1. Introduction

For my 501 project, I'll be working with the paper "Unitary Groups Over Local Rings"[1]. The paper contains a discussion of hermitian forms and unitary groups over a local ring. In my project, I'll provide an introduction to the properties of local rings, and a detailed discussion of hermitian forms defined on module over local ring. Several results are presented that investigate properties of such modules, as well as specific properties of hermitian forms on these modules, and relationships between a norm map and hermitian geometry.

1.1 Basics of Local Rings

This introduction gives a brief discussion of local fields and the construction of a local ring A from a local field K. First, some definitions:

- A field K is a **local field** if it is complete with respect to a discrete valuation and a has finite residue field. An equivalent definition is that a field is locally compact with respect to a non-discrete topology (see [8] for a detailed explanation). This allows an absolute value function to be defined. The real numbers $\mathbb{R}$ and rational numbers $\mathbb{Q}$ are examples of local fields, with the standard topology and absolute values.

- A local field K is said to be **archimidean** if for any element $x \in K$, there exists $n \in \mathbb{N}$ such that $|nx| > 1$. A local field is said to be **non-archimidean** if this property does not hold.

- In any field, the **ring of integers** refers to the set of all integral elements, that is, elements that are the root of a monic polynomial with integer coefficients (that is, coefficients from the set $\{z \cdot 1_K : z \in \mathbb{Z}\}$, where 1_k is the multiplicative identity of K).

- Given a ring A, an automorphism $* : A \to A$ (denoted $a \mapsto a^*$ for $a \in A$) is an **involution** if it satisfies $(a^*)^* = a$ for all $a \in A$ and $(ab)^* = b^*a^*$ for $a, b \in A$.

Given a prime number p, consider the representations of the integers $\mathbb{Z}$ base p. That is, for any integer a, a can be expressed as a sum

$$a = \sum_{i=0}^{n} a_i p^i$$

where $0 \leq a_i \leq p-1$. The p-adic norm, $|\cdot|_p$, can be applied to this representation, defined by

$$|x|_p = \begin{cases} p^{-n_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

where $n_p(x) = \max\{n : p^n | x\}$ if $p|x$ and $n_p(x) = 1$ if $p \nmid x$. This can be shown to satisfy the definition of a norm. Using this norm, every element a of the form

$$a = \sum_{i=k}^{\infty} a_i p_i \quad (k \text{ not necessarily positive})$$

can be shown to be a field, known as the p-adic numbers (denoted K for the remainder of the section). The standard integers $\mathbb{Z} \subset K$ form a ring of integers, denoted $\mathcal{O}$, with maximal ideal (p) and residue field $F_p = \mathcal{O}/\mathfrak{p}$ of characteristic p. Unlike the standard integers, elements of $\mathcal{O}\backslash(p)$ are invertible (see [4] for an explanation).

Define $F = K[\sqrt{p}]$. Depending on $p \mod 4$, the ring of integers of F is slightly different (see [6] or [7] for a more detailed discussion). Define

$$\omega = \begin{cases} \sqrt{p} & \text{if } p \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{p}}{2} & \text{if } p \equiv 1 \pmod 4 \end{cases}$$

Then the ring of integers $\mathcal{R} = \mathcal{O}[\omega]$. Then $\mathcal{R}$ is a free $\mathcal{O}$-module of rank 2. $\mathcal{R}$ is a principle ideal domain with a unique prime element ω (up to associates), and $\mathcal{R}/(\omega) \cong F_p$. There is an involution of F defined by $a + b\omega \mapsto a - b\omega$ that fixes K, with $\mathcal{R}$ invariant under this involution. Given $\ell \geq 1$, let $A = \mathcal{R}/(\omega)^{2\ell}$. Then A is a finite, commutative, principal ideal ring, with an involution inherited from $\mathcal{R}$. A is also a local ring, a concept that will be introduced in detail in the next section.

