1

General theory of quadratic forms

Throughout this book, rings R are commutative and contain the unity 1, and modules M over R are finitely generated with $1m = m$ for $m \in M$.

In this chapter, we give some basics about quadratic forms which include the so-called Witt theorem, Clifford algebra and quaternion algebra. Besides them, the theory of quadratic forms over finite fields is outlined. It is useful for readers to get used to how to deal with quadratic forms and also to their applications.

1.1 Symmetric bilinear forms

Let M be a module over a ring R and b a mapping from $M \times M$ to R satisfying the conditions

(1) $b(x, y) = b(y, x)$ for $x, y \in M$
(2) $b(rx + sy, z) = rb(x, z) + sb(y, z)$ for $r, s \in R, \quad x, y, z \in M$.

We call b a *symmetric bilinear form* and the pair (M, b) or simply M a *symmetric bilinear module* over R. When R is a field, we often use "space" instead of "module".

If M is free and $\{v_i\}_{i=1}^n$ is a basis of M, then we write

$$M \cong \langle A \rangle$$

for $A = (b(v_i, v_j))$. For another basis $\{u_i\}_{i=1}^n$, there is a matrix $T = (t_{ij})$ such that $(u_1, \cdots, u_n) = (v_1, \cdots, v_n)T$, $t_{ij} \in R, \det T \in R^\times$, and

$(b(u_i,u_j)) = (b(\sum_k t_{ki}v_k, \sum_h t_{hj}v_h)) = (\sum_{k,h} t_{ki}b(v_k,v_h)t_{hj}) = {}^tTAT = A[T]$ holds and so we have $M \cong \langle A \rangle \cong \langle A[T] \rangle$. Thus $\det A(R^\times)^2$ is independent of the choice of a basis and is uniquely determined by M, and we denote it by

$$\mathrm{d}\,M$$

and call it the *discriminant*. (It is defined only for free modules.)

For a non-zero symmetric bilinear space U over a field F, we call U *regular* if $\mathrm{d}\,U \neq 0$, and it is easy to see that

U is regular

$\Leftrightarrow$ if $b(x,U) = 0$, then $x = 0$

$\Leftrightarrow$ $\mathrm{Hom}_F(U,F) = \{y \mapsto b(x,y) \mid x \in U\}$

$\Leftrightarrow$ for a basis $\{u_i\}$ of U, there is a subset $\{v_i\}$ of U such that $b(u_i,v_j) = \delta_{i,j}$ (Kronecker's delta).

(We use "regular" for spaces only!)

For a subset S of a symmetric bilinear module M over a ring R, we put

$$S^\perp = \{x \in M \mid b(x,s) = 0 \quad \text{for} \quad s \in S\}.$$

For symmetric bilinear modules $M, M_1, \cdots, M_m$ over a ring R such that $M = M_1 \oplus \cdots \oplus M_m$, $b(M_i, M_j) = 0$ if $i \neq j$, we call M the *orthogonal sum* of $M_1, \cdots, M_m$ and write

$$M = M_1 \perp \cdots \perp M_m.$$

When M has a basis $\{v_i\}$ such that $M = Rv_1 \perp \cdots \perp Rv_n$, $\{v_i\}$ is called an *orthogonal basis* of M. By the above notation, $M \cong \perp_i \langle a_i \rangle$ with $a_i = b(v_i, v_i)$.

For a symmetric bilinear space $U = U_1 \perp \cdots \perp U_m$ over a field F, $\mathrm{d}\,U = \mathrm{d}\,U_1 \cdots \mathrm{d}\,U_m$ is clear and so U is regular if and only if every U_i is regular.

Proposition 1.1.1. *Let U be a symmetric bilinear space over a field F and V a subspace of U. If V is regular, then $U = V \perp V^\perp$ holds.*

Proof. Since V is regular, we have $V \cap V^\perp = \{x \in V \mid b(x,V) = 0\} = \{0\}$ and every linear mapping $f \in \mathrm{Hom}_F(V,F)$ is given by $x \mapsto b(x,y)$ for $y \in V$. For $u \in U$, $x \mapsto b(x,u)$ is a linear mapping from V to F. Therefore, there is an element $y \in V$ such that $b(x,u) = b(x,y)$ for $x \in V$, which implies $u - y \in V^\perp$. This means $U = V + V^\perp$ and then $U = V \oplus V^\perp = V \perp V^\perp$. □

