrightarrow{\cong} {}_2\operatorname{Br}(F)$ is an isomorphism (char$(F)\neq 2$)*

Remark. $I^0/I^2 = W(F)/I = \mathbb{Z}/2\mathbb{Z}$, $I/I^2 = F^*/F^{2*}, I^2/I^3 = {}_2\operatorname{Br}(F)$, what about $I^k/I^{k+1} =$?

For any field F there are defined cohomology groups $H^n(F,\mathbb{Z}/2\mathbb{Z})$, sometimes called "Galois cohomology groups", which satisfy $H^0(F,\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, $H^1(F,\mathbb{Z}/2\mathbb{Z}) = F^*/F^{2*}$ and $H^2(F,\mathbb{Z}/2\mathbb{Z}) =$

${}_2\operatorname{Br}(F)$ for any field F of characteristic $\neq 2$. This makes the statement of the following theorem plausible. For its proof and the development of the tools needed in the proof (motivic cohomology and motivic homotopy theory), Voevodsky was awarded the fields medal in 2002.

Theorem 2.82 (Voevodsky, conjectured by Milnor)**.** *Let F be a field of char $\neq 2$ then*

$$I^n(F)/I^{n+1}(F) \cong H^n(F, \mathbb{Z}/2\mathbb{Z})$$

Lemma 2.83. *Let F be a field with char$F \neq 2$ and V, W symmetric inner product spaces over F of dimension ≤ 3. Then $V \cong W \iff \dim V = \dim W, \det V = \det W \in F^*/F^{2*}$ and $\operatorname{Hasse} V = \operatorname{Hasse} W \in \operatorname{Br}(F)$*

Proof. "$\Rightarrow$" is clear

"$\Leftarrow$": $\dim V = \dim W = 1$: $V \cong \langle \det V \rangle = \langle \det W \rangle \cong W$, hence we are done.

$\dim V = \dim W = 2$: Then $V \cong \langle a, b \rangle, W \cong \langle c, d \rangle$ (char$F \neq 2$). $(\frac{a,b}{F}) = \operatorname{Hasse}(V) = \operatorname{Hasse}(W) = (\frac{c,d}{F}) \Rightarrow \langle a, b, -ab \rangle \cong \langle c, d, -cd \rangle \underset{ab=cd \in F^*/F^{2*}}{\Rightarrow} \langle a, b \rangle \cong \langle c, d \rangle$ (Witt cancellation)

$\dim V = \dim W = 3$: $V \cong \langle a, b, c \rangle, W \cong \langle x, y, z \rangle, a, b, c, x, y, z \in F^*$. $\operatorname{Hasse}(\langle a, b, c \rangle) = (\frac{-abc,-1}{F}) \operatorname{Hasse}(\langle -ab, -ac, -bc \rangle)$ (Exercise).

$$\begin{aligned} \operatorname{Hasse}(V) = \operatorname{Hasse}(W) \quad &, \quad abc = \det V = \det W = xyz \\ \underset{(*)}{\Rightarrow} \operatorname{Hasse}(\langle -ab, -ac, -bc \rangle) \quad &= \quad \operatorname{Hasse}(\langle -xy, -xz, -yz \rangle) \\ \Rightarrow \left(\frac{-ab, -ac}{F}\right)\left(\frac{-ab, -bc}{F}\right)\left(\frac{-ac, -bc}{F}\right) \quad &= \quad \left(\frac{-xy, -xz}{F}\right)\left(\frac{-xz, -yz}{F}\right)\left(\frac{-xz, -yz}{F}\right) \\ \Rightarrow \left(\frac{-ab, ab}{F}\right)\left(\frac{-ac, -bc}{F}\right) \quad &= \quad \left(\frac{-xy, xy}{F}\right)\left(\frac{-xz, -yz}{F}\right) \end{aligned}$$

but $(\frac{-ab,ab}{F}) = (\frac{1,1}{F})$ because $\langle -ab, ab, 1 \rangle \cong \langle 1, 1, -1 \rangle$

$$\begin{aligned} \Rightarrow \left(\frac{-ac, -bc}{F}\right) \quad &\cong \quad \left(\frac{-xz, -yz}{F}\right) \\ \Rightarrow \left\langle -ac, -bc, -abc^2 \right\rangle \quad &\cong \quad \left\langle -xz, -yz, -xyz^2 \right\rangle \\ \Rightarrow \langle -abc \rangle \otimes \langle -ac, -bc, -ab \rangle \quad &\cong \quad \langle -xyz \rangle \otimes \langle -xz, -yz, -xy \rangle \text{ as } \langle -\det V \rangle = \langle -\det W \rangle \\ \Rightarrow \langle b, a, c \rangle \quad &\cong \quad \langle y, x, z \rangle \end{aligned}$$

□

Proposition 2.84. *Let F be a field with char$F \neq 2$. Assume that every 5-dimensional symmetric inner product space is isotropic, i.e., represent 0 non-trivially. Then for symmetric inner product spaces V, W over F, $V \cong W \iff \dim V = \dim W, \det V = \det W \in F^*/F^{2*}, \operatorname{Hasse}(V) = \operatorname{Hasse}(W) \in \operatorname{Br}(F)$*

Remark. Proposition applies when $F = \mathbb{Q}_p$ (See below). (Also if $F =$ any local field, or non-real number field)

Proof. Induction on $n = \dim V = \dim W$

$n \leq 3$: This case is the previous lemma

Assume $n \geq 4$. $V \perp \langle -1 \rangle$ has dimension ≥ 5 hence it is isotropic. $\Rightarrow V \perp \langle -1 \rangle \cong V_0 \perp \langle 1, -1 \rangle \Rightarrow V \cong V_0 \perp \langle 1 \rangle$. Similarly $W \cong W_0 \perp \langle 1 \rangle$. Now

- $\dim V_0 = \dim W_0 = n - 1$.
- $\det V_0 = \det V_0 \cdot \det \langle 1 \rangle = \det V = \det W = \det W_0$
- $\operatorname{Hasse}(V_0 \perp \langle 1 \rangle) = \operatorname{Hasse}(V) = \operatorname{Hasse}(W) = \operatorname{Hasse}(W_0 \perp \langle 1 \rangle) \Rightarrow \operatorname{Hasse}(V_0) \cdot \operatorname{Hasse}(\langle 1 \rangle) \cdot (\frac{\det V_0,1}{F}) = \operatorname{Hasse}(W_0) \cdot \operatorname{Hasse}(\langle 1 \rangle) \cdot (\frac{\det W_0,1}{F}) \underset{\det V_0 = \det W_0}{\Rightarrow} \operatorname{Hasse}(V_0) = \operatorname{Hasse}(W_0)$

So by induction hypothesis $V_0 \cong W_0 \Rightarrow V = V_0 \perp \langle 1 \rangle \cong W_0 \perp \langle 1 \rangle = W$ □

Corollary 2.85. *Let F be a field with char$F \neq 2$ for which every 5-dimensional form is isotropic. Then $I^3F = 0$*

Proof. Let V be a symmetric inner product space over F, $[V] \in I^3F \subset I(F) \Rightarrow \dim_F V = 2k$. If $4 \nmid \dim V$ replace V with $V \perp \mathbb{H}$, this doesn't change $[V] = [V \perp \mathbb{H}]$. Hence we can assume $\dim V = 4 \cdot l$ for some $l \in \mathbb{N}$. Now

- $\dim V = 4l = \dim \mathbb{H}^{2l}$
- $\det V = (-1)^{\frac{\dim V}{2}} \text{disc} V = 1$ because $[V] \in I^2$ and $(-1)^{\frac{\dim V}{2}} = (-1)^{2l} = 1$. But $\det \mathbb{H}^{2l} = 1$
- Hasse$(V) = (\frac{(-1)^l,-1}{F}) \underbrace{s(V)}_{[F]\in \mathrm{Br}} = (\frac{(-1)^l,-1}{F})$, since $[V] \in I^3 \subset \ker(s : I^2 \to \mathrm{Br})$. But Hasse $\mathbb{H}^{2l} = (\frac{(-1)^l,-1}{F})$

So by the proposition we have $V \cong \mathbb{H}^{2l} \Rightarrow [V] = 0 \in W(F)$ □

2.8 Quadratic Forms over p-adic numbers

Definition 2.86. The p-adic integers $\mathbb{Z}_p$ are ($p \in \mathbb{Z}$ prime)

$$\begin{aligned}
\mathbb{Z}_p &= \lim_{n\to\infty} \mathbb{Z}/p^n\mathbb{Z} \\
&= \{(x_n)_{n\in\mathbb{N}_{\geq 1}} | x_n \in \mathbb{Z}/p^n\mathbb{Z}, x_{n+1} \equiv x_n \mod p^n\} \\
&= \{\sum_{i=0}^{\infty} a_i p^i | a_i \in \{0, \dots, p-1\}\} \\
&= \text{completion of } \mathbb{Z} \text{ with repsect to } ||a||_p = p^{-\nu_p(a)}
\end{aligned}$$