2. Background in Hermitian Geometry

In this section, we'll define and introduce introduce several objects that will be used throughout the paper. Some definitions:

- A ring is said to be **local** if it has a unique maximal left ideal or unique maximal right ideal.
- The **Jacobson radical** of a ring R, denoted $J(R)$ is the intersection of all maximal left (right) ideals. In a local ring, $J(R)$ coincides with the unique maximal left ideal and unique maximal right ideal, showing that the maximal ideal is two sided.

Throughout the paper, the following objects will be fixed:

- Let A be a local ring with identity.
- Let $\mathfrak{r}$ be the Jacobson radical of A. Because A is local, $\mathfrak{r}$ is maximal, two-sided, and contains all non-units of A.
- Let $*$ be an involution of A. Assume that elements fixed by $*$ are in the center of A, forming a ring $R = \{a \in A : a^* = a\}$. Note that R is local as well, with maximal ideal $R \cap \mathfrak{r}$. This is because any element of R that is not in $R \cap \mathfrak{r}$ is invertible by definition, and cannot be contained in any ideal.
- Let $Q : A^* \to R^* : a \mapsto aa^*$ denote the norm-map.

Example 2.1. Returning to the objects defined in the introduction, we can see an example of each of these objects using the p-adic integers. Let $K, \mathcal{O}, \mathfrak{p}, \mathcal{R}$ and ω be the same as defined previously. For simplicity, assume that $p \equiv 3 \mod 4$. Then $\omega = \sqrt{p}$. Then

- $A = \mathcal{R}/(\omega)^{2\ell}$ is a local ring with maximal ideal $\mathfrak{r} = (\omega)$.
- $A^* = A \backslash (\omega) = \{a + b\omega : a \notin (p)\}$.
- $* : A \to A$ is defined by $a + b\omega \mapsto a - b\omega$.
- $R = \{a + b\omega : b = 0\}$ with maximal ideal $\mathfrak{m} = (\omega)^2$.
- $R^* = \{a + b\omega : b = 0 \text{ and } a \notin (p)\}$.
- $Q : A^* \to R^* : a + b\omega \mapsto a^2 - b^2 p$.

Let V be a right A-module and $h : V \times V \to A$ be a Hermitian form. By definition, h is linear in the second variable and $h(v,u) = h(u,v)^*$ for $u, v \in V$. Then $h(u,u) = h(u,u)^*$ and $h(u,u) \in R \subseteq Z(A)$ for all $u \in V$.

Now consider the dual space V^*. Define an operation $V^* \times A \to V^*$ by $(\alpha a)(v) = a^*\alpha(v)$ where $\alpha \in V^*, a \in A, v \in V$. Under this operation, V^* is a right A-module. Now we can define a homomorphism of right A-modules $\gamma_h : V \to V^*$ associated with h given by $\gamma_h(u) = h(u,-)$. Additionally, for the remainder of the paper:

- Assume that h is non-degenerate; γ_h is an isomorphism.
- Let U be the subgroup of $GL(V)$ preserving h. That is, for $\varphi \in U, u, v \in V$, $h(\varphi(u), \varphi(v)) = h(u,v)$.
- Assume the existence of an element $d \in A$ such that $d + d^* = 1$.
- Assume that V is a free A-module of rank $m \geq 1$.

For the remainder of this section, let $\{v_1, v_2, \ldots, v_m\}$ be a basis of V.

Example 2.2. Continuing the example, let $a = v_1a_1 + \cdots v_ma_m$ and $b = v_1b_1 + \cdots v_mb_m$ with $a_i, b_i \in A$ for $1 \leq i \leq m$. Define $h : V \times V \to A$ by $h(a,b) = a_1^*b_1 + dotsc + a_m^*b_m$. This is a Hermitian form, and can be verified to be non-degenerate. For the rest of the paper, assume that this is how h is defined in all examples.