Proposition 1.1.2. *Let U be a symmetric bilinear space over a field F and V a subspace of U. Then $V \cap U^{\perp} = \{0\}$ if and only if $\mathrm{Hom}_F(V, F) = \{x \mapsto b(x, y) \mid y \in U\}$, and then $\dim V^{\perp} = \dim U - \dim V$.*

Proof. Suppose $V \cap U^{\perp} = \{0\}$. Take a subspace $W(\supset V)$ such that $U = W \oplus U^{\perp}$. If $w \in W$ satisfies $b(w, W) = \{0\}$, then $b(w, U) = \{0\}$ and hence $w \in U^{\perp} \cap W = \{0\}$. Thus W is regular, and for $f \in \mathrm{Hom}_F(V, F)$ we extend it to $\mathrm{Hom}_F(W, F)$ by $f(W_0) = 0$ with $W = W_0 \oplus V$. Because of regularity of W, there is an element y in W so that $f(x) = b(x, y)$ for x in W and especially in V. If, conversely $V \cap U^{\perp} \neq \{0\}$, then we take a basis $\{v_i\}$ of V such that $v_1 \in V \cap U^{\perp}$. A linear mapping f defined by $f(v_1) = 1, f(v_i) = 0$ $(i \geq 2)$ is not of form $f(x) = b(x, y)$, since $b(v_1, U) = 0$. Thus the former part has been proved.

Suppose $V \cap U^{\perp} = \{0\}$ and for a basis $\{v_i\}_{i=1}^m$ of V we can take a subset $\{u_i\}_{i=1}^m$ of U such that $b(v_i, u_j) = \delta_{ij}$ for $1 \leq i, j \leq m$. Then $\{u_i\}_{i=1}^m$ is linearly independent. We define a linear mapping

$$f : U \to U_0 := \oplus_{i=1}^m F u_i$$

by $f(u) = \sum_i b(u, v_i) u_i$. Then f is surjective by virtue of $f(u_i) = u_i$ and $\ker f = V^{\perp}$ is clear. Thus we have $\dim U - \dim V^{\perp} = \dim U_0 = \dim V$. □

The proof shows

Corollary 1.1.1. *In Proposition 1.1.2, $V \cap U^{\perp} = \{0\}$ if and only if V is contained in some regular subspace of U.*

1.2 Quadratic forms

Let M be a module over a ring R and q a mapping from M to R which satisfies the conditions

(i) $q(ax) = a^2 q(x)$ for $a \in R$, $x \in M$,
(ii) $b(x, y) := q(x + y) - q(x) - q(y)$ is a symmetric bilinear form.

We call the pair (M, q) or simply M a *quadratic module* over R, q a *quadratic form* and b the *associated symmetric bilinear form.* When R is a field, we often use "space" instead of "module".

Putting $x = y$, we have

$$b(x, x) = 2q(x) \quad \text{for } x \in M.$$

If 2 is in $R^{\times}$, then we can associate a symmetric bilinear form $\frac{1}{2} b(x, y) = B(x, y)$. Then $B(x, x) = q(x)$ and conversely for a given symmetric bilinear form $B(x, y), q(x) := B(x, x)$ is a quadratic form and $q(x+y) - q(x) - q(y) =$

$2B(x,y)$. Thus "quadratic module" and "symmetric bilinear module" are equivalent if $2 \in R^\times$.

In this section and the next we will associate $b(x,y)$ with M, but after 1.4, the fields are of characteristic 0, and we will prefer the bilinear form B instead of b. The difference between them is minor and the choice depends on the individual's taste.

Considering a quadratic module M as a symmetric bilinear module with $b(x,y)$ ($B(x,y)$ after section 1.4), the notations and terminology $\perp, M \cong \langle A \rangle, \mathrm{d}\, M$ and regular remain meaningful.

If 2 is a unit, then $\perp$ and "regular" are independent of the choice of $B(x,y)$ or $b(x,y)$. But $\mathrm{d}\, M$ differs by 2^n with $n = \operatorname{rank} M$, since $M \cong \langle A \rangle$ or $\langle 2^{-1}A \rangle$ for $A = (b(x,y))$, according to $b(x,y)$ or $B(x,y)$, respectively.

For a quadratic module M, we put

$$\operatorname{Rad} M := \{x \in M^\perp \mid q(x) = 0\}.$$

This is a submodule of M and if $2 \in R^\times$, then $\operatorname{Rad} M = M^\perp$.

