Quadratic Forms

Marco Schlichting
Notes by Florian Bouyer

January 22, 2012

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

Definition 1. Let \( R \) be a (commutative) ring and \( M \) a (left) \( R \)-module. Then a \textit{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 2. A bilinear form \( \beta : M \times M \to R \) is called \textit{symmetric} if \( \beta(x, y) = \beta(y, x) \forall x, y \in M \). It is called \textit{skew-symmetric} if \( \beta(x, y) = -\beta(y, x) \forall x, y \in M \). It is called \textit{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 \( (x_1, y_1) \times (x_2, y_2) \to x_1y_2 - x_2y_1 \) is symplectic and skew-symmetric

Remark. Any symplectic bilinear form is also skew-symmetric because \( \beta \) 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 \( \beta \) 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 3. A bilinear form \( \beta : M \times M \to R \) is called \textit{regular} or \textit{non-degenerate} or \textit{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 \( f(y) = \beta(x, y_0) \)

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. \( r, l : M \to M^v = \text{Hom}_R(M, R) = \{ f : M \to R : f \text{ is } R\text{-linear} \} \) 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. \( \text{say } r, l \text{ are surjective} \)

2. \( \text{say } r, l \text{ are injective} \)

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. injectivity \( \Rightarrow 2. \) surjectivity)

Definition 4. Let \( (M, \beta), (M', \beta') \) be bilinear forms. An \textit{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 \( (M, \beta) \) and \( (M', \beta') \) are isometric then \( (M, \beta) \) is symmetric (skew-symmetric, symplectic, regular) if and only if \( (M', \beta') \) is.

Definition 5. Let \( M \) be an \( R \)-module. A \textit{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 → 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 → M' such that q(x) = q'(f(x)) ∀x ∈ M.

Remark. If β is a (symmetric) bilinear form then \( q_β(x) = β(x, x) \) is a quadratic form because \( q_β(ax) = β(ax, ax) = a^2β(x, x) \) and \( \beta_q(x, y) = q_β(x + y) - q_β(x) - q_β(y) = β(x + y, x + y) - β(x, x) - β(y, y) = β(x, y) + β(y, x) \) is bilinear.

If β is symmetric then \( q_β = 2β \)

Corollary 6. If \( \frac{1}{2} \in R \) (i.e. 2 ∈ R is a unit) and M is an R-module then \{quadratic forms on M\} → \{symmetric bilinear forms on M\} by \( q \mapsto q_β \) is a bijection with inverse \{symmetric bilinear forms on M\} → \{quadratic forms on M\} defined by \( β \mapsto \frac{1}{2}q_β \).

Proof. Exercise □

Remark. If \( \frac{1}{2} \notin R \) 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 \( \mathbb{Z} \times \mathbb{Z} → \mathbb{Z} \) defined by \( x, y \mapsto xy \) does not come from a quadratic forms on \( \mathbb{Z} \) because if \( q : \mathbb{Z} → \mathbb{Z} \) is a quadratic form then \( q(a) = q(a \cdot 1) = a^2q(1) \) and \( β_q(x, y) = q(x + y) - q(x) - q(y) = (x + y)^2q(1) - x^2q(1) - y^2q(1) = 2xyq(1) \neq xy \)

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 7. A polynomial \( f = \sum a_{i_1,...,i_n} x_1^{i_1}...x_n^{i_n} ∈ R[x_1,...,x_n] \) is called homogenous of degree m if all occurring monomials \( x_1^{i_1}...x_n^{i_n} (a_{i_1,...,i_n} ≠ 0) \) has degree \( i_1 + ... + i_n = m \)

Example. \( x^3 + x^2y + z^3 \) is homogenous of degree 3
\( x^3 + x^2y + z^3 \) is not homogenous.

Every homogenous degree 2 polynomial \( f ∈ R[x_1,...,x_n] \) 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 \( f ∈ R[x_1,...,x_n] \) one can associate a (polynomial) function \( \bar{f} : R^n → R \) by \( (r_1,...,r_n) → f(r_1,...,r_n) \).

