Number Theory Notes

JLH

Date

Contents

Definition – Quadratic Form, bilinear form
Let M be a module over A a ring. Then $Q : M \to A$ is a quadratic form if

1. $\forall a \in A, \forall x \in M, Q(ax) = a^2Q(x)$
2. $\forall x, y \in M$,the map $M^2 \to A$ defined by $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is bilinear.

We say (Q, M) is a quadratic module.

We say $(\star \cdot \star) : M^2 \to A$ is a symmetric bilinear form if $\forall x, y \in M, (x \cdot y) = (y \cdot x)$.

Proposition – Correspondence between quadratic forms and symmetric bilinear forms
Let M be an A-module. Suppose $2 \in A^*$.

1. For any quadratic form $Q : M \to A$ there exists a symmetric bilinear form $(\star \cdot \star) : M^2 \to A$ such that $(x \cdot y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$.
2. For any symmetric bilinear form $(\star \cdot \star) : M^2 \to A$ there exists a quadratic form $Q : M \to A$ such that $Q(x) = (x \cdot x)$.
3. Going one way and then the other recovers the same form.

Note that in fields of characteristic 2 this would not work. We refer to $(\star \cdot \star)$ as the induced symmetric bilinear form of Q.

Definition – Metric morphism
Let $(V, Q), (V', Q')$ be quadratic forms. Then $f : V \to V'$ is a metric morphism if

1. f is linear.
2. $Q' \circ f = Q$.

We write $f : (V, Q) \to (V', Q')$ meaning the above.

Proposition – Metric morphisms commute with the bilinear form
Let $(V, Q), (V', Q')$ be quadratic forms and use $(\star \cdot \star)$, to denote their induced symmetric bilinear forms. If $f : V \to V'$ is a metric morphism then for all $x, y \in V$, $(f(x) \cdot f(y)) = (x \cdot y)$.

Proof. Let $x, y \in V$, then

$$\begin{aligned}
&(f(x) \cdot f(y)) \\
&= \frac{1}{2}(Q'(f(x) + f(y)) - Q'(f(x)) - Q'(f(y))) \\
&= \frac{1}{2}(Q(x + y) - Q(x) - Q(y)) \\
&= (x \cdot y)
\end{aligned}$$

□

Proposition – Matrix of a quadratic form
Suppose (Q, V) is a quadratic module over field K with finite dimension n. Take B a basis of V.

1. For any $x \in V$, writing $x_B = \sum_{i=1}^{n} x_i e_i$ gives us
$$Q(x) = \sum_{i=1}^{n} \sum_{j=1}^{n} (e_i \cdot e_j) x_i x_j$$
2. There exists a unique matrix given by $T_B = (e_i \cdot e_j)_{i,j=1}^{n} \in K^{n \times n}$ such that $Q(x) = x_B^T T_B x_B$.
3. The matrix T_B is symmetric; we call it the matrix of the quadratic form Q with respect to basis B.
4. Given another basis C of V and a change of basis matrix $X : K^{n \times n} \to K^{n \times n}$ taking basis B to C, we have
$$T_B = X^T T_C X$$
Thus $\det(T_B) = \det(X)^2 \det(T_C)$. Hence the determinant is determined up to multiplication by a square.
5. If $x, y \in V$ then $x \cdot y = x_B^T T_B y_B$.

Proof.

$$\begin{aligned}
Q(x) &= Q(\sum_{i=1}^{n} x_i e_i) \\
&= \left(\sum_{i=1}^{n} x_i e_i\right) \cdot \left(\sum_{i=1}^{n} x_i e_i\right) \\
&= \sum_{i=1}^{n} \left(x_i (e_i \cdot \sum_{j=1}^{n} x_j e_j) \right) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} (x_j x_i (e_i \cdot e_j)) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} (e_i \cdot e_j) x_i x_j \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} (T_B)_{ij} x_i x_j \\
&= x_B^T T_B x_B
\end{aligned}$$

Uniqueness of T_B follows from the fact that if T' were a matrix satisfying the above then it would agree on each T'_{ij}, hence determining the same matrix. Checking that T_B is symmetric follows from $(\star \cdot \star)$ being symmetric.

Let C be another basis of V X be the change of basis matrix from B to C. Then for any $x \in V$,

$$x_B^T X^T T_C X x_B = (X x_b)^T T_C (X x_b) = Q(X x_b)$$

By the definition of T_C. Hence by uniqueness of T_B in satisfying this property $X^T T_C X = T_B$.

Let $x, y \in V$ then

$$\begin{aligned}
x \cdot y &= \frac{1}{2} \left(Q(x+y) - Q(x) - Q(y)\right) \\
&= \frac{1}{2} (x_B^T T_B y_B + y_B^T T_B x_B) \\
&= \frac{1}{2} (x_B^T T_B y_B + x_B^T T_B^T y_B) \\
&= x_B^T T_B y_B
\end{aligned}$$

The third equality is because it is a 1×1 matrix, the fourth using the fact that T_B is symmetric. □

Definition – Discriminant

Suppose (Q, V) is a finite dimensional quadratic module over field K. Let B be a basis of V and T_B be the matrix of Q with respect to B. If $\det(T_B) \neq 0$ define

$$\operatorname{disc}(Q) := \det(T_B)(K^*)^2 \quad \in K^*/(K^*)^2$$

Otherwise $\mathrm{disc}(Q) = 0$. This is well defined due to the previous theorem.