Theorem 1.2.1. *Let U be a quadratic space over a field F. If $\operatorname{ch} F \neq 2$, then we have*

$$U = U_1 \perp \cdots \perp U_r \perp U^\perp$$

where the U_i's are regular and 1-dimensional.

If $\operatorname{ch} F = 2$, then we have

$$U = V_1 \perp \cdots \perp V_s \perp W_1 \perp \cdots \perp W_t \perp \operatorname{Rad} U,$$

where the V_i's are regular and 2-dimensional, the W_i's are 1-dimensional and $0 \le t \le [F^\times : (F^\times)^2]$ and

$$U^\perp = W_1 \perp \cdots \perp W_t \perp \operatorname{Rad} U.$$

Proof. Suppose $\operatorname{ch} F \neq 2$. If there is an element $u_1 \in U$ such that $q(u_1) \neq 0$, then $b(u_1,u_1) = 2q(u_1) \neq 0$ and so $U_1 = Fu_1$ is regular. Proposition 1.1.1 implies $U = U_1 \perp U_1^\perp$. Repeating this, we have $U = U_1 \perp \cdots \perp U_r \perp U_{r+1}$ where $U_1, \cdots, U_r$ are regular and 1-dimensional and $q(x) = 0$ for all $x \in U_{r+1}$, which implies $b(U_{r+1}, U_{r+1}) = 0$ and hence $U_{r+1} \subset U^\perp$. Decomposing $x \in U^\perp$ along the above orthogonal decomposition of U, $U^\perp \subset U_{r+1}$ is easy to see.

Next, suppose $\operatorname{ch} F = 2$. If $x, y \in U$ satisfies $b(x,y) \neq 0$, then $V_1 = F[x,y]$ is regular with $\mathrm{d}\, V_1 = -b(x,y)^2$, noting $b(x,x) = b(y,y) = 0$. Hence we have $U = V_1 \perp V_1^\perp$. Repeating this, we have $U = V_1 \perp \cdots \perp V_s \perp U_0$

where $V_1, \cdots, V_s$ are regular and 2-dimensional and $b(U_0, U_0) = 0$. As above, $U_0 = U^\perp$ holds. We take a direct sum decomposition

$$U^\perp = W_1 \oplus \cdots \oplus W_t \oplus \operatorname{Rad} U$$

where the W_i's are 1-dimensional. Since $b(U^\perp, U^\perp) = 0$, $U^\perp = W_1 \perp \cdots \perp W_t \perp \operatorname{Rad} U$ holds. Put $W_i = Fw_i$. Since $w_i \in U^\perp$ but $w_i \notin \operatorname{Rad} U$, $q(w_i) \neq 0$ holds. If $q(w_i)(F^\times)^2 = q(w_j)(F^\times)^2$ for $i \neq j$, then $q(w_i) = a^2 q(w_j)$ for $a \in F^\times$ holds and this means $q(w_i - aw_j) = 0$. Hence we have a contradiction $w_i - aw_j \in \operatorname{Rad} U$. Thus the $q(w_i)$'s give distinct representatives of $F^\times/(F^\times)^2$. □

Let M, N be quadratic modules over a ring R. If a linear mapping σ from M to N satisfies that

$$\sigma \text{ is injective and}$$
$$q(\sigma(x)) = q(x) \text{ for } x \in M,$$

we call σ an *isometry* from M to N and say that M is *represented* by N and write

$$\sigma : M \hookrightarrow N.$$

When $\sigma(M) = N$, we write

$$\sigma : M \cong N,$$

and say that M and N are *isometric*. The group of all isometries from M to itself is denoted by

$$O(M).$$

Suppose that R is a subring of a field F and generates F. For an R-submodule M of a quadratic space V over F satisfying $FM = V$, we denote by

$$O^+(M) := \{\sigma \in O(M) \mid \det \sigma = 1 \ \}$$

where $\det \sigma$ is defined by $\det T$ for a matrix T with

$$(\sigma(v_1), \cdots, \sigma(v_n)) = (v_1, \cdots, v_n)T$$

for a basis $\{v_i\}$ of V.

For an isometry σ from M to N, it is easy to see

$$b(\sigma(x), \sigma(y)) = b(x, y)$$

for $x, y \in M$.

