1 Classification of Hermitian Forms

A vector $v \in V$ is said to be **primitive** if $v \notin V\mathfrak{r}$. This is equivalent to saying that v belongs to a basis of V. We say that h is **isotropic** if there is a primitive vector $v \in V$ such that $h(v,v) = 0$.

Lemma 1.1. *Suppose h is isotropic. Then, given any $r \in R$ there is a primitive vector v satisfying $h(v,v) = r$.*

Proof. By assumption, h is isotropic so there is a primitive vector $u \in V$ such that $h(u,u) = 0$. Because h is assumed to be non-degenerate, there exists $w \in V$ such that $h(u,w) = d$. Set $s = r - h(w,w) \in R$ and $v = us + w$. Then

$$\begin{aligned} h(v,v) &= h(us+w, us+w) \\ &= sh(u,w) + sh(u,w) + sh(w,u) + h(w,w) \\ &= s(d+d^*) + h(w,w) \\ &= s + h(w,w) \\ &= r - h(w,w) + h(w,w) \\ &= r \end{aligned}$$

□

We assume for the remainder of the paper that the squaring map of the 1-group $1+\mathfrak{m}$ is an epimorphism and that $R/\mathfrak{m} = F_q$ is a field of finite order q and odd characteristic. Thus $[F_q^* : F_q^{*2}] = 2$. To see this, pick $r \in F_q^* \backslash F_q^{*2}$. Then the minimal polynomial of x is $t^2 - r^2 \in F_q^{*2}[t]$. A similar argument shows that $[R^* : R^{*2}] = 2$. We can now fix an element $\varepsilon \in R^* \backslash R^{*2}$. Since $R^{*2} \subseteq Q(A^*)$, we infer $Q(A^*) = R^*$ if Q is surjective and $Q(A^*) = R^{*2}$ otherwise.

Proposition 1.1. *The division ring $A/\mathfrak{r}$ is commutative. Moreover,*

(a) *If the involution that $*$ induces on $A/\mathfrak{r}$ is the identity then Q is not surjective and $A/\mathfrak{r} \cong F_q$.*

(b) *If the involution that $*$ induces on $A/\mathfrak{r}$ is not the identity then Q is surjective and $A/\mathfrak{r} \cong F_{q^q}$.*

Proof. We begin embedding $R/\mathfrak{m}$ in $A/\mathfrak{r}$ using the mapping $x + \mathfrak{m} \mapsto x + \mathfrak{r}$ for $x \in R$. Thus $R/\mathfrak{m}$ can be viewed as a subfield of $A/\mathfrak{r}$. Now let $\circ$ be the involution that $*$ induces on $A/\mathfrak{r}(a + \mathfrak{r} \mapsto a^* + \mathfrak{r})$ and let $k = \{a \in A/\mathfrak{r} :$

$a^\circ = a\}$ be the set of all elements of $A/\mathfrak{r}$ that are fixed by $\circ$. Then $R/\mathfrak{m} \subseteq k$ (by definition, R is fixed under $*$). Conversely, assume that $a + \mathfrak{r} \in k$. Then $a - a^* \in \mathfrak{r}$, so

$$a = \frac{a + a^*}{2} + \frac{a - a*}{2} \in R + \mathfrak{r}$$

and $k \subseteq (R + \mathfrak{r})/\mathfrak{r} = R/\mathfrak{m}$. Thus $k = R/m$.

(a) In this case, $A/\mathfrak{r} = k = R/\mathfrak{m}$ and the norm map $(A/\mathfrak{r})^* \to (R/\mathfrak{m})^*$ (induced by Q) is the squaring map of F_q^*. This map is not surjective, so the norm map Q is not surjective.

(b) In this case, we assume that $A/\mathfrak{r}$ properly contains k. Then for any $f \in A/\mathfrak{r}\backslash k$, the minimal polynomial of f is $(t - f)(t - f^\circ) = t^2 - (f + f^\circ)t + ff^\circ \in k[t]$.