Definition – Orthogonal complement
Suppose (Q, V) is a finite dimensional quadratic module over field K. If $x, y \in V$ and $x \cdot y = 0$ then we say x, y are orthogonal. For $U \subseteq V$,

$$U^{\perp} := \{x \in V \mid \forall h \in U, x \cdot h = 0\}$$

This is a subspace. If $W \subseteq V$ then we say W, U are orthogonal if $W \subseteq U^{\perp}$. This is if and only if $U \subseteq W^{\perp}$. Define $\mathrm{rad}U = U \cap U^{\perp}$.

Proposition – Degenerate Q
Suppose (Q, V) is a quadratic module over field K with finite dimension. We say Q is degenerate over V when $\mathrm{disc}(Q) = 0$. This holds if and only if $\mathrm{rad}(V) \neq \{0\}$.

Proof. Let B be a basis of V.

$$\begin{aligned}
\mathrm{disc}(Q) = 0 &\Leftrightarrow \det(T_B) = 0 \\
&\Leftrightarrow \exists x \in V \setminus \{0\}, T_B x_B = 0 \\
&\Leftrightarrow \exists x \in V \setminus \{0\}, \forall y \in V, y_B^T T_B x_B = 0 \\
&\Leftrightarrow \exists x \in V \setminus \{0\}, \forall y \in V, x \cdot y = 0 \\
&\Leftrightarrow V^{\perp} \neq \{0\}
\end{aligned}$$

□

Definition – Dual Space
Suppose (Q, V) is a finite dimensional quadratic module over field K. Let U be a subspace of V. Define

$$U^{\diamond} := \{u^{\diamond} : U \to K \mid u^{\diamond} \text{ linear}\}$$

For any linear $T : U \to W$ define

$$T^{\diamond} : U^{\diamond} \to W^{\diamond} := \star \circ T$$

Define $q_U : V \to U^{\diamond}$ by $x \to (x \cdot \star)$. Check that q_U is linear and has kernel $U^{\perp}$. Check that $q_U =\downarrow_U^V q_V$ is the canonical surjection from $V^{\diamond}$ to $U^{\diamond}$. Thus by the previous proposition Q is non-degenerate over V if and only if q_V is injective if and only if q_V is an isomorphism. (The dimension of $V^{\diamond}$ is equal to that of V.)

Definition – Orthogonal direct sum
Suppose (Q, V) is a quadratic module over field K with finite dimension. Suppose $\{U_i\}_{i \leq m}$ be subspaces of V, pairwise orthogonal and whose direct sum is V. Then define Q_i as Q restricted to U_i. If

$x = \sum_{i \le m} x_i u_i \in V$ then

$$Q(x) = \left(\sum_{i \le m} x_i u_i \right) \cdot \left(\sum_{j \le m} x_j u_j \right) = \sum_{i \le m} x_i^2 (u_i \cdot u_i) = \sum_{i \le m} Q_i(x_i)$$

Conversely, suppose $\{(Q_i, U_i)\}_{i \le m}$ are finite dimensional quadratic modules over K. Then there exists a unique quadratic form $Q : \bigoplus_{i \le m} \to K$ that agree with each Q_i upon restriction. It is given by the related bilinear map

$$(\star \cdot \star) : \left(\sum_{i \le m} x_i u_i, \sum_{i \le m} y_i u_i \right) \mapsto \sum_{i \le m} x_i y_i \mathbb{Q}_i(u_i)$$

We write $\widehat{\bigoplus} U_i$ to mean the orthogonal direct sum of U_i.

Definition

If a space is the sum of

Proposition

If (V, Q) is a non-degenerate finite dimensional quadratic module over a field K. Then

1. All metric functions from (V, Q) are injective.
2. For any subspace U,
$$U^{\perp\perp} = U, \quad \dim U + \dim U^{\perp} = \dim V$$
3. For any subsace U, U non-degenerate if and only if $U^{\perp}$ is non-degenerate.
4. If a subspace U is non-degenerate then $V = U \widehat{\oplus} U^{\perp}$.
5. If $V = U \oplus U^{\perp}$ then U and $U^{\perp}$ are orthogonal and non-degenerate.

Proof.

1. Let f be a metric function out of V. Then let $x \in \ker(f)$.
$$\forall y \in V, x \cdot y = f(x) \cdot f(y) = 0$$
Hence $x = 0$ as V is non-degenerate.
2. Let $U \le V$. Clearly $U \subseteq U^{\perp\perp}$. Suffices to show that they have the same dimension. We construct an exact sequence
$$0 \longrightarrow U^{\perp} \xrightarrow{\subseteq} V \xrightarrow{p_U} U^{\diamond} \longrightarrow 0$$

Note that $q_U =\downarrow_U^V q_V$ is surjective because V is non-degenerate tells us q_V is bijective.

Hence by rank-nullity we have

$$\dim V = \dim U^\perp + \dim U^\diamond = \dim U^\perp + \dim U$$

Applying the above result to $U^\perp$ gives us

$$\dim V = \dim U^{\perp\perp} \dim U^\perp$$

Hence $\dim U = \dim U^{\perp\perp}$ and $U = U^{\perp\perp}$.

3. For any subsace U, U non-degenerate if and only if $U \cap U^\perp = \mathrm{rad}(U) = \{0\}$ if and only if $U^\perp \cap U^{\perp\perp} = \mathrm{rad}(U^\perp) = \{0\}$ if and only if $\mathbb{U}^\perp$ is non-degenerate.
4. If a subspace U is non-degenerate then as remarked $U \cap U^\perp$ and $\dim U + \dim U^\perp = V$ hence $V = U \widehat{\oplus} U^\perp$.
5. If $V = U \oplus U^\perp$ then $U \cap U^\perp$ thus U and $U^\perp$ are non-degenerate. Naturally they are orthogonal.

$\square$