Conversely, an injective linear mapping σ from M to N which satisfies $b(\sigma(x), \sigma(y)) = b(x, y)$ is an isometry if $2 \in R^\times$, since $q(x) = 2^{-1}b(x, x)$.

For quadratic modules M, N and a linear mapping σ from M to N with $q(\sigma(x)) = q(x)$ for $x \in M$, $\sigma(x) = 0$ yields $x \in M^\perp$ since $b(x, M) = b(\sigma(x), \sigma(M)) = \{0\}$. If, moreover M is a regular quadratic space, then σ is an isometry.

Now we give an important example of isometry.

Proposition 1.2.1. *Let M be a quadratic module over a ring R. For an element x in M with $q(x) \in R^\times$, we put*

$$\tau_x(y) := y - b(x,y)q(x)^{-1}x \quad \textit{for } y \in M.$$

Then τ_x is an isometry from M to M and satisfies

$$\tau_x(x) = -x,\ \tau_x(y) = y \ \textit{for } y \in x^\perp, \ \textit{and } \tau_x^2 = \mathrm{id}\,.$$

Proof. $\tau_x(x) = -x$ and $\tau_x(y) = y$ for $y \in x^\perp$ are easy.

$$\tau_x^2(y) = \tau_x(y) - b(x,y)q(x)^{-1}\tau_x(x) = y$$

implies $\tau_x^2 = \mathrm{id}$ and the bijectivity of τ_x. Finally

$$q(\tau_x(y)) = q(y) + b(x,y)^2q(x)^{-2}q(x) - b(x,y)q(x)^{-1}b(x,y) = q(y)$$

implies that τ_x is an isometry. □

τ_x is called a *symmetry*. If R is a field, then the determinant of a transformation τ_x is -1.

The following theorem of Witt type is due to Kneser.

Theorem 1.2.2. *Let $\tilde{R} \supset R$ be rings and P a proper ideal of R satisfying $R = R^\times \cup P$ and $R^\times \cap P = \emptyset$. Let L, M, N, H be R-submodules of a quadratic module U over $\tilde{R}$ such that they are finitely generated over R, M, N are free R-modules and $L \supset M, N, H$. Suppose that*

(1) $$q(H) \subset R,\ b(L,H) \subset R,$$

(2a) $$\mathrm{Hom}_R(M,R) = \{x \mapsto b(x,y) \mid y \in H\},$$

(2b) $$\mathrm{Hom}_R(N,R) = \{x \mapsto b(x,y) \mid y \in H\},$$

and $\sigma : M \cong N$ is an isometry such that

(3) $$\sigma(x) \equiv x \bmod H$$

for $x \in M$.

Then σ can be extended to an element of $O(L)$ which satisfies

(4) $$\sigma = \mathrm{id} \quad \textit{on } H^\perp$$

and (3) for every x in L.

Proof. For z in H with $q(z) \in R^\times$, the symmetry

$$\tau_z(x) = x - b(x,z)q(z)^{-1}z$$

satisfies three properties: $\tau_z(L) = L$ because of the property (1), secondly (3) for $x \in L$ and (4) by definition of τ_z. For a submodule J of H, we denote by $S(J)$ a subgroup of $O(L)$ generated by τ_x ($x \in J, q(x) \in R^\times$), and then every element in $S(J)$ satisfies the condition (3) for $x \in L$ and the condition (4). Note that the quotient ring $\bar{R} := R/P$ is a field. First, we will prove a preparatory assertion:

Assertion 1. *We assume, moreover*

$$\text{(5)} \qquad \sharp\bar{R} > 2 \Rightarrow q(x) \in R^\times \ \textit{ for some } x \in H,$$
$$\text{(6)} \qquad \sharp\bar{R} = 2 \Rightarrow q(x) \in R^\times \ \textit{ and } \ b(x,H) \subset P \ \textit{ for some } x \in H.$$

Then σ is a restriction of an element of $S(H)$.

We prove this by induction of the rank of M.

Suppose rank $M = 1$ and $M = Rm, N = Rn, n = \sigma(m)$, and put, by (3)

$$\text{(7)} \qquad h = n - m \in H.$$

Then $q(h) = 2q(n) - b(n,m) = 2q(m) - b(n,m)$ and (7), (1) imply

$$\text{(8)} \qquad q(h) = b(n,h) = -b(m,h) \in R.$$

If $q(h) \in R^\times$, then $\tau_h(m) = m - b(h,m)q(h)^{-1}h = n$ by (8), (7), and we complete the proof in the case of rank $M = 1$.