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

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

Claim. If \( f ∈ R[x_1,...,x_n] \) is homogenous of degree 2 then \( \bar{f} : \mathbb{R}^n → \mathbb{R} \) is a quadratic from

Proof. Note: If \( q_1, q_2 \) are quadratic forms on M then \( q_1 + q_2 \) and \( a q_1 \) are all quadratic forms \( ∀ a ∈ R \). Thus can assume \( f = x_i x_j \). Then \( f(r_1,...,r_n) = r_i r_j \) so

1. \( \bar{f}(ar) = a^2 \bar{f}(r) ∀ a ∈ R, r ∈ \mathbb{R}^n \)
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 \( r, s ∈ \mathbb{R}^n \)

Lemma 8. For any (commutative!) ring \( R \), the map
\[
\begin{cases}
\text{homogenous polynomials of degree 2 in } n \text{ variables} \\
\rightarrow \{\text{quadratic forms } R^n\}
\end{cases}
\]
defined by \( f → \bar{f} \) is bijective.
Proof. Exercise

If \( R^n \to R^n \) 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 \( x_j \mapsto A_*(x_j) = \sum_{j=1}^na_{ij}x_j \) which sends homogenous polynomials of degree \( m \) to homogenous polynomials of the degree \( m \).

Definition 9. 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 10. The map

\[
\{ \text{homogenous polynomials of degree 2 in } n \text{ variables} \} / \text{linear equivalence} \to \{ \text{quadratic forms on } R^n \} / \text{isometry}
\]

is bijective.

Proof. Exercise

1.1 Free bilinear form modules

Definition 11. A bilinear \( R \)-module \((M,\beta)\) is called free of rank \( n \) (\( n \in \mathbb{N} \)) if \( M \cong R^n \)

If \((M,\beta)\) 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 \( \beta \) 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 \( B = \begin{pmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{pmatrix} \)

Lemma 12. Let \((M,\beta)\) be a free bilinear form module of rank \( n \) with basis \( e_1,...,e_n \), then \( \beta \) is non-degenerate \( \iff \) the associated bilinear form matrix \( B = \beta(e_i,e_j) \in M_n(R) \) is invertible

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

\[
x \mapsto r(x) = \beta(x,-), \quad r(x)(y) = \beta(x,y)
\]

\[
\mapsto l(x) = \beta(-,x), \quad l(x)(y) = \beta(y,x)
\]

are bijective. \( M \) has basis \( e_1,...,e_n \). Then \( \text{Hom}_R(M,R) \) has basis \( e^1,...,e^n \) where \( e^i_j \) where \( e^i_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \)

i.e. \( e^i_j \) \( (\sum x_je_j) = x_i \). Let \((r_i)\) receptively \((l_i)\) be the \( n \times n \) of \( r,l \) with respect to basis \( e_1,...,e_n \) of \( M \) and \( e^1,...,e^n \) of \( \text{Hom}_R(M,R) \) i.e.

\[
\sum_{k=1}^n r_{ij}e^k = r(e_j) \quad \text{and} \quad \sum_{k=1}^n l_{kj}e^k = l(e_i) \quad \text{so} \quad \beta(e_j,e_i)r(e_j) = \sum_{k=1}^n r_{kj}e^k(e_i) = \sum_{k=1}^n r_{kj}e^k(e_i) = r_i \quad \forall i,j \Rightarrow (r_i) = B^T = \text{transpose of } B.
\]

Similarly \((e^i_j) = B \) so \( \beta \) non degenerated \( \iff \) \( r,l \) are isometry \( \iff \) \( (r_i)(l_i) \) are invertible \( \iff \) \( B^T,B \) are invertible

\( \Box \)