Lemma 2.3. *There is a vector $u \in V$ such that $h(u,u) \in R^*$.*

Proof. Assume otherwise; that $h(u,u) \in \mathfrak{m}$ for all $u \in V$. Then using the linearity of h:

$$h(u,v) + h(u,v)^* = h(u+v, u+v) - h(u,u) - h(v,v) \in \mathfrak{m}$$

for all $u, v \in V$. Let $\alpha \in V^*$ be the linear functional such that $\alpha(v_1) = d$ and $\alpha(v_i) = 0$ for all $i > 1$. Because h is assumed to be non-degenerate, there exists $u \in V$ such that $h(u,-) = \alpha$. Then $d = \alpha(v_1) = h(u, v_1)$ and $1 = d + d^* = h(u,v_1) + h(u,v_1)^* \notin \mathfrak{m}$, contradicting the original hypothesis. $\square$

Example 2.4. Note that in the p-adic numbers, 2^{-1} is a series satisfying $2^{-1} + 2^{-1} = 1$. Because 2^{-1} is a p-adic integer, $2^{-1} \in R$ and is fixed under the involution. Thus $d = 2^{-1}$. Using h as defined in example 2.2, pick $u = v_1 2^{-1}$. Then $h(u, v_1) = 2^{-1}$ and $h(u, v_i) = 0$ for $i \neq 1$, as desired.

Lemma 2.5. *V has an orthogonal basis $u_1, u_2, \ldots u_m$. Any such basis satisfies $h(u_i, u_i) \in R^*$.*

Proof. Prove with induction on m. Assume that $m = 1$. By lemma 2.3, there exists $u \in V$ such that $h(u,u) \in R^*$. Then $u = v_1 a_1$ for some $a_1 \in A^*$, and $h(u,u) = h(v_1 a_1, v_1 a_1) = a_1^* h(v_1, v_1) a_1 \in R*$ implying that $h(v_1, v_1) \in R^*$. Now assume that $m > 1$ and that the hypothesis holds for $m-1$. Once again, there exists $u \in V$ such that $h(u,u) \in R^*$. Then $u = v_1 a_1 + \cdots + v_m a_m$ with $a_i \in A$. If all $a_i \in \mathfrak{r}$, then $h(u,u) \in \mathfrak{m}$, a contradiction. Without loss of generality, assume that $a_1 \notin \mathfrak{r}$. Then if $u_1 = v_1 a_1$, the set $\{u_1, v_2, \ldots, v_m\}$ is a basis of V. For $1 < i \leq m$, set

$$u_i = v_i - u_1[h(u_1, v_i)/h(u_1, u_1)]$$

Then $u_1, u_2, \ldots, u_m$ is a basis of V satisfying $h(u_1, u_i) = 0$ for $1 < i \leq m$. Let $V_1 = u_1 A$ and $V_2 = \text{span}\{u_2, \ldots, u_m\}$. Then $V = V_1 \perp V_2$ and the restriction of h to V_2 induces an isomorphism $V_2 \to V_2^*$. Applying the inductive hypothesis to this space completes the proof. □

Lemma 2.6. *(a) Suppose $u_1, \ldots, u_s \in V$ are orthogonal and satisfy $h(u_i, u_i) \in R^*$. Then $u_1, \ldots, u_s \in V$ can be extended to an orthogonal basis of V with the same property.*

(b) If V_1 is a submodule of V such that the restriction of h to V_1 is non-degenerate there is another such submodule V_2 of V such that $V = V_1 \perp V_2$.