Suppose

$$\text{(9)} \qquad q(h) \in P.$$

First, we show that if there is an element f in H satisfying

$$\text{(10)} \qquad q(f), b(f,m), b(f,n) \in R^\times,$$

then the proof in the case of rank $M = 1$ is completed.

Supposing the existence of such f, we put $g := n - \tau_f(m)$; then (7), (10) imply

$$\text{(11)} \qquad g = h + b(f,m)q(f)^{-1}f \in H,$$

and

$$\begin{aligned} q(g) &= q(h) + b(f,m)^2 q(f)^{-2} q(f) + b(f,m)q(f)^{-1}b(h,f) \\ \text{(12)} \qquad &= q(h) + b(f,m)b(f,n)q(f)^{-1} \in R^\times \end{aligned}$$

by (9), (10).

Moreover, we have

$$\begin{aligned} \tau_g(n) &= n - b(n,g)q(g)^{-1}g \\ &= n - (b(n,h) + b(f,m)q(f)^{-1}b(n,f))q(g)^{-1}g \quad \text{by (11)} \\ &= n - (b(n,h) + q(g) - q(h))q(g)^{-1}g \quad \text{by (12)} \\ &= n - g \quad \text{by (8)} \\ &= \tau_f(m) \quad \text{by definition of } \ g. \end{aligned}$$

Thus σ is a restriction of $\tau_g \tau_f \in S(H)$.

It remains to show the existence of f.

We denote a vector space H/PH over $\bar{R}$ by $\bar{H}$ and an element of $\bar{H}, \bar{R}$ represented by $x \in H, y \in R$ by $\bar{x}, \bar{y}$, respectively. By virtue of (1), $\bar{H}$ becomes a quadratic space over $\bar{R}$ by $\bar{q}(\bar{x}) := \overline{q(x)}$ for $x \in H$. This is well defined by (1). Put

$$\bar{m}^{\perp} = \{\bar{x} \in \bar{H} \mid \bar{b}(\bar{x}, \bar{m}) = 0\},$$
$$\bar{n}^{\perp} = \{\bar{x} \in \bar{H} \mid \bar{b}(\bar{x}, \bar{n}) = 0\}.$$

The condition (10) is equivalent to $\bar{q}(\bar{H} \setminus (\bar{m}^{\perp} \cup \bar{n}^{\perp})) \neq 0$. From (8), (9) follows $\bar{m}^{\perp} \cap \bar{n}^{\perp} \ni \bar{h}$, and by virtue of (2) there exist $h_m, h_n \in H$ such that $b(m, h_m) = 1$ and $b(n, h_n) = 1$. Thus $\dim \bar{m}^{\perp} = \dim \bar{n}^{\perp} = \dim \bar{H} - 1$.

Suppose

$$\bar{q}(\bar{H} \setminus (\bar{m}^{\perp} \cup \bar{n}^{\perp})) = 0. \tag{13}$$

For $\bar{x} \in \bar{m}^{\perp} \cap \bar{n}^{\perp}$ and $\bar{y} \in \bar{H} \setminus (\bar{m}^{\perp} \cup \bar{n}^{\perp})$, we have, by (13)

$$\bar{q}(a\bar{x} + \bar{y}) = a^2 \bar{q}(\bar{x}) + a\bar{b}(\bar{x}, \bar{y}) + \bar{q}(\bar{y}) = 0 \quad \text{for } a \in \bar{R}. \tag{14}$$

If $\sharp \bar{R} > 2$, then (14) implies

$$\bar{q}(\bar{x}) = \bar{b}(\bar{x}, \bar{y}) = \bar{q}(\bar{y}) = 0. \tag{15}$$

Note that $\bar{h} \in \bar{m}^{\perp} \cap \bar{n}^{\perp}$, and the vectors which are not in the union of two hyperplanes $\bar{m}^{\perp}$, $\bar{n}^{\perp}$ span the whole space if the number of elements of the coefficient field is greater than 2. Putting $\bar{x} := \bar{h}$ in (15), we have $\bar{b}(\bar{h}, \bar{H}) = 0$ and then $\bar{m}^{\perp} = \bar{n}^{\perp}$ by (7). From this with (15) it follows that $\bar{q}(\bar{m}^{\perp}) = \bar{q}(\bar{H} \setminus \bar{m}^{\perp}) = 0$ and so $\bar{q}(\bar{H}) = 0$. This contradicts the assumption (5).