Lemma 13. Let \((M,\beta),(M',\beta')\) be two free bilinear form modules over \( R \) of rank \( n \) with basis \( e_1,...,e_n \) for \( M' \) then \((M,\beta)\) and \((M',\beta')\) 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. \( \Rightarrow \) \( \Rightarrow \): Let \( f : M \to M' \) be an isometry. Let \((f_i)\) 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 \( \Rightarrow \) \( (f_i) \) invertible and \( \beta(e_i,e_j) = \beta'(f(e_i),f(e_j)) = \beta'(\sum_{k=1}^n f_{ki}e'_k,\sum_{l=1}^n f_{lj}e'_l) = \sum_{l=1}^n f_{ki}\beta'(e'_k,e'_l)f_{lj} = (A^T B' A)_{ij} \). Hence \( B = A^T B' A \)

\( \Leftarrow \): \( A = (f_i) \in M_n(R) \) 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

\( \Box \)

Definition 14. Let \( B \in M_n(R) \) we let \((B)\) stand for the bilinear form module \((R^n,\beta),\beta : R^n \times R^n \to R \) defined by

\[
(x,y) \mapsto \beta(x,y) = x^T B y
\]

This is a free bilinear form module with basis \( e_1,...,e_n \) 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. \((B) \cong (B')\) for \(B, B' \in M_n(R) \iff \exists A \in M_n(R)\) invertible such that \(B' = A^TBA\)

**Definition 15.** The **determinant** of a non-degenerate free bilinear form module \(M = (M, \beta)\) with basis \(e_1, \ldots, e_n\) is the determinant \(\det M = \det(\beta(e_i, e_j))_{i,j=1,\ldots,n} \in R^*/R^{2*}\). 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 \(\beta(e_i', e_j') = A^T(\beta(e_i, e_j))A \Rightarrow \det(\beta(e_i', e_j')) = (\det(A))^2 \det(\beta(e_i, e_j))\)

**Example.** Recall \((a)\) is \(R \times R \rightarrow R\) defined by \(x, y \mapsto axy\).

- If \((1) = (2) \Rightarrow \det(1) = \det(2) \in R^*/R^{2*} \Rightarrow 2\) is a square \(\Rightarrow (1) \not\in (2)\) over \(Q\)
- If \(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow 1 = -1 \in R^*/R^{2*} \Rightarrow (-1)\) is a square \(\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\)

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

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

**Proof.** Exercise.

**Lemma 16.** Let \(R\) be (commutative!) ring and \(f : R^n \rightarrow R^k\) 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 \(f : (R/m)^n \rightarrow (R/m)^l\) 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 \(\infty\) dimension and \(A = \text{End}_k(V)\) then \(A \oplus A \cong A\) as \(A\) module

\section{Orthogonal sum}

**Definition 17.** Let \((M, \beta)\) and \((M', \beta')\) be two bilinear form modules. Their **orthogonal sum** \((M, \beta) \perp (M', \beta')\) has underlying module \(M \oplus M'\) and bilinear form \((M \oplus M') \rightarrow R\) 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 \((B) \perp (B') = \begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix}\)
- If \((M, \beta)\) and \((M', \beta')\) are regular (symmetric, skew-symmetric, symplectic) then so is \((M, \beta) \perp (M', \beta')\)

**Definition 18.** Let \((M, \beta)\) 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 19.** Let \((M, \beta)\) be symmetric or skew-symmetric and \(N \subset M\) a sub-module such that \((N, \beta|_N)\) 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 \(\beta|_N\) is non degenerate we have \(x = 0\). So \(M \supset N + N^\perp = N \perp N^\perp\).

We next need to check \(N + N^\perp = M\). Let \(x \in M\) then \(\beta(x,-)|_N \in \text{Hom}_R(N,R)\) \(\beta|_N\text{ non-degenerate} \Rightarrow \exists x_0 \in N\) \(\beta(x,y) = \beta(x_0,y) \forall y \in N\) then \(\beta(x-x_0, y) = 0 \forall y \in N \Rightarrow x - x_0 \in N^\perp \Rightarrow x = x_0 + x - x_0\). Thus \(N + N^\perp = M\), \(N \supset N^\perp = M\)

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 \(\beta(x + u, y + v) = \beta(x,y) + \beta(x,v) + \beta(u,v) + \beta(u,v) = \beta(N,x,y) + \beta(N^\perp, u,v)\)

**Corollary 20.** If \((M, \beta)\) 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 $\beta(x, x) = R \setminus R^* \forall x \in M_0 = M$ then take $N = M_0 = M$ and we are done. So assume $\exists x \in M_0 : \beta(x, x) \in R^* \text{ then } ax \neq 0 \in M \forall a \in R \setminus \{0\}$ (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. 