$\mathbb{Z}_p$ is a Discrete Valuation Ring with maximal ideal $p\mathbb{Z}_p$ and residue field $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$

Definition 2.87. The p-adic rational numbers $\mathbb{Q}_p$ are

$$\begin{aligned}
\mathbb{Q}_p &= \text{field of fractions of } \mathbb{Z}_p \\
&= \text{completion of } \mathbb{Q} \text{ with respect to } ||a||_p = p^{-\nu_p(a)} \\
&= \{\sum_{i=N}^{\infty} a_i p^i | a_i \in \{0, \dots, p-1\}, N \in \mathbb{Z}\}
\end{aligned}$$

We have the surjective ring homomorphism $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ by $\sum_{i=1}^{\infty} a_i p^i \mapsto \sum_{i=1}^{k} a_i p^i \mod p^n$ ($k \geq n-1$). $x \in \mathbb{Z}_p$ is a unit $\iff x \in \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ is a unit ($\mathbb{Z}_p$ local). So $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ is a unit $\iff a_0 \neq 0$ in $\mathbb{F}_p$.

We want to understand $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$. If p is odd this is an exercise. For $p = 2$ we first look at $\mathbb{Z}_2^*/\mathbb{Z}_2^{2*}$. We have a ring homomorphism $\mathbb{Z}_2 \to \mathbb{Z}/8\mathbb{Z}$ defined by $\sum_{i=0}^{\infty} a_i 2^i \mapsto a_0 + a_1 2 + a_2 4$. Therefore $(\mathbb{Z}_2)^* \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^*$ is surjective by the map $1 + \sum_{i=1}^{\infty} a_i 2^i \mapsto 1 + a_1 2 + a_2 4$. Now $(\mathbb{Z}_2)^{2*} \to (\mathbb{Z}/8\mathbb{Z})^{2*} = \{1^2, 3^2, 5^2, 7^2\} = \{1\}$, so we have a well defined group homomorphism $(\mathbb{Z}_2)^*/(\mathbb{Z}_2)^{2*} \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^*$.

Proposition 2.88. *The map $\mathbb{Z}_2^*/\mathbb{Z}_2^{2*} \to (\mathbb{Z}/8\mathbb{Z})^*$ defined by $\sum_{i=0}^{\infty} a_i z^i \mapsto a_0 + a_1 2 + a_2 4$ is an isomorphism.*

Proof. We already know that the map is surjective. $z = 1 + \sum_{i=1}^{\infty} a_i 2^i \in$ kernel of the map $\iff a_1, a_2 = 0 \iff x = 1 + 8y$ for some $y \in \mathbb{Z}_2$. We need to sow that x is a square in $\mathbb{Z}_2$.

$$\begin{aligned}
z &= (1+8y)^{1/2} \\
&:= \sum_{k=0}^{\infty} \binom{1/2}{k} (8y)^k \\
&= \sum_{k=0}^{\infty} \binom{1/2}{k} 4^k (2y)^k \\
&= \sum_{k=0}^{\infty} b_k (2y)^k
\end{aligned}$$

where

$$\begin{aligned} b_k &= \binom{1/2}{k} 4^k \\ &= \frac{1/2(1/2-1)\cdot\dots\cdot(1/2-k+1)}{k!} 4^k \\ &= \frac{(1/2)^k \cdot 1\cdot(-1)\cdot\dots\cdot(-2k+3)}{k!} 4^k \\ &= (-1)^{k-1}\cdot 1\cdot 3\cdot\dots\cdot(2k-3)\cdot\frac{2^k}{k!}. \end{aligned}$$

Now $k = \nu_2(2^k) \geq \nu_2(k!)$ since $\nu_2(k!) \leq$ (number of even number $\leq k$) + (number of number divisible by $4 \leq k$) $+\dots \leq \lfloor \frac{k}{2} \rfloor + \lfloor \frac{k}{4} \rfloor + \dots \leq \sum_{i=1}^{\infty} \frac{k}{2^i} = \frac{k}{2}\sum_{i=0}^{\infty}\frac{1}{2^i} = \frac{k}{2}\frac{1}{1-\frac{1}{2}} = \frac{k}{2}2 = k$. Hence $\nu_2(b_k) \geq 0$ and since $\mathbb{Z}_2 = \{t \in \mathbb{Q}_2 | \nu_2(t) \geq 0\}$ we have that $b_k \in \mathbb{Z}_2$.

$$\begin{aligned} \left\| \sum_{k=n}^{m} \underbrace{b_k y^k}_{\in\mathbb{Z}_2} \cdot 2^k \right\|_2 &= \left\| \underbrace{\sum_{k=n}^{\infty} b_k y^k 2^{k-n}}_{\in\mathbb{Z}_2} \right\|_2 \|2^n\|_2 \\ &\leq 1\cdot 2^{-n} \end{aligned}$$

where $||a||_2 = 2^{-\nu_2(a)} \leq 1$ for all $a \in \mathbb{Z}_2$. Hence $m \mapsto \sum_{k=0}^{m} b_k y^k 2^k$ is a Cauchy sequence $\Rightarrow z := \sum_{k=0}^{\infty} b_k y^k 2^k$ defines an element in $\mathbb{Z}_2$. Then $z^2 = x$. □

Remark. For p odd $\mathbb{Z}_p^*/\mathbb{Z}_p^{2*} \overset{\cong}{\to} \mathbb{F}_p^*/\mathbb{F}_p^{2*}$ (reduction mod p) is an isomorphism (exercise)

Corollary 2.89. *The map*

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \overset{\cong}{\to} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^*/\mathbb{Z}_p^{2*} = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{2*} & p \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 = (\mathbb{Z}/2\mathbb{Z})^3 & p = 2 \end{cases}$$

defined by $p^\nu a \mapsto \nu, a$ where $a \in \mathbb{Z}_p^*$is an isomorphism.

Proof. For any Discrete Valuation Ring R with field of fractions F, the map $F^* \overset{\cong}{\to} \mathbb{Z} \times R^*$ defined by $p^\nu a \mapsto \nu, a$ where $a \in R^*$ is a isomorphism. Hence $F^*/F^{2*} \overset{\cong}{\to} \mathbb{Z}/2\mathbb{Z} \times R^*/R^{2*}$. Now $(\mathbb{Z}/8\mathbb{Z})^*$ is generated by $3, 5$ and $3^2 = 5^2 = 1 \mod 8$, hence $(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

Corollary 2.90. $\mathbb{Z}_2^*/\mathbb{Z}_2^{2*} = \{1, 3, 5, 7\}$ *and* $\mathbb{Q}_2^*/\mathbb{Q}_2^{2*} = \{1, 3, 5, 7, 2, 6, 10, 14\}$.

Proposition 2.91. *Let $p \in \mathbb{Z}$ be a prime. Then there is, up to isometry, a unique anisotropic 4-dimensional regular quadratic form over $\mathbb{Q}_p$. This form has determinant 1 and represents all of $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$.*

Proof. $p =$ odd (exercise)

$p = 2$: Consider all possible 2-dimensioanl forms $\langle 1, a\rangle$ where $a \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$. Set $D_a = \{t \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} | t$ represent $\langle 1, a\rangle\}$

$\langle 1, a\rangle$	$D_a \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} = \{1, 3, 5, 7, 2, 6, 10, 14\}$
$\langle 1, 1\rangle$	$1, 2, 5, 10$
$\langle 1, 2\rangle$	$1, 2, 3, 6$
$\langle 1, 3\rangle$	$1, 3, 5, 7$
$\langle 1, 5\rangle$	$1, 5, 6, 14$
$\langle 1, 6\rangle$	$1, 6, 7, 10$
$\langle 1, 7\rangle$	Hyperbolic
$\langle 1, 10\rangle$	$1, 3, 10, 14$
$\langle 1, 14\rangle$	$1, 2, 7, 14$

We check this table for $\langle 1, 1\rangle$: This represent $1, 2, 5, 10$ because $1 = 1\cdot 1^2 + 1\cdot 0^2$, $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$ and $10 = 3^2 + 1^2$, and it does not represent $3, 7, 6, 14$ because $x^2 + y^2 \in \{3, 7, 6, 14\}$ has no solution in $\mathbb{Z}_2$ since it has no solution $\mod 8$ as $x^2+y^2 \in \{0,1,2\} \mod 8$ since $x^2, y^2 \in \{0,1\} \mod 8$. If $x^2+y^2 = a \in \{3,7,6,14\}$ has a solution in $\mathbb{Q}_2$ clearing denominators (multiplying with respect to 2^n) $(*)\, x^2+y^2 = at^2$ has a solution in $\mathbb{Z}_2$ and not all of x,y,t are divisible by 2.