Suppose $\sharp \bar{R} = 2$ and put

$$H_1 := \bar{m}^{\perp} \cap \bar{n}^{\perp} \cap \bar{H}^{\perp} \text{ and } H_2 := (\bar{H} \setminus (\bar{m}^{\perp} \cup \bar{n}^{\perp})) \cap \bar{H}^{\perp};$$

then (14) implies $\bar{q}(H_1) = \bar{q}(H_2) = 0$, noting $\bar{b}(\bar{H}_1, \bar{H}_2) = 0$. For $\bar{x} \in \bar{H}$, we have

$$\begin{aligned} \bar{x} \in \bar{m}^{\perp} \cap \bar{H}^{\perp} &\Leftrightarrow \bar{b}(\bar{x}, \bar{m}) = 0, \bar{b}(\bar{x}, \bar{H}) = 0 \\ &\Leftrightarrow \bar{b}(\bar{x}, \bar{n}) = 0, \bar{b}(\bar{x}, \bar{H}) = 0 \text{ by (7)} \\ &\Leftrightarrow \bar{x} \in \bar{n}^{\perp} \cap \bar{H}^{\perp}, \end{aligned}$$

and hence $H_1 = \bar{m}^\perp \cap \bar{H}^\perp = \bar{n}^\perp \cap \bar{H}^\perp$, and then

$$H_2 = (\bar{H} \setminus \bar{m}^\perp) \cap (\bar{H} \setminus \bar{n}^\perp) \cap \bar{H}^\perp = \bar{H}^\perp \setminus H_1.$$

This means $\bar{q}(\bar{H}^\perp) = \bar{q}(H_1) \cup \bar{q}(H_2) = 0$ which contradicts (6). Thus we have completed the proof in the case of rank $M = 1$.

Suppose $r = \operatorname{rank} M > 1$. Let $\{m_1, \cdots, m_r\}$ be a basis of M and we take $h_i \in H$ such that $b(m_i, h_j) = \delta_{ij}$ by virtue of the assumption (2). It is easy to see

$$H = \oplus_i Rh_i \oplus K, K := M^\perp \cap H. \tag{16}$$

From the assumption (5), (6) there is an element $\bar{h} \in \bar{H}$ or $\bar{H}^\perp$ such that $\bar{q}(\bar{h}) \neq 0$ according to $\sharp\bar{R} > 2$ or $\sharp\bar{R} = 2$. Changing a basis if necessary, we may suppose

$$\bar{h} \in \bar{R}\bar{h}_r + \bar{K}. \tag{17}$$

Applying the inductive assumption to $M_0 := \oplus_{i=1}^{r-1} Rm_i$, there is $\tau \in S(H)$ such that $\tau = \sigma$ on M_0. Taking $\tau^{-1}(N), \tau^{-1}\sigma$ instead of N, σ, they satisfy conditions (2), (3), because of $\tau(H) = H$ and a remark at the beginning of the proof. Hence we may suppose

$$\sigma(m_i) = m_i \ \text{ for } 1 \le i \le r-1, \tag{18}$$

taking $\tau^{-1}\sigma$ as σ again. Then, for $x \in M$ and $1 \le i \le r-1$, we have $b(\sigma(x) - x, m_i) = b(\sigma(x), m_i) - b(x, m_i) = 0$ by (18) and hence by (3), (16)

$$\sigma(x) - x \in H \cap M_0^\perp = Rh_r + K \text{ for } x \in M. \tag{19}$$

We show that conditions (1), $\cdots$, (6) are satisfied for $M_1 = Rm_r, H_0 = Rh_r + K$ instead of M, H respectively. (1) follows from $H_0 \subset H$. By definition of h_r, we have $b(m_r, h_r) = 1$ and so the condition (2a) for M_1. Since $\{m_1, \cdots, m_{r-1}, \sigma(m_r)\}$ is a basis of N, there is an element $h' \in H$ such that $b(m_i, h') = 0$ for $1 \le i \le r-1$ and $b(\sigma(m_r), h') = 1$ from the original assumption (2b). Hence h' is in $H \cap M_0^\perp = Rh_r + K = H_0$ and so (2b) holds for $\sigma(M_1)$. The condition (3) follows from (19), and (5), (6) do from (17). Hence, by the inductive assumption, there exists $\tau \in S(H_0)$ such that $\tau(m_r) = \sigma(m_r)$, moreover $m_1, \cdots, m_{r-1} \in H_0^\perp$ implies $\tau(m_i) = m_i = \sigma(m_i)$ for $1 \le i \le r-1$. Thus we have $\sigma = \tau$ on M and $\tau \in S(H_0) \subset S(H)$ completes the proof of the assertion.