Let $f, e \in A/\mathfrak{r}$. The goal is to show that f and e commute. Let $f_1 = f - (f + f^\circ)/2$ and $e_1 = e - (e + e^\circ)/2$. Since $(f + f^\circ)/2, (e + e^\circ)/2 \in k$ (which is a field), it is sufficient to show that f_1 and e_1 commute. Note that $f_1^\circ = -f_1$ and $e_1^\circ = -e_1$. Then

$$(e_1 f_1 + f_1 e_1)^\circ = f_1^\circ e_1^\circ + e_1^\circ f_1^\circ = f_1 e_1 + e_1 f_1$$

and $e_1 f_1 + f_1 e_1 \in k$. Thus $k\langle f_1, e_1\rangle$ is the k-span of $1, f_1, e_1, f_1 e_1$ and $k\langle f_1, e_1\rangle$ is a finite dimensional division algebra over k. Thus by Wedderburn's theorem, $k\langle f_1, e_1$ is a field, implying that f and e commute.

Thus $A/\mathfrak{r}$ is a field, algebraic over $k = R/\mathfrak{m}$, where every element of $A/\mathfrak{r}\backslash k$ has degree 2 over k. Since every algebraic extension of k is separable, the primitive element theorem implies that $[A/\mathfrak{r} : k] = 2$.

We now want to show that the norm map $\hat{Q} : (A/\mathfrak{r})^* \to k^*$ induced by $*$ is surjective. Because $k \subseteq A/\mathfrak{r}$, if $r \in k^2$, then there exists $s \in k$ with s fixed under $*$ and $s^2 = r$. Thus $\hat{Q}(s) = s^2 = r$. Now pick $x \in k\backslash k^2$. Then $\sqrt{x} \notin k$.

Consider two cases:

Case 1: Assume $-x \notin k^2$. Then $A/\mathfrak{r} \cong F_{q^2} = k(\sqrt{-x})$. Every element of $A/\mathfrak{r}$ can be written in the form $a + b\sqrt{-x}$ with $a, b \in k$ and

$$\hat{Q}(a + b\sqrt{-x}) = a^2 - b^2 \cdot -x = a^2 + b^2 x.$$

Then taking $s = \sqrt{-x}$ gives $\hat{Q}(s) = x$ and $x \in \hat{Q}\,(A/\mathfrak{r}))$.

Case 2: Assume that $-x \in k^2$. Because exactly half of the elements in k^* have square roots, there must exist some element $z \in k^*$ where $\sqrt{z} \in k^*$ and $\sqrt{z+1} \notin k^*$. Then $F_{q^2} = k(\sqrt{z+1})$. Now take $s = \sqrt{-x}\sqrt{z} + \sqrt{-x}\sqrt{z+1}$. Then

$$\hat{Q}(s) = (-xz) - (-x(z+1)) = (z+1)x - zx = x$$

and $\hat{Q}$ is surjective.

It follows that the norm map $(A/\mathfrak{r})^* \to (R/\mathfrak{m})^*$ induced by $\star$ is surjective, implying that the norm map $A^* \to R^*$ is as well since the squaring map of $1 + \mathfrak{m}$ is surjective. $\square$

Proposition 1.2. *Suppose $m \geq 2$. Then given any unit $r \in R$ there is a primitive vector $v \in V$ satisfying $h(v, v) = r$.*

Proof. Cosider two cases:

- h is isotropic. Then 1.1 applies.
- h is non-isotropic.