Proof. (a) Because $\{v_1, \ldots, v_m\}$ is a basis of v, $u_1 = v_1 a_1 + \cdots + v_m a_m$ for some $a_i \in A$. Since $h(u_1, u_1) \in R^*$ (by lemma 2.3), one of the scalars must be a unit. Without loss of generality, assume $a_1 \in A*$. Thus $u_1, v_2, \ldots, v_m$ is a basis of V. Suppose $1 \leq t \leq s$ and the list $u_1, \ldots, u_t, v_{t+1}, \ldots, v_m$ is a basis of V. Then

$$u_{t+1} = u_1 b_1 + \cdots + u_t b_t + v_{t+1} b_{t+1} + \cdots + v_m b_m$$

for some $b_i \in A$. Suppose, if possible, that $b_i \in \mathfrak{r}$ for all $i \geq t+1$. Then for every $i \leq t$,

$$0 = h(u_i, u_{t+1}) = h(u_i, u_i) b_i + h(u_i, v_{t+1}) b_{t+1} + \cdots + h(u_i, v_m) b_m$$

implying that $b_i \in \mathfrak{r}$ for all $1 \leq i \leq t$, contradicting the assumption that $h(u_{t+1}, u_{t+1}) \in R^*$. Thus at least one of $b_{t+1}, \ldots, b_m$ is a unit (assume b_{t+1} and $u_1, \ldots u_t, u_{t+1}, v_{t+2}, \ldots, v_m$ is a basis of V.

This process can be repeated to extend $u_1, \ldots, u_s$ to a basis $u_1, \ldots, u_s, u_{s+1}, \ldots u_m$ of V. For $s < i \leq m$, let

$$z_i = u_i - ([u_1 h(u_1, u_i)/h(u_1, u_1)] + \cdots + u_s h(u_s, u_i)/h(u_s, u_s)].$$

Then $u_1, \ldots, u_s, z_1, \ldots, z_{m-s}$ is a basis of V satisfying $h(u_i, z_j) = 0$. If follows that the restriction of h to $M = \text{span}\{z_1, \ldots, z_{m-s}\}$ is non-degenerate and by lemma 2.5 that M has an orthogonal basis with $h(z_i, z_i) \in R^*$ for any $i \leq m - s$.

(b) Follows from (a) and lemma 2.5 □

Lemma 2.7. *Let $u_1, \ldots u_s \in V$, with corresponding Gram matrix $M \in M_s(A)$, defined by $M_{ij} = h(u_i, u_j)$. If $M \in GL_m(A)$, then $u_1, \ldots, u_s$ are linearly independent.*

Proof. Suppose $a_1, \ldots, a_s$ satisfy $u_1a_1 + \cdots + u_sa_s = 0$. Then for $1 \leq i \leq s$

$$0 = h(u_i, u_1a_1 + \cdots + u_sa_s) = h(u_i, u_1)a_1 + \cdots + h(u_i, u_s)a_s$$

implying that

$$M \begin{pmatrix} a_1 \\ \vdots \\ c_1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since M is inverible, the desired result follows. □

3. 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 $h(v, v) = 0$.

Example 3.1. Using h as defined in example 2.2, h is not isotropic. To see this, let $u = v_1 a_1 + \dots v_m a_m$ where $a_i = b_i + c_i\sqrt{p}$. Then

$$\begin{aligned} h(u,u) &= a_1^* a_1 + \cdots + a_m^* a_m \\ &= b_1^2 - c_1^2 p + \cdots + b_m - c_m^2 p \\ &= \sum_{i=1}^{m} b_i^2 - \sum_{i=1}^{m} c_i^2 p \end{aligned}$$

Then if $h(u, u) = 0$

$$\sum_{i=1}^{m} b_i^2 = p \sum_{i=1}^{m} c_i^2$$

Assume that

$$\sum_{i=1}^{m} c_i = sp^j$$

where $p \nmid s$. Then s is invertible and

$$\sum_{i=1}^{m} b_i^2 = sp^{j+1}.$$

Similarly, $p - 1$ is invertible because $p - 1 \notin (\sqrt{p})$. Then

$$\begin{aligned} s^{-1}(p-1)^{-1}\left(\sum b_i^2 - \sum c_i^2\right) &= s^{-1}(p-1)^{-1}(sp^{j+1} - sp^j) \\ &= p^j \end{aligned}$$

implying that $s^{-1}(p-1)^{-1} | p^j$, a contradiction. Thus h cannot be isotropic.