$\Rightarrow M = \frac{Rx}{\langle u_1, \ldots, u_k \rangle}$ with $u_1 = \beta(x, x) \in R^*$ contradicting Lemma 16.

Repeat with $M_1$ in place of $M_0$ to obtain $M = \langle u_1 \rangle \cap \cdots \cap \langle u_n \rangle \subseteq M_k$. We can repeat 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 $R^n \rightarrow M = \langle u_1 \rangle \cap \cdots \cap \langle u_n \rangle \subseteq M_k \rightarrow R^k \Rightarrow n \geq k$

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

Proof. If $N = \langle u_1 \rangle \cap \cdots \cap \langle u_n \rangle$ and if $N$ is non-degenerate with respect to base $e_1, \ldots, e_n$ then $\langle u_i \rangle$ are non-degenerate 

$\Rightarrow u_i \in R^*$. $\beta(e_i, e_j) = \begin{cases} u_i & i = j \in 1, \ldots, l \\ 0 & i \neq j \end{cases}$ in particular $\beta(e_1, e_1) = u_1 \in R^*$

Theorem 21 (Existence of orthogonal basis over fields of char $\neq 2$). Let $k$ be a field of char $\neq 2$ and $(M, \beta)$ a finite dimensional symmetric bilinear form. Then $M = \langle u_1 \rangle \cap \cdots \cap \langle u_l \rangle \subseteq N$ such that $\beta|_N = 0$, $\beta(x, y) = 0$ $\forall x, y \in N$. In particular $(M, \beta)$ has an orthogonal basis, $e_1, \ldots, e_l$ such that $\beta(e_i, e_j) = \begin{cases} 0 & j = i + 1, \ldots, n \\ 0 & j \neq i \end{cases}$

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

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

Definition 22. 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 $k = R/m \subset R$ 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 $m \subset R \Rightarrow m \subset R \setminus R^*$.

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

$(R, m, k)$ 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 $m = 0$

- $\mathbb{Z}_p = \{ \frac{a}{p} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \mid b \} \text{ where } p \in \mathbb{Z} \text{ is prime. This is a local ring with maximal ideal } m = \{ \frac{a}{p} \in \mathbb{Q} : p \mid b, p \mid a \}$. Then $\mathbb{Z}_p/m = \mathbb{F}_p$

- $k$ field $k[T]/T^n$ is a local ring with maximal ideal $(T)$

Definition 23. 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 24. 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 $\exists N : M \oplus N \cong R^n$. Let $p : R^n \rightarrow R^a$ be the linear map $R^n \xrightarrow{f} M \oplus N \xrightarrow{g} M \oplus N \xrightarrow{f^{-1}} R^n$ and let $p$ be the composition of all these maps. Note that $p^2 = (f^{-1}qf)^2 = f^{-1}qff^{-1}qf = f^{-1}q^2f = p$ and $im \frac{f}{p} \cong M$.
Then an other base change gives $\mu \oplus \nu$ leads to $\mu \oplus \nu$ and $\mu \oplus \nu$.

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 $\mathbb{Z}^n$ for some finite abelian group. If $F$ is finitely generated projective over $\mathbb{Z}$ then $P \subseteq \mathbb{Z}^n \Rightarrow P$ has no element of finite order. $\Rightarrow P = \mathbb{Z}^n$ for some finite abelian group.