By lemma 2.2, there is an orthogonal basis $u_1, u_2, \dots u_m$ of V such that $h(u_i, u_i) \in R^\star$. Let $a = h(u_1, u_2) \in R^\star$ and $b = h(u_2, u_2) \in R^*$. if $t_1, t_2 \in R^*$, then $v = u_1t_1 + u_2t_2$ is primitive (because it is part of a basis), so

$$0 \neq h(v, v) = at_1^2 + bt_2^2.$$

Dividing by a and letting $c = b/a \in R^*$,

$$0 \neq t_1^2 + ct^2$$

implying that $-c$ is not a square in R^*. Let $S = R[t]/(t^2 + c)$ and $\delta = t + (t^2 + c) \in S$. Then $S = R[\delta], \delta^2 = -c$ and every element of S can be uniquely written in teh form $t_1 + t_2\delta$ with $t_1, t_2 \in R$. We have an involution $s \mapsto \hat{s}$ defined by $t_1 + t_2\delta \mapsto t_1 - t_2\delta$, whose corresponding norm map $J : S^* \to R^*$ given by $s \mapsto s\hat{s}$, or $t_1 + t_2\delta \mapsto t_1^2 + ct_2^2$.

We claim that S is local with maximal ideal $S\mathfrak{m}$. Let $t_1, t_2 \in R$, not both in $\mathfrak{m}$, and consider $J(t_1 + t_2\delta) = t_1^2 + ct_2^2$. If one of t_1, t_2 is in m, then $t_1^2 + ct_2^2 \in R^*$. To see this, assume that either t_1 or $t_2 \notin \mathfrak{m}$. Then if $t_1^2 + ct_2^2 \in \mathfrak{m}$, $t_1^2 = -ct_2^2 + m$ and $ct_2^2 = -t_1^2 - m$ for some $m \in \mathfrak{m}$. Since either t_1, t_2 is invertible, this implies that both $t_1, t_2 \in \mathfrak{m}$, a contradiction.

Thus $t_1^2 + ct_2^2 \in R^*$ and $t_1 + t_2\delta \in S^\star$. Now suppose that both $t_1, t_2 \in R^*$ but $t_1 + t_2\delta \notin S^\star$. Then $t_1^2 + ct_2^2 = f \in \mathfrak{m}$, and

$$-c = (t_1^{-1})^2(t_1^2 - f) = (t_2^{-1})^2 t_1^2(1 - (t_1^{-1})^2 f)$$

. By assumption (because A is a local ring), $1 - (t_1^{-1})^2 f \in R^{*2}$, implying that $-c \in R^{*2}$, a contradiction. Thus S is local with maximal ideal $S\mathfrak{m}$.

Thus $S/S\mathfrak{m}$ is a field. The imbedding $R/\mathfrak{m} \to S/S\mathfrak{m}$ allows us to view $S/S\mathfrak{m}$ as a vector space over $R/\mathfrak{m}$, with $\{1 + S\mathfrak{m}, \delta + \mathfrak{m}\}$ as a basis. Thus $S/S\mathfrak{m}$ is a quadratic extension of $R/\mathfrak{m}$. The involution of S induces the $R/\mathfrak{m}$-automorphism of $S/S\mathfrak{m}$ of orer 2 and the norm map J induces the norm map $(S/S\mathfrak{m})^* \to (R/\mathfrak{m})^*$.

Since $R/\mathfrak{m}$ is known to be F_q, this map is known to be surjective. We claim that J is surjective. Indeed, pick $e \in R^*$. Then by the surjectivity of the norm map, there is $s \in S$ and $f \in \mathfrak{m}$ such that

$$j(s) = e + f = e(1 + e^{-1}f).$$

Since $1 + e^{-1}f \in R^{*2}$ (by surjectivity of squaring map of $1 + \mathfrak{m}$), it follows that e is in the image of J, as claimed.

By the claim there are $t_1, t_2 inR$ with at least one in R^*, such that $t_1^2 + t_2^2 c = r/a$. Then $v = u_1 t_1 + u_2 t_2$ is primitive and

$$h(v, v) = at_1^2 + bt_2^2 = r.$$

This completes the proof. □

Theorem 1.1. *There is an orthogonal basis $v_1, v_2, \ldots, v_m$ of V satisfying*

$$\begin{aligned} h(v_1, v_1) = \cdots = h(v_{m-1}, v_{m-1}) = 1 \textit{ and} \\ h(v_m, v_m) = 1 \textit{ if } QA^* = R^* \\ h(v_m, v_m) \in \{1, \varepsilon\} \textit{ if } Q(A^*) = R^{*2} \end{aligned}$$