Lemma 3.2. *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

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

□

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 $[R^* : R^{*2}] = 2$. For the remainder of the paper, 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 3.3. *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 $A/\mathfrak{r} \cong F_{q^2}$.*

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 $A/\mathfrak{r}$ by $a + \mathfrak{r} \mapsto a^* + \mathfrak{r}$. 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 $k = R/m$. Consider two cases:

(a) The involution that $*$ induces on $A/\mathfrak{r}$ is the identity: 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. Because R is commutative and $\mathfrak{m}$ is a maximal ideal, $R/\mathfrak{m}$ is a

field, implying that $A/\mathfrak{r}$ is commutative. This completes the proof of this case. (b) The involution that $*$ induces on $A/\mathfrak{r}$ is not the identity: 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

$$(e_1f_1 + f_1e_1)^\circ = f_1^\circ e_1^\circ + e_1^\circ f_1^\circ = f_1e_1 + e_1f_1$$

and $e_1f_1 + f_1e_1 \in k$. Thus $k\langle f_1, e_1\rangle$ is the k-span of $1, f_1, e_1, f_1e_1$ 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 $[A/\mathfrak{r} : k] = 2$.

Let $\hat{Q} : (A/\mathfrak{r})^* \to k^*$ be the norm map induced by Q. We now want to show that $\hat{Q}$ 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

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

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.

Using the fact that the squaring map of $1 + \mathfrak{m}$ is surjective, this can be used to show that $Q : A^* \to R^*$ is surjective. □

Example 3.4. Recall that in our example, $\mathfrak{r} = (\sqrt{p})$ and $\mathfrak{m} = (p)$. Thus $A/\mathfrak{r} \cong R/\mathfrak{m} \cong F_p$. Furthermore, the involution $*$ induces on $A/\mathfrak{r}$ is the identity. Pick $c \in F_p \backslash F_p^2$. Then c cannot be in the image of $*$, because for any $a + b\sqrt{p} \in A$, $c \not\equiv a^2 \mod p$, and therefore $c \neq a^2 - b^2 p$. Thus Q is not surjective.

Proposition 3.5. *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:

Case 1: h is isotropic. Then 3.2 applies.

Case 2: h is non-isotropic.

By lemma 2.5, there is an orthogonal basis $u_1, u_2, \ldots u_m$ of V such that $h(u_i, u_i) \in R^*$. Let $a = h(u_1, u_2) \in R^*$ and $b = h(u_2, u_2) \in R^*$. if $t_1, t_2 \in R^*$, then $v = u_1 t_1 + u_2 t_2$ is primitive (because it is part of a basis), so

$$0 \neq h(v, v) = a t_1^2 + b t_2^2.$$

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

$$0 \neq t_1^2 + c t^2$$

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 the 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 $t_1 + t_2\delta \mapsto t_1^2 + c t_2^2$.

We claim that S is local with maximal ideal $S\mathfrak{m}$. To show this, we want to show that any non-invertible element of S is contained in $S\mathfrak{m}$. Let $t_1, t_2 \in R$, not both in $\mathfrak{m}$, and consider $J(t_1 + t_2\delta) = t_1^2 + c t_2^2$. This breaks into two cases:

Case 1: One of $t_1, t_2 \in \mathfrak{m}$. Then if $t_1^2 + c t_2^2 \in \mathfrak{m}$, $t_1^2 = -c t_2^2 + m$ and $c t_2^2 = -t_1^2 - m$ 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 $t_1^2 + c t_2^2 \in R^*$ and $t_1 + t_2\delta \in S^*$.

Case 2: Both $t_1, t_2 \notin \mathfrak{m}$. Suppose that $t_1 + t_2\delta \notin S^*$. Then $t_1^2 + c t_2^2 = f \in \mathfrak{m}$, 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 $t_1 + t_2\delta \in S^*$.

Therefore $S\mathfrak{m}$ is an ideal of S, containing every non-unit, implying that it is maximal and that S is local.