Case 1. $2 \nmid t$ then $t \in \mathbb{Z}_2^* \Rightarrow t^2 = 1 \mod 8$ and $(*)$ has no solution $\mod 8$

Case 2. $t = 2u$ and $2 \nmid x$ then $x^2 = 1 \mod 8$, $\underbrace{x^2}_{1} + y^2 = 4u^2 a$ has no solution $\mod 8$ as $y^2 \in \{1,0\}$ $\mod 8$.

Hence $\langle 1,1\rangle$ does not represent $3,7,6,14$.

We also can check that $\langle 1,1\rangle \cong \langle 2,2\rangle \cong \langle 5,5\rangle \cong \langle 10,10\rangle \ncong \langle 3,3\rangle \cong \langle 7,7\rangle \cong \langle 6,6\rangle \cong \langle 14,14\rangle$. e.g., $\langle 1,1\rangle \cong \langle 2,2\rangle \cong \langle 5,5\rangle \cong \langle 10,10\rangle$ since $\langle 1,1\rangle$ represents 2,5 and 10 and the all have the same determinant. Now $\langle 1,1\rangle \ncong \langle 3,3\rangle = \langle 3\rangle \cdot \langle 1,1\rangle$ because $\langle 1,1\rangle$ represent $1,2,5,10$ but $\langle 3\rangle \cdot \langle 1,1\rangle$ represents $3,6,15 = 7, 30 = 14 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^*$.

Let ϕ be a 4-dimensional anisotropic form over $\mathbb{Q}_2$, $\phi = \langle d, \dots\rangle$, then $\psi = \langle d\rangle\, \phi$ is also anisotropic and represent $d^2 = 1 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$. So $\psi = \langle 1, a, -b, -bc\rangle$ for some $a,b,c \in \mathbb{Q}_2^*$. Rewrite this as $\psi = \langle 1, a\rangle \perp \langle -b\rangle \cdot \langle 1, c\rangle$. If $\langle 1,a\rangle$ and $\langle b\rangle \cdot \langle 1,c\rangle$ represent a common element, then ψ represent 0 which contradicts the fact that ψ is anisotropic. Note also that $a, c \neq 7$ because $\langle 1,a\rangle$ and $\langle 1,c\rangle$ are not hyperbolic. Therefore $D_a \cap bD_c = \emptyset \underset{|D_a|=|D_c|}{\Rightarrow} D_a \sqcup bD_c = \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$. We can use the table to see $D_a \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$ is a subgroup. Now $1 \in D_a, D_c$, $1 \notin bD_c \underset{D_c\,\text{subgroup}}{\Rightarrow} bD_c \cap D_c = \emptyset \Rightarrow D_c \sqcup bD_c = D_a \sqcup bD_c = \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \Rightarrow D_a = D_c \underset{\text{table}}{\Rightarrow} a = c \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \Rightarrow \psi = \langle 1, a, -b, -ab\rangle \Rightarrow \det\psi = 1$. Now $\phi = \langle d^2\rangle \cdot \psi = \langle d\rangle\, \psi = \langle d, da, -db, -dab\rangle$ has determinant $= 1 \Rightarrow$ every anisotropic 4-dimensional form has determinant 1. In particular $\langle -1, a, -b, -ab\rangle$ is isotropic as it has determinant $-1 \neq 1 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \Rightarrow \langle -1, a, -b, -ab\rangle = \langle -1, 1, \dots\rangle \Rightarrow \langle a, -b, -ab\rangle$ represent 1. Hence $\psi = \langle 1, a, -b, -ab\rangle = \langle 1, 1, e, e\rangle$ since $\det\psi = 1$. But $e \notin \{3,7,6,14\}$ because otherwise $\langle e, e\rangle \underset{\text{table}}{=} \langle 7,7\rangle = \langle -1,-1\rangle$and ψ isotropic $\Rightarrow e \in \{1,2,5,10\}$, $\langle e,e\rangle \underset{\text{table}}{\cong} \langle 1,1\rangle \Rightarrow \psi = \langle 1,1,1,1\rangle$.

Let us check $\psi = \langle 1,1,1,1\rangle$ is indeed anisotropic because otherwise $\langle 1,1,1,1\rangle \cong \langle 1, -1, \_, \_\rangle \Rightarrow \langle 1,1,1\rangle$ represent $-1 = 7 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$ but $x^2+y^2+z^2 = 7$ has no solution in $\mathbb{Q}_2^*$ because $x^2+y^2+z^2$ has no solution in $\mathbb{Z}_2$ (since no solution $\mod 8$). If $x^2+y^2+z^2 = 7$ has a solution in $\mathbb{Q}_2$ then there exists $x^2+y^2+z^2 = 7t^2$ for some $x,y,z,t \in \mathbb{Z}_2$ and not all of x,y,z,t are divisible by 2.

Case 1. If $2 \nmid t$ then $t \in \mathbb{Z}_2^* \Rightarrow t^2 = 1 \mod 8$ contradiction since $x^2+y^2+z^2 = 7$ has no solution $\mod 8$

Case 2. If $2|t \Rightarrow t = 2u, u \in \mathbb{Z}_2$ and one of x,y,z is not divisible by 2, say $2 \nmid x \Rightarrow x^2+y^2+z^2 = 4\cdot 7\cdot u^2$ has no solution $\mod 8$ since $x^2 = 1 \mod 8$ and $y^2, z^2 \in \{1,0\} \mod 8$ while $4\cdot 7u^2 \in \{0,4\}$ $\mod 8$.

Hence $\psi = \langle 1,1,1,1\rangle$ is anisotropic.Now $\langle 1,1\rangle$, hence ψ, represents $1,2,5,10$ and ψ also represents $-1 = 7 = 2^2+1^2+1^2+1^2 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$. $\langle -1\rangle \cdot \psi$ represents 1 and is anisotropic $\Rightarrow \langle -1\rangle \cdot \psi = \psi \Rightarrow \psi \cong \langle -1,-1,-1,-1\rangle \equiv \langle 7,7,7,7\rangle \underset{\text{table}}{\Rightarrow} \psi \cong \langle d\rangle\, \psi = \phi\, \forall d \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$ ☐

Theorem 2.92. *Let $p \in \mathbb{Z}$ be a prime then:*

1. *Every 5-dimensional inner product space over $\mathbb{Q}_p$ is isotropic*
2. *$I^3(\mathbb{Q}_p) = 0$, $I^2(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$ generated by the unique anisotropic form of dimension 4. $I/I^2(\mathbb{Q}_p) = \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$, $\frac{W(\mathbb{Q}_p)}{I(\mathbb{Q}_p)} = \mathbb{Z}/2\mathbb{Z}$*

Proof. 1. $\langle a_1, \dots, a_5\rangle$ anisotropic $\Rightarrow \langle a_1, \dots, a_4\rangle$ is anisotropic hence is the unique 4-dimensional anisotropic form representing all of $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$, in particular $\langle a_1, \dots, a_4\rangle$ represents $-a_5 \Rightarrow \langle a_1, \dots, a_5\rangle$ isotropic

2. Now 1. $\Rightarrow I^3(\mathbb{Q}_p) = 0$ by Corollary 2.85. $I^2(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$ because let ϕ be the unique 4-dimensional anisotropic form over $\mathbb{Q}_p$ then $\phi \in I$ because $\dim\phi = 4 = 0 \in \mathbb{Z}/2\mathbb{Z}$ and $0 \neq \phi \in I^2$ because $\mathrm{disc}\phi = \det\phi = 1 \Rightarrow 0 \neq \phi \in \ker(\mathrm{disc}) = I^2$. If $0 \neq \psi \in I^2$ is anisotropic, $\phi \neq \psi \Rightarrow \dim\psi < 4, \dim\psi = 0 \mod 2$ since $\psi \in I, \Rightarrow \dim\psi = 2 \Rightarrow \psi = \langle a, b\rangle$ but $1 = \mathrm{disc}\psi = -ab$ since

disc$I^2 = 1 \Rightarrow \psi = \langle a, -a \rangle$ is hyperbolic, in particular not anisotropic $\Rightarrow \psi = 0 \in W(\mathbb{Q}_p)$. Hence, $I^2 = \{0, \phi\} = \mathbb{Z}/2\mathbb{Z}$. The rest is true for any field F with char$F \neq 2$

$\square$

Theorem 2.93. *Let $p \in \mathbb{Z}$ be a prime. Then the Witt groups of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are:*

Case 1. p odd:

$$W(\mathbb{Z}_p) \xrightarrow{\cong} W(\mathbb{F}_p) \qquad \text{(reduction} \quad \text{mod } p)$$

$$W(\mathbb{Q}_p) \xrightarrow[\cong]{\partial^1, \partial^2} W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$$

where ∂^1, ∂^2 are the first and second residue homomorphism ($\partial^1(\zeta) = \partial^2(\langle p \rangle \otimes \zeta)$)

Case 2. $p = 2$

$$W(\mathbb{Z}_2) \xrightarrow{\cong} \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$W(\mathbb{Q}_2) \xrightarrow{\cong} \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$$

Proof. The case p is odd is left as an exercise.