Proof. To prove this, we'll use induction on m. Assume that $m = 1$. By lemma 2.2, V has a basis $\{u_1\}$ such that $h(u_1, u_1) \in R^*$. If $Q(A^*) = R^*$, then $h(u_1, u_1) = aa^*$ for some $a \in A^*$. Let $v = u_1 a^{-1}$. Then

$$h(v, v) = a^{-1} * a^{-1} h(u, u) = 1.$$

If $Q(A^*) = R^{*2}$, then $h(u_1, u_1) = \varepsilon b$ for some $b \in R^{*2}$ (note that from earlier result, $[R^* : R^{*2}] = 2$). Then $b = r^2$ for some $r \in R^*$. Let $v = r^{-1}u_1$. Then

$$h(v, v) = (r^{-1})^2 h(u, u) = b^{-1}\varepsilon b = \varepsilon.$$

Now assume that $m > 1$ and that the hypothesis is true for $m-1$. By proposision 2.4, there exists u_1 such that $h(u_1, u_1) = 1$. Using lemma 2.3, this can be extended to a basis $u_1, v_2, \ldots, v_m$. But $V' = \text{span}\{v_2, \ldots v_m\}$ has dimension $m-1$ and thus there is a basis $u_2, \ldots u_m$ of V'. Then $\{u_1, u_2, \ldots, u_m\}$ is a basis of V with the desired property. □

Let $\mathfrak{i}$ be a $*$ invariant ideal of A and let $\overline{A} = A/\mathfrak{i}$. Then $*$ induces an involution on $\overline{A}$. Moreover, $\overline{V} = V/V\mathfrak{i}$ is a free $\overline{A}$ module of rank m and the map $\overline{h} : \overline{V} \times \overline{V} \to \overline{A}$, given by $\overline{h}(v+V\mathfrak{i}, w+V\mathfrak{i}) = h(v, w)$ is a non-degenerate hermitian form.

Recall that when A is commutative the discriminant of h is the element of $R^*/Q(A^*)$ obtained by taking the determinanat of the Gram matrix of h relative to any basis of V.

Corollary 1.1. *Let h_1 and h_2 be non-degenerate hermitian forms on V. Then the following conditions are equivalent:*

(a) h_1 and h_2 are equivalent.

(b) The reductions $\overline{h_1}$ and h_2 modulo $\mathfrak{r}$ are equivalent.

(c) The discriminants of $\overline{h_1}$ and $\overline{h_2}$ are the same.

Proof. Need to fill this in □

Given $r_1, \ldots, r_m \in R^*$ we say that h is of type $\{r_1, \ldots, r_m\}$ if there is a basis B of V relative to which h has matrix $\text{diag}\{r_1, \ldots, r_m\}$. In that case, h is also of type $\{s_1, \ldots, s_m\}$ for $s_1 \in R^*$, if and only if $(r_1 \cdots r_m)(s_1 \cdots s_m)^{-1} \in Q(A^*)$.

Proof. Assume that h is of type $\{r_1, \ldots, r_m\}$ and of type $\{s_1, \ldots s_m\}$. Because the determinant is invariant under the choice of basis, $r_1 \cdots r_m = s_1 \cdots s_m$ and $(r_1 \cdots r_m)(s_1 \cdots s_m)^{-1} = 1 \in Q(A*)$.