Proof of Theorem 1.2.2. Let V be a binary quadratic module over $\tilde{R}$ with basis $\{v_1, v_2\}$ such that $q(a_1v_1 + a_2v_2) = a_1a_2$ for $a_i \in \tilde{R}$. Put

$$U' = U \perp V, L' = L \perp (Rv_1 + Rv_2), M' = M \perp Rv_1,$$
$$N' = N \perp Rv_1, H' = H \perp R(v_1 + v_2), \sigma' = \sigma \perp (\text{id on } Rv_1).$$

Then $q(v_1 + v_2) = 1$ and moreover $b(v_1 + v_2, H') \subset P$ if $\sharp\bar{R} = 2$. With M', N', H', σ' instead of M, N, H, σ, conditions (1), $\cdots$, (6) are satisfied and hence there exists $\tau \in S(H')$ such that $\tau = \sigma'$ on M'. Now $b(v_1 + v_2, v_1 - v_2) = 0$ implies $v_1 - v_2 \in H'^{\perp}$ and so $\tau(v_1 - v_2) = v_1 - v_2$, hence $\tau(v_i) = v_i$ for $i = 1, 2$ by $\tau(v_1) = \sigma'(v_1) = v_1$. Also $L = L' \cap \{v_1, v_2\}^{\perp}$ and $\tau(L') = L'$ yield $\tau \in O(L)$. Thus we have completed the proof. □

We note that the conditions (1) and (3) are absorbed in definitions in the case of $\tilde{R} = R$ and $U = L = H$ and that this case is also quite useful.

Corollary 1.2.1. *Let U be a quadratic space over a field F, and V, W subspaces satisfying $V \cap U^{\perp} = W \cap U^{\perp} = \{0\}$. Then every isometry $\sigma : V \cong W$ is extended to an isometry of U, and if $\operatorname{ch} F \neq 2$ and $q(U) \neq 0$ then it is a product of symmetries.*

Proof. In the theorem, we put $\tilde{R} = R := F$, $P := \{0\}$, $L = H := U$, $M := V$, $N := W$. Conditions (1), (3) are obviously satisfied and (2) is done by Proposition 1.1.2. The latter part follows from Assertion 1 with the condition (5). □

Corollary 1.2.2. *Let U be a regular quadratic space over a field F with $\operatorname{ch} F \neq 2$. Then $O(U)$ is generated by symmetries.*

Proof. In the previous corollary, we have only to put $U = V = W$. □

Corollary 1.2.3. *Let $V = V_1 \perp V_2$, $W = W_1 \perp W_2$ be quadratic spaces over a field F and suppose that $V \hookrightarrow W$, $V_1 \cong W_1$ and V_1 is regular. Then V_2 is represented by W_2. If, moreover $V \cong W$, then $V_2 \cong W_2$.*

Proof. Since V is represented by W, we may suppose that V is a subspace of W, and let σ be an isometry from V_1 to W_1. We can extend it to σ_1 in $O(W)$ by Corollary 1.2.1, since V_1 is regular. Then we have $\sigma_1(V_2) \subset \sigma_1(V_1^{\perp}) \subset \sigma_1(V_1)^{\perp} = W_1^{\perp} = W_2$. Hence V_2 is represented by W_2. If $V \cong W$, then we have $\dim V_2 = \dim W_2$ and hence $\sigma_1(V_2) = W_2$. □

Other applications are given later.

Let U be a quadratic space over a field F. For a non-zero vector x, we call x *anisotropic* if $q(x) \neq 0$, *isotropic* if $q(x) = 0$, respectively. If U contains an isotropic vector, then U is called *isotropic*, otherwise *anisotropic*, that is if $q(x) = 0$ for $x \in U$ implies $x = 0$, then U is anisotropic. If $q(U) = 0$, then U is called *totally isotropic*.