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 $I \subseteq R$ 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 $I \cong \mathbb{Z}^n$, $n \neq 0$ because $I \neq 0$. Let’s compute $R/I$:

$$
\begin{align*}
R/I &= \mathbb{Z}[T]/(T^2 + 5, 2, 1 + T) \\
&= \mathbb{F}_2[T]/(T^2 + 5, T + 1) \\
&= \mathbb{F}_2[T]/(T^2 + 1, T + 1) \\
&= \mathbb{F}_2[T]/((T + 1)^2, T + 1) \\
&= \mathbb{F}_2[T]/(T + 1) \\
&\cong \mathbb{F}_2
\end{align*}
$$
Assume $n = 1$ then $I = R t$ for some $t \in R$. Now $t$ is not a unit because otherwise $0 = R / R t$ contradicting $R / I = F_2$. If $t \notin R^*: I = R t \Rightarrow 2 = a t \Rightarrow a \in R^* \Rightarrow I = R t = R_{1/2} \Rightarrow R \cdot 2$ and irreducible

$$R / I = \frac{\mathbb{Z}[T]}{T^2 + 5} / \frac{I}{2R}$$

$$= \mathbb{Z}[T] / (T^2 + 5, 2)$$

$$= F_2[T] / (T^2 + 1)$$

$$= F_2[T] / (T + 1)^2$$

$$\neq F_2$$

$\Rightarrow I \cong R^n \Rightarrow n \geq 2$. So $R^n \cong I \subset R$, let $F$ be 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 $n \neq 2$.

**Definition 25.** An inner product space is a non-degenerate bilinear form module $(M, \beta)$ where $M$ is finitely generated and projective.

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

**Definition 26.** Let $R$ be a ring. The hyperbolic plane $\mathbb{H}$ is the symmetric inner product space $\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$ 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 $\mathbb{H} \cong (1) \perp (-1)$ because $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} \\ 1 & \frac{1}{2} \end{pmatrix}$ 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 $\begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2 x y \notin R^* \forall x, y \in \mathbb{H}$ since $2 \notin R^*$. If $(\mathbb{H}, \beta)$ had an orthogonal basis $e_1, e_2$ then $\beta(e_i, e_j) \in R^* \Rightarrow \mathbb{H}$ has no orthogonal basis.

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

**Theorem 27.** Let $(R, m, k)$ be a local ring and $M = (M, \beta)$ a symmetric inner product space.

- If $\text{char} k \neq 2$ then $M$ has an orthogonal basis

- If $\text{char} k = 2$ then $M = \langle u_1 \rangle \perp \cdots \perp \langle u_1 \rangle \perp N_1 \perp \cdots \perp N_r$ where $u_i \in R^*$ and $N_i = \langle \begin{pmatrix} a_i & 1 \\ 1 & b_i \end{pmatrix} \rangle$, $a_i, b_i \in m$

**Proof.** Recall $M$ finitely generated, $\beta$ is symmetric $\Rightarrow M = \langle u_1 \rangle \perp \cdots \perp \langle u_1 \rangle \perp N$ 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 $\Rightarrow M \cong R^n + 1$, same for $N$ so $N \cong R^n$.

If $n = 0$ done. So assume $n \geq 1$. Then $\beta$ non-degenerate $\Rightarrow \exists \varphi : R^n = N \rightarrow R$ 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 $\text{char} k \neq 2$ ($2 \notin m = R \setminus R^* \Rightarrow 2 \in R^*$). If $N \neq 0 \Rightarrow \exists x, y \in N, \beta(x, y) = 1$. Then $x + y \in N$ so $\beta(x + y, x + y) = \beta(x, x) + 2\beta(x, y) + \beta(y, y) \Rightarrow 2 \in m \Rightarrow N = 0$ (due to the contradiction of $\text{char} k \neq 2$)

Now assume that $\text{char} k = 2$. 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 $\beta : R \times R \rightarrow R, \beta(x, y) = xy \cdot \beta(1, 1)$ and $\beta$ 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 $N \cong R^n, \varphi : R^n \rightarrow R$ by
Motivation: Let Corollary 30.