Now assume that h is of type $\{r_1, \ldots, r_m\}$ with respect to basis B and $(r_1 \cdots r_m)(s_1 \cdots s_m)^{-1} \in Q(A^*)$. It's clear that if $m = 1$ that this implies that h is of type $\{s_1\}$. Consider the case that $m > 1$ and assume also that h is not of type $\{s_1, s_2, \ldots, s_m\}$. Then for every orthogonal basis B of V, let k_B denote the number of $v_i \in V$ such that $h(v_i, v_i) \neq s_i$, and let $k = \min\{k_B : B \text{ is a basis of } V\}$. Because h is not of type $\{s_1, \ldots, s_m\}$, $k > 0$. Similarly, by proposition 3.4, $k <= m-1$. Without loss of generality, assume that $h(v_i, v_i) = s_i$ when $i <= m-k$ and $h(v_i, v_i) = d_i s_i$ where $d_i \neq 1$

(mod $Q(A^*)$) when $i > m-k$. Because h is of type $\{h(v_i, v_i)\}$, and $\det(h)$ is invariant under choice of basis,

$$\prod_{i=1}^{m} r_i = \prod_{i=1}^{m} h(v_i, v_i) = \left(\prod_{i=1}^{m-k} s_i\right)\left(\prod_{i=m-k}^{m} d_i s_i\right)$$

and by assumption,

$$\prod_{i=m-k}^{m} d_i = 1 \mod Q(A^*).$$

This result shows that $k > 1$. Now let $V_1 = \text{span}\{v_i : i \leq m-k\}$ and $V_2 = \text{span}\{v_i : i > m-k\}$. Because $k \geq 2$, by prop 3.4 there exists an orthogonal basis $\{w_1, \ldots, w_k\}$ with $h(w_1, w_1) = s_{m-k+1}$. But then $V' = \{v_1, v_2, \ldots, v_{m-k}, w_1, \ldots, w_k\}$ is a basis for V with $k_{V'} < k$, contradicting the assumption that k was minimized. Thus $d_i = 1$ (mod $Q(A^*)$) for all i, and for some basis V, h is of type $\{s_1, s_2, \ldots, s_m\}$. $\square$

Statement 1. *When m is even then h is of type $\{1, -1, \ldots, 1, -1\}$ (define this as kind I) or $\{1, -1, \ldots, 1, -\varepsilon\}$ (kind II). When m is odd then h is of type $\{1, -1, \ldots, 1, -1, -1\}$ (kind I) or of type $\{1, -1, \ldots, 1, -1, -\varepsilon\}$ (kind II).*

Proof. By theorem 3.5, we know that h is of type $\{1, 1, \ldots, 1\}$ or $\{1, 1, \ldots, \varepsilon\}$. If $-1 \in Q(A^*)$, then the result is immediate. Assume that Q is not surjective and that $-1 \notin Q(A^*)$. Let $r = 1$ if h is of type $\{1, 1, \ldots, 1\}$ and $r = \varepsilon$ if h is of type $\{1, 1, \ldots, \varepsilon\}$. Let $k = \frac{m}{2}$ if m is even, and $k = \frac{m}{2} + 1$ if m is odd. By the previous result, if $r(-1)^k\delta^{-1}$, then h is of type $\{1, -1, \ldots, 1, -\delta\}$ (m even) or $\{1, -1, \ldots, 1, -1, -\delta\}$ (m odd), where $\delta \in \{1, \varepsilon\}$. Note that because $-1 \notin Q(A^*) = R^{*2}$ and $\varepsilon \notin Q(A^*)$, because $[R^* : R^{*2}] = 2$, $-\varepsilon \in Q(A^*)$. Consider 4 cases:

Case 1: $r = 1$ and k even Let $\delta = 1$. Then $r(-1)^k\delta = 1 \in Q(A*)$ and h is of type $\{1, -1, \ldots, -1\}$.

Case 2: $r = 1$ and k odd Let $\delta = \varepsilon$. Then $r(-1)^k\delta = -\varepsilon \in Q(A)$ and h is of type $\{1, -1, \ldots, -\varepsilon\}$.

Case 3: $r = \varepsilon$ and k even Let $\delta = \varepsilon$. Result follows similarly.

Case 4: $r = \varepsilon$ and k odd Let $\delta = 1$. Result follows similarly.

$\square$

Additionally, it is clear from these prior results that h is of kind I and kind II if and only if $Q(A^*) = R^*$.