$p = 2$: $I^3(\mathbb{Q}_2) = 0, I^2(\mathbb{Q}_2) = \mathbb{Z}/2\mathbb{Z}, I/I^2(\mathbb{Q}_2) = \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \cong (\mathbb{Z}/8\mathbb{Z})^* \times (\mathbb{Z}/2\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^3, W(\mathbb{Q})/I = \mathbb{Z}/2\mathbb{Z}$. $0 = I^3 \subset I^2 \subset I \subset W(\mathbb{Q}_2)$. $|W(\mathbb{Q}_2)| = |W/I| \cdot |I/I^2| \cdot |I^2| = 2 \cdot 8 \cdot 2 = 32 \Rightarrow$ every element of $W(\mathbb{Q}_2)$ has order a power of 2. We have:

- $\langle 1 \rangle \in W(\mathbb{Q}_2)$ has order 8 because $0 \neq 4\langle 1 \rangle = \langle 1,1,1,1 \rangle$ as it is a generator of $I^2(\mathbb{Q}_2) = \mathbb{Z}/2\mathbb{Z}$ and $8\langle 1 \rangle = 4\langle 1 \rangle + 4\langle 1 \rangle = 4\langle 1 \rangle + 4\langle -1 \rangle = 0$ because $\langle 1,1,1,1 \rangle = \langle -1,-1,-1,-1 \rangle = \langle -1 \rangle \otimes \langle 1,1,1,1 \rangle$ (both are anisotropic and there exists a unique anisotropic form of dimension 4) over $\mathbb{Q}_2$.
- $\langle 1,3 \rangle \in W(\mathbb{Q}_2)$ has order 2 because it represents -1 as $1 + 3 \cdot 3^2 = 28 = 2^2 \cdot 7 = 7 = -1 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$. So $\langle 1,3 \rangle \cong \langle -1,-3 \rangle$ and $\langle 1,3 \rangle + \langle 1,3 \rangle = \langle 1,-1 \rangle + \underbrace{\langle 3,-3 \rangle}_{\text{hyperbolic}} = 0 \in W(\mathbb{Q}_2)$ and $\langle 1,3 \rangle \neq 0 \in W(\mathbb{Q}_2)$ since disc $\langle 1,3 \rangle = -3 = 5 \neq 1 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$
- $\langle 1,6 \rangle \in W(\mathbb{Q}_2)$ has order 2 because it represent -1 as $-1 = 7 = 1 \cdot 1^2 + 6 \cdot 1^2 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$. So $\langle 1,6 \rangle \cong \langle -1,-6 \rangle \Rightarrow \langle 1,6 \rangle + \langle 1,6 \rangle = \langle -1,-6 \rangle + \langle 1,6 \rangle = \langle 1,-1 \rangle + \langle 6,-6 \rangle = 0 \in W(\mathbb{Q}_2)$ and $0 \neq \langle 1,6 \rangle \in W(\mathbb{Q}_2)$ because disc $\langle 1,6 \rangle = -6 \neq 1 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$

Hence the map $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to W(\mathbb{Q}_2)$ defined by $a, b, c \mapsto a\langle 1 \rangle + b\langle 1,3 \rangle + c\langle 1,6 \rangle$ is well defined. Both groups have order 32. In order to show that the map is an isomorphism it suffices to show that it is injective. Assume $0 = a\langle 1 \rangle + b\langle 1,3 \rangle + c\langle 1,6 \rangle \in W(\mathbb{Q}_2)$. Now $b\langle 1,3 \rangle + c\langle 1,6 \rangle$ has order $\leq 2 \Rightarrow a\langle 1 \rangle$ has order $\leq 2 \Rightarrow a = 4 \mod 8 \Rightarrow a\langle 1 \rangle = a'\langle 1,1,1,1 \rangle$ with $a' \in \mathbb{Z}/2\mathbb{Z}$. We compute the discriminant

$$\begin{aligned}
\mathrm{disc}(a'\langle 1,1,1,1 \rangle + b\langle 1,3 \rangle + c\langle 1,6 \rangle) &= (\mathrm{disc}\,\langle 1,1,1,1 \rangle)^{a'} \cdot \mathrm{disc}(\langle 1,3 \rangle)^b \cdot \mathrm{disc}(\langle 1,6 \rangle)^c \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \\
&= 1 \cdot (-3)^3(-6)^c = 5^b \cdot 10^c \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}.
\end{aligned}$$

Now $5 \neq 10 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{2*}$, hence, they linearly independent in the $\mathbb{F}_2$-vector space in $\mathbb{Q}_2^*/\mathbb{Q}_2^{2*} = (\mathbb{Z}/2\mathbb{Z})^3 \Rightarrow b, c = 0 \in \mathbb{Z}/2\mathbb{Z} \Rightarrow a'\langle 1,1,1,1 \rangle = 0 \Rightarrow a' = 0$ since $\langle 1,1,1,1 \rangle \neq 0 \in W(\mathbb{Q}_2) \Rightarrow$ the map is injective. Hence $W(\mathbb{Q}_2) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

$\langle 1 \rangle, \langle 1,3 \rangle \in W(\mathbb{Z}_2)$ since $1, 3 \in \mathbb{Z}_2^*$, $W(\mathbb{Z}_2) \hookrightarrow W(\mathbb{Q}_2)$ is injective, it follows that $(\mathbb{Z}/8\mathbb{Z})\langle 1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z})\langle 1,3 \rangle \subset W(\mathbb{Z}_2) \Rightarrow |W(\mathbb{Z}_2)| \geq 8 \cdot 2 = 16$. Also $W(\mathbb{Z}_2) \to W(\mathbb{Q}_2) \overset{\partial^2}{\twoheadrightarrow} W(\mathbb{F}_2)$ is zero. $W(\mathbb{Z}_2) \subset \ker(\partial^2) \Rightarrow |W(\mathbb{Z}_2)| \leq |\ker(\partial^2)| = \frac{|W(\mathbb{Q}_2)|}{|W(\mathbb{F}_2)|} = \frac{32}{2} = 16 \Rightarrow |W(\mathbb{Z}_2)| = 16$. Hence $(\mathbb{Z}/8\mathbb{Z})\langle 1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z})\langle 1,3 \rangle = W(\mathbb{Z}_2)$. $\square$

Lemma 2.94 (Definition). *Set $\mathbb{Q}_\infty = \mathbb{R}$, $p = \infty =$ "infinite prime". For $p \in \mathbb{Z} \cup \{\infty\}$ prime there is a unique quaternion algebra over $\mathbb{Q}_p$ that doesn't split (i.e., $\ncong M_2(\mathbb{Q}_p)$). Therefore,* Hasse$(V) =$

$\begin{cases}[A] & \in \mathrm{Br}(\mathbb{Q}_p)\\ [\mathbb{Q}_p] & \in \mathrm{Br}(\mathbb{Q}_p)\end{cases}$, *where A is a division quaternion algebra. The* Hasse symbol $h_p(V)$ *for a symmetric inner product space V over $\mathbb{Q}_p$ is defined by*

$$h_p(V) = \begin{cases}-1 & \text{if } \mathrm{Hasse}(V)\,\text{does not split}\,(\neq [\mathbb{Q}_p] \in \mathrm{Br}(\mathbb{Q}_p))\\ 1 & \text{if } \mathrm{Hasse}(V) = [\mathbb{Q}_p] \in \mathrm{Br}(\mathbb{Q}_p)\end{cases}$$

For $a, b \in \mathbb{Q}_p^*$, the Hilbert Symbol *is:*

$$(a,b)_p = h_p(\langle a,b\rangle) = \begin{cases}1 & \textit{if } \left(\frac{a,b}{\mathbb{Q}_p}\right) \text{splits}\\ -1 & \text{if } \left(\frac{a,b}{\mathbb{Q}_p}\right) \text{does not split}\end{cases}$$

Proof. We need to justify that there exists a unique non-split quaternion algebra over $\mathbb{Q}_p$. If $p = \infty$ then $\mathrm{Br}(\mathbb{Q}_\infty) = \mathrm{Br}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\}$, so $\mathbb{H}$ is the unique non-split quaternion algebra over $\mathbb{R}$.