Example. \( \beta \) and free modules of finite rank (over a commutative ring), and also over finitely generated projective modules over local rings. Since \( \det \) done \( Z \) : \( M \) ⇒ \( (2) \) \( \beta \) \( \in R^* \) ⇒ \( x, y \) linearly independent

and \( N_1 := Rx + Ry \subset N \) is isometric to \( \left( \begin{array}{c}
\alpha \\
1 \\
b
\end{array} \right) \) ⇒ \( N = N_1 \cap N_1^\perp \) and apply induction hypothesis to \( N_1^\perp \) and we are done \( \Box \)

Example. \((M, \beta) = \left( \begin{array}{c}
2 \\
1 \\
1
\end{array} \right) \) over \( \mathbb{Z}(2) = \{ \frac{a}{q} \in \mathbb{Q} : q \} \). \( \det \left( \begin{array}{c}
2 \\
1 \\
1
\end{array} \right) = 3 \) 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 \( M = \left( \begin{array}{c}
0 \\
1 \\
1
\end{array} \right) \) 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, \( x = \left( \begin{array}{c}
1 \\
0
\end{array} \right) \) 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 \( (Rx)^\perp = \{ y \in M : \beta(x, y) = 0 \} = \left\{ \left( \begin{array}{c}
\alpha \\
\beta
\end{array} \right) \in \mathbb{R}^2 | (1 \ 0) \left( \begin{array}{c}
2 \\
1 \\
1
\end{array} \right) \left( \begin{array}{c}
\alpha \\
\beta
\end{array} \right) = 0 \right\} = R \left( \begin{array}{c}
1 \\
-2
\end{array} \right) \Rightarrow \left( \begin{array}{c}
\alpha \\
\beta
\end{array} \right) \in \mathbb{R} \) 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 28. Let \((M, \beta)\) be a symplectic inner product space (\( \beta \) symplectic if \( \beta(x, x) = 0 \forall x \in M \)). A symplectic basis of \( M \) is a basis \( x_1, y_2, x_2, y_3, ..., x_n, y_n \) 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 \( \beta \) w.r.t. the basis \( x_1, y_1, ..., x_n, y_n \) is

\[
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
-1 & 0 & 1 & \cdots & 0 \\
0 & -1 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & 1 & -1 \\
-1 & \cdots & 0 & -1 & 0
\end{pmatrix}
\]

Theorem 29. Let \((R, m, k)\) be a local ring and \((M, \beta)\) a symplectic inner product space. Then \((M, \beta)\) has a symplectic basis

Proof. \((M, \beta)\) inner product space ⇒ \( \beta \) non-degenerate, \( M \) projective ⇒ free (since \( R \) local) ⇒ \( \exists x, y \in M : \beta(x, y) = 1 \).
So the inner product matrix of \( \beta \) with respect to \( \{ x, y \} \) is \( \left( \begin{array}{c}
\beta(x, x) \\
\beta(x, y) \\
\beta(y, x) \\
\beta(y, y)
\end{array} \right) \) \( \beta_{\text{symplectic}} = \left( \begin{array}{c}
0 & 1 \\
-1 & 0
\end{array} \right) \). 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 ⇒ \( M = N_1 \cap N_1^\perp \) repeating the same argument with \( N_1^\perp \) instead of \( M \) we obtain \( M = N_1 \cap N_2 \cap \cdots \cap N_n \)

\[\left( \begin{array}{c}
0 \\
-1
\end{array} \right) \]

where \( N_i = \left( \begin{array}{c}
0 \\
-1
\end{array} \right) \) \( N_i \)

\( \Box \)

Corollary 30. Over a local ring any symplectic inner product space has even dimension. Moreover, two symplectic inner product spaces are isometric if and only if they have the same rank.

2.0.1 With 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 $\langle -1 \rangle \perp \langle -1 \rangle \perp \langle -1 \rangle \cong \langle -1 \rangle \perp \mathbb{H}(\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \rangle \cong \langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rangle \rangle \cong \langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \rangle \rangle \; \text{but} \; \langle -1 \rangle \perp \langle -1 \rangle \cong \mathbb{H}$ because $\mathbb{H}$ has no orthogonal basis over $\mathbb{F}_2$.