Even when Q is not surjective, if m is odd there is only one unitary group of rank m, regardless of h, since h and εh are non-equivalent and have the same unitary group.

Lemma 1.2. *Let Λ be the set of all values $h(u, u)$ with $u \in V$ primitive. Assume that the involution $*$ induces on $A/\mathfrak{r}$ is the identity.*

(a) *Suppose $m = 1$. If h is of type $\{1\}$ then $\Lambda = R^{*2}$ and if h is of type $\{\varepsilon\}$ then $\Lambda = R^*/R^{*2}$.*

(b) *Suppose $m = 2$. If h is of type $\{1, -1\}$, then $\Lambda = R$ and if h is of type $\{1, -\varepsilon\}$ then $\Lambda = R^*$.*

(c) *If $m > 2$ then $\Lambda = R$.*

Proof. (a) Assume $m = 1$. Assume that h is of type $\{1\}$. Then $\{u_1\}$ is a basis of V with $h(u_1, u_1) = 1$. Pick $r \in R^{*2}$. Because $*$ is the identity on $A/\mathfrak{r}$, $Q(A^*) = R^{*2}$. Pick $r \in R^{*2}$. Then $r = Q(a) = aa^*$ for some $a \in A^*$ and $h(u_1 a^*, u_1 a^*) = aa^* = r$. Thus $R^{*2} \subseteq \Lambda$. Now let $v \in V$ be primitive. Because $m = 1$, $v = u_1 a$ for some $a \in A^*$ and $h(v, v) \in Q(A) = R^{*2}$. Thus $\Lambda = R^{*2}$. A similar argument shows that $\Lambda = R \backslash R^{*2}$ when h is of type $\{\varepsilon\}$.

(b) Assume $m = 2$ and h is of type $\{1, -1\}$ with corresponding basis vectors u_1, u_2. Then $u_1 + u_2$ is primitive and $h(u_1 + u_2, u_1 + u_2) = 0$. Applying Lemma 3.1 shows that $\Lambda = R$.

Suppose instead that h is of type $\{1, -\varepsilon\}$. Assume that $v = u_1 a_1 + u_2 a_2$ is primitive and $h(v, v) \in \mathfrak{m}$. That is, $a_1 a_1^* - \varepsilon a_2 a_2^* = f \in \mathfrak{m}$. Because v is primitive, at least one a_1, a_2 is a unit. Without loss of generality, assume that $a_1 \in A^*$. Then a_2 is also a unit because $\varepsilon a_2 a_2 \star \neq 0$ in $A/\mathfrak{r}$. Becuase $Q(A) = R^{*2}$, $a_1^2 = b_1 b_1^*$ and $a_2^2 = b_2 b_2^*$ for some $b_1, b_2 \in R^*$. Then $b_1 b_1^* - \varepsilon b_2 b_2^* = f$ and $c_1^2 - \delta c_2^2 = 0$ in $A/\mathfrak{r}$ with $c_1, c_2, \delta \neq 0$. But $\delta = c_1^2 (c_2^{-1})^2 = (c_1 c_2^{-1})^2$, contradicting the assumption that $\varepsilon \notin R^{*2}$. Thus $h(v, v) \in R^*$ for all primitive v. Because h is of type $\{-1, \varepsilon\}$ as well as $\{1, -\varepsilon\}$ there are primitive vectors u and v with $h(u, u) = 1$ and $h(v, v) = \varepsilon$. Thus $\Lambda = R^*$.

(c) Assume that $u_1, u_2, \ldots u_m$ is an orthogonal basis of V with $h(u_i, u_i) \in R^*$. Then $-h(u_3, u_3) \in R^*$ an by proposition 3.4, there exists a primitive vector $v \in u_1 A \oplus u_2 A$ with $h(v, v) = -h(v_3, v_3)$. Then $u = v + u_3$ is primitive with $h(u, u) = 0$, and applying lemma 3.1 shows that $\Lambda = R$. $\square$