If $p < \infty$: $(\frac{a,b}{\mathbb{Q}_p}), (\frac{c,d}{\mathbb{Q}_p}) \not\cong M_2(\mathbb{Q}_2) \iff \langle a, b, -ab, -1\rangle, \langle c, d, -cd, -1\rangle \not\cong \langle 1, 1, -1, -1\rangle$ (all forms are in $I^2(\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z}$ as disc $= 0$ for them) $\iff \langle a, b, -ab, -1\rangle, \langle c, d, -cd, -1\rangle$ are both the unique anisotropic 4-dimensional form over $\mathbb{Q}_p \iff \langle a, b, -ab, -1\rangle \cong \langle c, d, -cd, -1\rangle \not\cong \langle 1, 1, -1, -1\rangle \iff (\frac{a,b}{\mathbb{Q}_p}) \cong (\frac{c,d}{\mathbb{Q}_p}) \not\cong (\frac{1,1}{\mathbb{Q}_p}) = M_2(\mathbb{Q}_p)$. □

Hilbert Reciprocity Law. *Let V be a symmetric inner product space over $\mathbb{Q}$. Then $h_p(V) = 1$ for all but finitely many primes $p \in \mathbb{Z} \cup \{\infty\}$. And $\prod_{p \in \mathbb{Z}\cup\{\infty\}\text{ prime}} h_p(V) = 1$*

Proof. Since $h_p(V)$ is a product of Hilbert Symbols $(a,b)_p$, it suffices to show claim for $V = \langle a, b\rangle$ and thus $\prod_{p\in\mathbb{Z}\cup\{\infty\}}(a,b)_p = 1\,\forall a, b \in \mathbb{Q}_p^*$. To show $\prod(a,b)_p = 1$, using bilinearity of Hilbert symbol $(ab, c) = (a,c)_p(b,c)_p$, we just need to show $\prod(a,b)_p = 1$ for a, b prime or ±1. In this case, express $(a,b)_p$ in terms of Legendre symbol which mean the proof is a consequence of Quadratic Reciprocity. (Details are left as an exercise) □

Corollary 2.95. *Let V, W be inner product spaces over $\mathbb{Q}$. Let $q \in \mathbb{Z} \cup \{\infty\}$ be a prime. If $h_p(V) = h_p(W)\,\forall p \in \mathbb{Z}\cup\{\infty\}$ prime, $p \neq q$. Then $h_q(V) = h_q(W)$*

Proof. $\prod_{p\in\mathbb{Z}\cup\{\infty\}} h_p(V) = 1 = \prod_{p\in\mathbb{Z}\cup\{\infty\}} h_p(W)$ □

We will need this theorem:

Theorem 2.96 (Dirichlet)**.** *Let $a, b \in \mathbb{Z}$ be integers with $\gcd(a,b) = 1$, then the set of integers of the form $a + nb$, $n \in \mathbb{Z}$, contains infinitely many primes.*

Proof. This theorem is beyond the scope of this module □

Strong Hasse principle for quadratic forms over $\mathbb{Q}$. *A symmetric inner product space V over $\mathbb{Q}$ is isotropic if and only if V is isotropic over $\mathbb{R}$ and $\mathbb{Q}_p\,\forall p \in \mathbb{Z}$ prime.*

Remark. The Theorem says: A homogeneous quadratic polynomial has a non-trivial zero in $\mathbb{Q}$ if and only if it has a non-trivial zero in $\mathbb{R}$ and $\mathbb{Q}_p\,\forall p \in \mathbb{Z}$ prime.

Proof. **"$\Rightarrow$":** Is clear.

"$\Leftarrow$": We assume Dirichlet Theorem. We use induction on $n = \dim_{\mathbb{Q}} V$

- **$n = 1$:** Every 1-dimensional inner space is anisotropic (over any field)
- **$n = 2$:** A 2-dimensional form V is isotropic over $\mathbb{Q}$ (any field of characteristic not 2) $\iff$ V hyperbolic over $\mathbb{Q}$, i.e., $V \cong \mathbb{H} \iff V \cong \mathbb{H}$ over $\mathbb{R}$ and $\mathbb{Q}_p\,\forall p \in \mathbb{Z}$ prime $\iff$ V is isotropic over $\mathbb{R}$ and $\mathbb{Q}_p\,\forall p \in \mathbb{Z}$ prime
- **$n = 3:$** V isotropic over $\mathbb{Q} \iff V \cong \langle 1, -1, -\det V\rangle$ over $\mathbb{Q} \iff V \cong \langle 1, -1, -\det V\rangle$ over $\mathbb{R}$ and $\mathbb{Q}_p\,\forall p$ prime (Weak Hasse Principle) $\iff$ V isotropic over $\mathbb{R}$ and $\mathbb{Q}_p\,\forall p$ primes.
- **$n = 4$:** Write $V = \langle d_1, d_2, d_3, d_4\rangle$ with $d_i \in \mathbb{Z}\setminus\{0\}$ square free, $d = \det V$ square free. Let $\mathscr{P} = \{2\} \cup \{p \in \mathbb{Z}\text{ prime } : p | d_1 \dots d_4\} < \infty$. Write V_p for $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Now V_p is isotropic by assumption, $\Rightarrow V_p \cong \langle 1, -1\rangle \perp \langle a_p, -a_p d\rangle$ (over $\mathbb{Q}_p$) with $a_p \in \mathbb{Z}\setminus\{0\}$ square free.

- If $p \notin \mathscr{P}$ we can assume that $a_p \in \mathbb{Z}_p^*$ and $a_\infty = 1$. Otherwise if $p = \infty$ replace (V, β) with $(V, -\beta)$, and if $\infty \neq p \notin \mathscr{P}$ we would have $a_p = pb_p$ (as $a_p \in \mathbb{Z}_p \setminus \{0\}$ square free). Therefore, $0 \underset{p \nmid d_1 \ldots d_4}{=} \partial_p^2 V = \partial_p^2 \langle 1, -1, pb_p, -pb_p d\rangle = \langle b_p, -b_p d\rangle \Rightarrow \operatorname{disc}\langle b_p, -b_p d\rangle = d = 1 \in \mathbb{F}_p^*/\mathbb{F}_p^{2*} \cong \mathbb{Z}_p^*/\mathbb{Z}_p^{2*}$ and d is a square in $\mathbb{Q}_p \Rightarrow \langle a_p, -a_p d\rangle \cong \langle a_p, -a_p\rangle \cong \langle 1, -1\rangle$ over $\mathbb{Q}_p$ and we can even assume $a_p = 1$
- There exists $q \in \mathbb{Z}$ prime such that $a := q\pi = a_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}\, \forall p \in \mathscr{P}$ where $\pi = \prod_{p \in \mathscr{P}, \nu(a_p)=1} p$ (Note $\nu(a_p) = 0$ or 1 as $a_p \in \mathbb{Z}_p$ is square free). To justify existence of q note that $a_p = \pi u_p, u_p \in \mathbb{Z}_p^*$. By the Chinese Remainder Theorem $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/8\mathbb{Z} \times \prod_{p \in \mathscr{P}, p \neq 2} \mathbb{Z}/p\mathbb{Z}$ is surjective. So there exists an integer r such that $r = a_2 \in (\mathbb{Z}/8\mathbb{Z})^* \subset \mathbb{Z}/8\mathbb{Z}$ and $r = u_p \in \mathbb{Z}/p\mathbb{Z}$ for $p \in \mathscr{P} \setminus \{2\}$. In fact, any integer of the form $r + ns$ with $s = 2^3 \prod_{p \in \mathscr{P} \setminus \{2\}} p$ can be chosen instead of r. Since the a_p's are units, it follows that s and r are relatively prime. By Dirichlet's theorem on existence on infinitely many primes in an arithmetic progression, we can choose $r = q$ a prime. By construction $a = q\pi = a_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$.

Claim: $V \cong \langle 1, -1\rangle \perp \langle a, -ad\rangle$ over $\mathbb{Q}$ (in particular, V isotropic over $\mathbb{Q}$ as it contains $\mathbb{H}$)

Proof of claim: By the weak Hasse principle it suffices to show that $(V_p =)\ \langle 1, -1, a_p, -a_p d\rangle = \langle 1, -1, a, -ad\rangle$ over $\mathbb{Q}_p\ \forall p \in \mathbb{Z} \cup \{\infty\}$ prime.

Case 1. $p \in \mathscr{P}$: We have $\langle a_p, -a_p d\rangle \cong \langle a, -ad\rangle$ since, by construction of a, we have $a = a_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$ for $p \in \mathscr{P}$.

Case 2. $p \notin \mathscr{P}$ and $p \neq q, \infty$: One checks that ∂^1 and ∂^2 agree: $\partial^1\langle a_p, -a_p d\rangle = \langle a_p, -a_p d\rangle = \langle a, -ad\rangle = \partial^1\langle a, -ad\rangle \in W(\mathbb{F}_p)$ because p does not divide a, a_p, d and over $\mathbb{F}_p$ quadratic forms are classified by rank and determinant. Further, we have $\partial^2\langle a_p, -a_p d\rangle = 0 = \partial^2\langle a, -ad\rangle \in W(\mathbb{F}_p)$ because p does not divide a, a_p, d. And so $\underset{p \neq 2}{\Rightarrow} \langle a, -ad\rangle \cong \langle a_p, -a_p d\rangle$ over $\mathbb{Q}_p$.

Case 3. $p = \infty$: $\langle a, -ad\rangle = \langle a_\infty, -a_\infty d\rangle$ over $\mathbb{R} = \mathbb{Q}_\infty$ because $a_\infty = 1$ and $a > 0$.

Case 4. q: Over $\mathbb{Q}_q$ the forms $\langle 1, -1, a, -ad\rangle$ and V have the same rank ($= 4$), determinant d and Hasse invariant (by Hilbert reciprocity, as both are isometric over $\mathbb{Q}_p$, $p \neq q$, and thus have same Hasse symbol over $\mathbb{Q}_p$, $p \neq q$) $\Rightarrow \langle 1, -1, a, -ad\rangle \cong V$ over $\mathbb{Q}_q$.

$n \geq 5$**:** Choose an orthogonal sum decomposition $V \cong U \perp W$ with $\dim U = 2$ and $\dim W = n - 2 \geq 3$. Want to find a non-degenerate subspace of V of dimension less than n which is isotropic over $\mathbb{R}$ and $\mathbb{Q}_p\, \forall p$. Then by induction hypothesis, this subspace is isotropic over $\mathbb{Q}$, hence V is isotropic over $\mathbb{Q}$. If (U or) W is isotropic over $\mathbb{R}$ and $\mathbb{Q}_p\, \forall p$ then by induction (U or)W is isotropic over $\mathbb{Q}$ (then so is V and we are done). Hence suppose W anisotropic over some $\mathbb{Q}_p$. Let $\mathscr{P} = \{p \in \mathbb{Z} \cup \{\infty\} \text{ prime} | W \text{ anisotropic over } \mathbb{Q}_p\}$ ($\neq \emptyset$). $\mathscr{P}$ is a finite set because $\dim W \geq 3$ and $\langle a, b, c\rangle$ ($a, b, c \in \mathbb{Z}$) is isotropic over $\mathbb{Q}_p$ ($p \neq 2$) if and only if $\langle a, b, c\rangle \cong \langle 1, -1, -abc\rangle$ over $\mathbb{Q}_p$, but if $p \nmid a, b, c$ and $p \neq 2, \infty$ then $\langle a, b, c\rangle \cong \langle 1, -1, -abc\rangle$ over $\mathbb{Q}_p$. (This holds because if $p \neq 2, \infty$ then $\partial^2\text{LHS} = 0 = \partial^2\text{RHS}$, $\partial^1\text{LHS} = \langle a, b, c\rangle = \langle 1, -1, -abc\rangle = \partial^1\text{RHS}$, recall $W(\mathbb{Q}_p) \underset{\partial^1, \partial^2}{\cong} W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$ and over $\mathbb{F}_p$ quadratic forms are classified by rank and determinant)

Let q be the quadratic form of (V, β), $q(x) = \beta(x, x)$, q isotropic over $\mathbb{Q}_p\, \forall p \in \mathbb{Z} \cup \{\infty\}$ prime. Hence $\forall p \in \mathbb{Z} \cup \{\infty\}$ there exists $0 \neq u_p \in U \otimes \mathbb{Q}_p$ and $0 \neq w_p \in W \otimes \mathbb{Q}_p$ such that $q(u_p) + q(w_p) = 0$

Claim: There exists $u \in \mathbb{Z} \setminus \{0\}$ such that $q(u) = q(u_p) \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$ for all $p \in \mathscr{P}$

Then the claim $\Rightarrow \mathbb{Q}u \perp W \subset V$ has dimension $n-1$ and is isotropic over $\mathbb{R}$ and $\mathbb{Q}_p\, \forall p$ prime because W isotropic over $\mathbb{Q}_p\, \forall p \notin \mathscr{P}$ and $Qu \perp W$ isotropic over $p \in \mathscr{P}$ as $q(u) + q(w_p) = 0\, \forall p \in \mathscr{P}$. So by induction hypothesis the subspace $\mathbb{Q}u \perp W$ is isotropic over $\mathbb{Q} \Rightarrow V$ is isotropic over $\mathbb{Q}$

Justification of the claim: Now $q = ax^2 + by^2$ with $a, b \in \mathbb{Z} \setminus \{0\}$ so $u_p = (x_p, y_p) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Case 1. Assume first $\infty \notin \mathscr{P}$, then $p^{l_p}\xi_p = q(u_p) = ax_p^2 + by_p^2 \in \mathbb{Z}_p \setminus \{0\}$ where $\xi_p \in \mathbb{Z}_p^*$ and $l_p \in \mathbb{Z}_{\geq 0}$. By the Chinese Remainder Theorem the map $\mathbb{Z} \twoheadrightarrow \prod_{p \in \mathscr{P}} \mathbb{Z}/p^{l_p+3} = \prod_{p \in \mathscr{P}} \mathbb{Z}_p/p^{l_p+3}$ is surjective. Hence there exists $x, y \in \mathbb{Z}$ such that $x = x_p,\ y =$

$y_p \mod p^{l_p+3}$ for $p \in \mathscr{P}$. and Set $u = (x, y)$. Then $q(u) = ax^2 + by^2 = ax_p^2 + by_p^2 \in \mathbb{Z}_p/p^{l_p+3}$ implies that $ax^2 + by^2 = p^{l_p} e_p$ with $e_p = \xi_p \mod p^3$. Now $\xi_p \in \mathbb{Z}_p^*$ implies that $\xi_p = e_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}$ due to the fact that

- $e_p = \xi_p \mod p^3$
- $\mathbb{Z}_p^*/\mathbb{Z}_p^{2*} = \mathbb{F}_p^*/\mathbb{F}_p^{2*} \mod p$ (p odd)
- $\mathbb{Z}_2^*/\mathbb{Z}_2^{2*} = (\mathbb{Z}/2^3\mathbb{Z})^*$

Now $\xi_p = e_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \Rightarrow p^{l_p}\xi_p = p^{l_p} e_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}\, \forall p \in \mathscr{P} \Rightarrow ax^2 + by^2 = ax_p^2 + by_p^2 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \Rightarrow q(u) = q(u_p) \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}\, \forall p \in \mathscr{P}$

Case 2. If $\infty \in \mathscr{P}$, $\mathbb{Q}_\infty = \mathbb{R}$. Then $q(u_\infty) \in \mathbb{R}^*/\mathbb{R}^{2*}$ either > 0 or < 0, by replacing q with $-q$ we can assume $q(u_\infty) > 0$. Let $u_\infty = (x_\infty, y_\infty) \in \mathbb{R} \times \mathbb{R}$, $q(u_\infty) = ax^2 + by^2$ not both $a, b < 0$ since $q(u_\infty) > 0$, so without loss of generality we can assume $a > 0$. Choose x, y as in the first case such that moreover $x^2 > -\frac{b}{a} y^2$ then $q(u) = q(u_p) \in \mathbb{Q}_p^*/\mathbb{Q}_p^{2*}\, \forall p \in \mathscr{P} \setminus \{\infty\}$ as above. Furthermore $q(u) = ax^2 + by^2 > 0 \Rightarrow q(u) = q(u_\infty) \in \mathbb{R}^2/\mathbb{R}^{2*}$.

This ends the proof of the claim.

□

Definition 2.97. Let q be a rational (or integral) quadratic form. Then q is said to be

- *positive definite* if $q(x) > 0\, \forall x \neq 0$.
- *negative definite* if $q(x) < 0\, \forall x \neq 0$.
- *indefinite* if q is neither positive nor negative definite.

Corollary 2.98. *Let q be a rational quadratic form of dimension ≥ 5. If q is indefinite, then it represents 0 over $\mathbb{Q}$.*

Proof. By the strong Hasse principle, we nee to see that q represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ for all $p \in \mathbb{Z}$ prime. Since q indefinite $\Rightarrow q_{\mathbb{R}} = \langle 1, -1 \rangle \perp \ldots$ so q represent 0 over $\mathbb{R}$. Since dimension of $q \geq 5 \Rightarrow q$ represent 0 over $\mathbb{Q}_p$ for all p prime because every 5 dimensional form over $\mathbb{Q}_p$ is isotropic. □

2.9 Integral quadratic forms

Recall $W(\mathbb{Z}) \underset{\text{sgn}}{\overset{\cong}{\rightarrow}} \mathbb{Z}$.

Definition 2.99. A symmetric inner product space over $\mathbb{Z}$, (V, β) is called:

- *even* (or of type II) if $\beta(x, x) \in \mathbb{Z}$ is even $\forall x \in V$
- *odd* (or of type I) if $\exists x \in V$ such that $\beta(x, x) \in \mathbb{Z}$ is odd.

Remark.

- A symmetric inner product space over $\mathbb{Z}$ is also called unimodular lattice
- If q is a quadratic form over $\mathbb{Z}$ then $\beta(x, y) = q(x + y) - q(x) - q(y)$ and $\beta(x, x) = 2q(X)$. So the even symmetric inner product spaces over $\mathbb{Z}$ are precisely the inner product spaces that come from regular quadratic forms.

Lemma 2.100. *Let (V, β) be an indefinite symmetric inner product space over $\mathbb{Z}$ then there exists $x \in V, x \neq 0$ such that $\beta(x, x) = 0$.*

Proof. Recall that the image of $W(\mathbb{Z}) \hookrightarrow W(\mathbb{Q})$ is generated by $\langle 1 \rangle$ and $\langle -1 \rangle$. (V, β) indefinite $\Rightarrow V_{\mathbb{Q}} = V \otimes_{\mathbb{Z}} \mathbb{Q} = \langle 1, -1 \rangle \perp \ldots$ isotropic $\Rightarrow \exists x \in V_{\mathbb{Q}}$, $x \neq 0$ such that $\beta(x, x) = 0$. But $V \subset V_{\mathbb{Q}}, x = \frac{y}{n}$ for some $n \in \mathbb{Z} \setminus \{0\}$, $y \in V \Rightarrow \beta(y, y) = \beta(nx, nx) = n^2 \beta(x, x) = 0$ and $0 \neq y \in V$ □

Theorem 2.101. *Let (V, β) be an odd (i.e., type I) indefinite symmetric inner product space over $\mathbb{Z}$. Then (V, β) has an orthogonal basis. In particular $(V, \beta) \cong m \langle 1 \rangle \perp n \langle -1 \rangle$ over $\mathbb{Z}$.*

Proof. Claim: $(V,\beta) \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & \text{odd} \end{pmatrix} \right\rangle \perp (V',\beta')$.

The theorem follows from claim by induction on dimension V: For $k \in \mathbb{Z}$ we have

$$\begin{pmatrix} 0 & 1 \\ 1 & 2k+1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k+1 & k \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & k+1 \\ 1 & k \end{pmatrix}}_{\det=-1} \Rightarrow \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 2k+1 \end{pmatrix} \right\rangle \cong \langle 1, -1 \rangle .$$

From this the theorem follows as we have $\langle 1 \rangle \perp V'$ or $\langle -1 \rangle \perp V'$ is indefinite and both are odd and have dimension less that V, and $V = \langle \pm 1 \rangle \perp (\langle \mp 1 \rangle \perp V')$

To prove the claim: We know (V,β) indefinite $\underset{\text{previous lemma}}{\Rightarrow}$ $\exists x \in V$ with $x \neq 0$ and $\beta(x,x) = 0$. Now (V,β) inner product space over $\mathbb{Z} \Rightarrow V = \mathbb{Z}^n$. So $x = (a_1, \dots, a_n) \in \mathbb{Z}^n$, we can assume $d = \gcd(a_1, \dots, a_n) = 1$ (otherwise replace x with $\frac{x}{d}$). We can extend x to a $\mathbb{Z}$ basis $x_1 = x, x_2, \dots, x_n$ of $V = \mathbb{Z}^n$ because $\phi : V/\mathbb{Z}x \to (V \otimes_{\mathbb{Z}} \mathbb{Q})/\mathbb{Q}x$ is injective as $y = (c_1, \dots, c_n) \in \ker \phi$ then $\exists r, s \in \mathbb{Z}$ with $r \neq 0$ and $ry = sx \Rightarrow rc_i = sa_i$ for all $i = 1, \dots, n$, since $\gcd(a_1, \dots, a_n) = 1$ there exists $b_1, \dots, b_n \in \mathbb{Z}$ such that $\sum a_i b_i = 1$. So $r \sum c_i b_i = s \sum a_i b_i = s \Rightarrow s = rt$ where $t = \sum c_i b_i$, hence $ry = sx \Rightarrow ry = rtx \underset{r \neq 0}{\Rightarrow} y = tx \Rightarrow y = 0 \in V/\mathbb{Z}x$. Hence our map is indeed injective. Now $V/\mathbb{Z}x$ is a finitely generated $\mathbb{Z}$-module, submodule of $\frac{V \otimes_{\mathbb{Z}} \mathbb{Q}}{\mathbb{Q}x} = \mathbb{Q}^{n-1} \Rightarrow V/x$ is a free $\mathbb{Z}$-module $\Rightarrow V \overset{p}{\twoheadrightarrow} V/x$ has a section $\sigma : V/\mathbb{Z}x \to V$ $(p\sigma = 1) \Rightarrow V = x \oplus \underbrace{\operatorname{im} \sigma}_{\cong V/x \cong \mathbb{Z}^{n-1}}$. Hence x can be extended to a $\mathbb{Z}$-basis $x_1 = x, x_2, \dots, x_n$ of V.

Let $y_1, \dots, y_n$ be the dual basis of $x_1, \dots, x_n$, i.e., $\beta(x_i, y_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$ which exists because β is non-degenerated $\Rightarrow \beta : V \overset{\cong}{\to} \operatorname{Hom}(V, \mathbb{Z}) \cong \mathbb{Z}^n$ has a $\mathbb{Z}$ basis $e_1, \dots, e_n$, where $(e_i)(\sum \alpha_j x_j) = \alpha_i$, $y_i \overset{\beta}{\leftrightarrow} e_i$. Now (V,β) odd $\Rightarrow$ there exists $k \in \{1, \dots, n\}$ such that $\beta(y_k, y_k)$ is odd. If $\beta(y_1, y_1)$ is odd then $\beta|_{(\mathbb{Z}x_1 + \mathbb{Z}y_1)} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & \text{odd} \end{pmatrix} \right\rangle \Rightarrow (V,\beta) \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & \text{odd} \end{pmatrix} \right\rangle \overset{\text{non-degenerate}}{\perp} (\mathbb{Z}x_1 \oplus \mathbb{Z}y_1)^{\perp}$. If $\beta(y_1, y_1)$ even and $\beta(y_k, y_k)$ odd for $k \neq 1$ then $\beta|_{(\mathbb{Z}x_1 + \mathbb{Z}(y_1 + y_k))} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & \text{odd} \end{pmatrix} \right\rangle \Rightarrow (V,\beta) \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & \text{odd} \end{pmatrix} \right\rangle \overset{\text{non-degenerate}}{\perp} (\mathbb{Z}x_1 \oplus \mathbb{Z}(y_1 + y_k))^{\perp}$ ☐

Theorem 2.102. *If (V,β) is an even symmetric inner product space over $\mathbb{Z}$ then its signature is divisible by* 8.

Proof. Let (V,β) be an arbitary symmetric inner product space over $\mathbb{Z}$. Then $V/2V = V \otimes_{\mathbb{Z}} \mathbb{F}_2$ is a symmetric inner product space over $\mathbb{F}_2$. But over $\mathbb{F}_2$ the map $x \mapsto \beta(x,x)$ is linear because $\beta(x+y, x+y) = \beta(x,x) + \underbrace{2\beta(x,y)}_{=0} + \beta(y,y) \in \mathbb{F}_2$. As $V/2V$ is non degenerate, there exists a unique $\overline{u} \in V/2V$ such that $\beta(\overline{u}, x) = \beta(x,x) \mod 2 \, \forall x \in V$. If $u, u' \in V$ are two lifts of $\overline{u} \in V/2V$ then $u' = u + 2v$ for some $v \in V$, and $\beta(u', u') = \beta(u,u) + 4(\underbrace{\beta(u,v) + \beta(v,v)}_{=0 \mod 2}) = \beta(u,u) \in \mathbb{Z}/8\mathbb{Z}$ because $\beta(u,v) = \beta(v,v) \in \mathbb{F}_2$ by definition of u. Set $\phi(V) := \beta(u,u) \in \mathbb{Z}/8\mathbb{Z}$ for any lift u of $\overline{u} \in V/2V$. We have seen that $\phi(V)$ does not depend on the lift u of $\overline{u}$. From the definition of ϕ we have $\phi(V \perp W) = \phi(V) + \phi(W)$ and $\phi(\langle 1 \rangle) = 1$, $\phi(\langle -1 \rangle) = -1$, so $\phi : W(\mathbb{Z}) \to \mathbb{Z}/8\mathbb{Z} : V \mapsto \phi(V)$ is a well defined map. If (V,β) is even then $\beta(x,x) = 0 \mod 2 \, \forall x \in V$ and we can choose $\overline{u} = 0 \Rightarrow u = 0 \Rightarrow \phi(V) = 0 \in \mathbb{Z}/8\mathbb{Z}$. Since $\phi(\langle 1 \rangle) = 1 \Rightarrow \phi : \mathbb{Z} \cdot \langle 1 \rangle = W(\mathbb{Z}) \to \mathbb{Z}/8\mathbb{Z}$ is the signature. Now, if (V,β) is even then $\beta(x,x) = 0 \mod 2 \, \forall x \in V$ and $\overline{u} = 0 \Rightarrow$ we can choose $u = 0 \Rightarrow \phi(V) = 0 \in \mathbb{Z}/8\mathbb{Z}$. This implies that signature of any even symmetric inner product space over $\mathbb{Z}$ is divisible by 8. ☐

Corollary 2.103. *Every even positive definite inner product space over $\mathbb{Z}$ has rank divisible by* 8.

Proof. If M is positive definite then $\operatorname{rk} M = \operatorname{sgn} M$. ☐

Theorem 2.104. *Let M, N be indefinite symmetric inner product spaces over $\mathbb{Z}$. Then $M \cong N$ $\iff$ M, N have the same rank, signature and type (odd or even).*

Proof. If M, N are odd then M, N have orthogonal basis, by Theorem 2.101,then the theorem follows.
If M, N are even, we do not have the time to prove this in this course. $\square$

Example. Of even positive definite inner product spaces over $\mathbb{Z}$.

General Remark: Let $\mathbb{R}^n$ be equipped with standard Euclidean inner product $\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = \sum_{i=1}^n x_i y_i$. If $M \subseteq \mathbb{R}^n$ is a finitely generated $\mathbb{Z}$-submodule, then $M \cong \mathbb{Z}^k$ for some $k \leq n$. Restricting $\langle , \rangle_{\mathbb{R}^n}$ to M defines a symmetric bilinear form $\beta(x, y) = \langle x, y \rangle \in \mathbb{R}$ on M with values in $\mathbb{R}$. Assume $\operatorname{rk}_{\mathbb{Z}} M = n = \dim_{\mathbb{R}} \mathbb{R}^n \Rightarrow \mathbb{R}^n/M$ compact Riemanian manifold. $\operatorname{Vol}(\mathbb{R}^n/M)$ = volume of parallelepiped spanned by a $\mathbb{Z}$-basis of M. If we let $A = (b_1, \ldots, b_n)$ where $b_1, \ldots, b_n$ is a $\mathbb{Z}$-basis of M then $\operatorname{Vol}(\mathbb{R}^n/M) = |\det A| = \sqrt{\det(A^T A)} = \sqrt{\det \underbrace{(\langle b_i, b_j \rangle)_{i,j=1,\ldots,n}}_{\text{biliner form matrix of } M}} \Rightarrow$ a finitely generated $M \subset \mathbb{R}^n$ of $\operatorname{rk}_{\mathbb{Z}} M = n$ defines a (positive definite) inner product space over $\mathbb{Z}$ if and only if:

- $\langle x, y \rangle \in \mathbb{Z} \, \forall x, y \in M$, and
- $\operatorname{Vol}(\mathbb{R}^n/M) = 1$

In fact every possible definite inner product space (M, β) over $\mathbb{Z}$ arises in that way, because $\mathbb{R}^n \cong M \otimes_{\mathbb{Z}} \mathbb{R} \supset M$ and $\beta_{\mathbb{R}} \cong \underbrace{\langle 1, \ldots, 1 \rangle}_{n}$ over $\mathbb{R}$ since (M, β) is positive definite.

Lemma 2.105. *Let $E_{4m} \subseteq \mathbb{R}^{4m}$ be the $\mathbb{Z}$-submodule ($m \in \mathbb{Z}_{\geq 1}$) generated by $e_i + e_j$ $(i, j = 1, \ldots, 4m)$ and $\frac{1}{2}(e_1 + e_2 + \cdots + e_{4m})$ where $e_i = (0, \ldots, 0, \underset{\substack{\uparrow \\ i}}{1}, 0, \ldots, 0)$ is the standard basis vector of $\mathbb{R}^{4m}$. Then E_{4m} is a symmetric inner product space over $\mathbb{Z}$ of rank $4m$ which is even (respectively odd) if m is even (respectively odd)*

Proof.

- $E_{4m} \subset \mathbb{R}^{4m}$ finitely generated $\mathbb{Z}$-submodule $\Rightarrow E_{4m}$ free $\mathbb{Z}$-module, i.e., $E_{4m} \cong \mathbb{Z}^k$. Now $\operatorname{rk}_{\mathbb{Z}} E_{4m} = \dim_{\mathbb{Q}} E_{4m} \otimes_{\mathbb{Z}} \mathbb{Q} = 4m$ because $e_i + e_j, i, j = 1, \ldots, 4m$ and $\frac{1}{2}(e_1 + \cdots + e_{4m})$ span $\mathbb{Q}^n$. (Note that this contains $2e_i, i = 1, \ldots, m$ by setting $i = j$).
- $\langle x, y \rangle \in \mathbb{Z} \, \forall x, y \in E_{4m}$. (check for x, y generators of E_{4m}). E.g., $\langle e_i + e_j, e_i + e_j \rangle = \begin{cases} 2 & i \neq j \\ 4 & i = j \end{cases}$, $\left\langle \frac{1}{2}(e_1 + \cdots + e_{4m}), \frac{1}{2}(e_1 + \cdots + e_{4m}) \right\rangle = \frac{1}{4} 4m = m \Rightarrow E_{4m}$ is even if and only if m even.
- We are left to check it is non-degenerate. We will use the following trick: If $M \subset N \subset \mathbb{R}^n$ of rank n $\mathbb{Z}$-submodule, then $\mathbb{R}^n/M \twoheadrightarrow \mathbb{R}^n/N$ covering with $|N/M|$ sheets because N/M acts freely on $\mathbb{R}^n/M$ with quotient $\mathbb{R}^n/N$. So $|N/M| \cdot \operatorname{Vol}(\mathbb{R}^n/N) = \operatorname{Vol}(\mathbb{R}^n/M) \, \forall M \subset N \subset \mathbb{R}^n$ rk $= n$ $\mathbb{Z}$-submodules.

  Now we prove E_{4m} is non-degenerate, i.e., $\operatorname{Vol}(\mathbb{R}^{4m}/E_{4m}) = 1$. Let $E^0 \subset E_{4m}$ be the $\mathbb{Z}$-submodule generated by $e_i + e_j, i, j = 1, \ldots 4m$. Then E_{4m}/E^0 is generated by $\xi = \frac{1}{2}(e_1 + \cdots + e_{4m}) \notin E^0$, and $2\xi \in E^0$ so $2\xi = 0 \in E_{4m}/E^0$. Therefore $E_{4m}/E^0 = \mathbb{Z}/2\mathbb{Z} \Rightarrow 2\operatorname{Vol}(\mathbb{R}^{4m}/E_{4m}) = \operatorname{Vol}(\mathbb{R}^{4m}/E^0)$. But notice $E^0 \subset \mathbb{Z}^{4m}$ where $\mathbb{Z}^{4m}$ is generated by $e_1, \ldots, e_{4m}$. Now $\mathbb{Z}^{4m}/E^0$ is generated by e_1 because $e_i = e_i + e_1 - e_1 \, \forall i = 2, \ldots, 4m$. Now $e_1 \notin E^0$ but $2e_1 = e_1 + e_1 \in E^0 \Rightarrow \mathbb{Z}^{4m}/E^0 = \mathbb{Z}/2\mathbb{Z} \Rightarrow \operatorname{Vol}(\mathbb{R}^{4m}/E^0) = 2\operatorname{Vol}(\mathbb{R}^{4m}/\mathbb{Z}^{4m}) \Rightarrow \operatorname{Vol}(\mathbb{R}^{4m}/E^{4m}) = \operatorname{Vol}(\mathbb{R}^{4m}/\mathbb{Z}^{4m}) = 1 \Rightarrow E_{4m}$ is non-degenerate.

$\square$

Corollary 2.106. *E_{8m} is an even positive definite symmetric inner product space of rank $8m$*

Fact. *For all $n \in \mathbb{Z}_{\geq 0}$, $\{$symmetric inner product spaces over $\mathbb{Z}$ of given rank $n\}/$isometry is a finite set.*

Example.

rank$n$	8	16	24	32
number of even positive definite inner products space over $\mathbb{Z}$	1	2	24	Unknown ≥ 10
representative	E_8	$E_{16}, E_8 \perp E_8$	Niemeier (1968)	