Because S is commutative, $S/S\mathfrak{m}$ 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 $\{1+S\mathfrak{m}, \delta+S\mathfrak{m}\}$ 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 order 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 $t_1, t_2 \in R$ 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 3.6. *There is an orthogonal basis $v_1, v_2, \ldots, v_m$ of V satisfying*

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

Proof. To prove this, we'll use induction on m. Assume that $m = 1$. By lemma 2.5, 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 $v_1 = u_1 a^{-1}$. Then

$$h(v_1, v_1) = (a^{-1})^* a^{-1} h(u, u) = 1.$$

If $Q(A^*) = R^{*2}$, then consider two cases.

Case 1: $h(u_1, u_1) \in R^* * \backslash R^{*2}$. Then there exists v such that $h(v, v) = 1$, as shown.

Case 2: $h(u_1, u_1) \in R^{*2}$. 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

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

Taking $v_1 = v$ gives $h(v_1, v_1) \in \{1, \varepsilon\}$.

Now assume that $m > 1$ and that the hypothesis is true for $m - 1$. By proposition 3.5, there exists v_1 such that $h(v_1, v_1) = 1$. Using lemma 2.6, this can be extended to an orthogonal basis $v_1, u_2, \ldots, u_m$. Let $V' = \text{span}\{u_2, \ldots, u_m\}$. Then V' has dimension $m-1$ and by the inductive hypothesis there exits is a basis $v_2, \ldots v_m$ of V'. Then $\{v_1, v_2, \ldots, v_m\}$ is a basis of V with the desired property. □

Example 3.7. In our example, because h was defined in terms of $v_1, \ldots, v_m$, this basis will by be orthogonal by the definition of h, and $h(v_i, v_i) = 1$ for all i.

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 3.8. *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 $\overline{h_2}$ modulo $\mathfrak{r}$ are equivalent.

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

Proof. (a) implies (b): Assume that h_1 and h_2 are equivalent. Then there exists some isomorphism $T : V \to V$ (with matrix representation T) such that $h_1(v, w) = h_2(Tv, Tw)$ for all $v, w \in V$. Then

$$\overline{h_1}(v + V\mathfrak{r}, w + V\mathfrak{r}) = h_1(v, w) = h_2(Tv, Tw) = \overline{h_2}(Tv + V\mathfrak{r}, Tw + V\mathfrak{r})$$

and $\overline{h_1}$ is equivalent to $\overline{h_2}$.

(b) implies (c): Assume that $v_1 + V\mathfrak{r}, \ldots, v_m + V\mathfrak{r}$ is the orthogonal basis for $\overline{V}$ given in theorem 3.6 and that $\overline{h_1}(v+V\mathfrak{r}, w+V\mathfrak{r}) = \overline{h_2}(Tv+V\mathfrak{r}, Tw+V\mathfrak{r})$ for some invertible T and all $v \in V$. Then $Tv_1 + V\mathfrak{r}, \ldots, Tv_m + V\mathfrak{r}$ is a basis; and is orthogonal with respect to $\overline{h_2}$. Let d represent the discriminant function. Using the fact that the determinant is invariant under choice of

basis:

$$\begin{aligned} d(\overline{h_1}) &= \prod_{i=1}^{m} \overline{h}_1(v_i + V\mathfrak{r}, v_i + V\mathfrak{r}) \\ &= \prod_{i=1}^{m} \overline{h_2}(Tv_i + V\mathfrak{r}, Tv_i + V\mathfrak{r}) \\ &= d(\overline{h2}) \end{aligned}$$

(c) implies (a): Assume that the discriminants of $\overline{h_1}$ and $\overline{h_2}$ are the same. Let $v_1, \ldots, v_m$ and $w_1, \ldots, w_m$ be orthogonal bases satisfying theorem 3.6 for h_1 and h_2 respectively. Then $h_1(v_i, v_i) = h_2(w_i, w_i)$ for all i (because the discriminants are equal, it is ensured that $h_1(v_m, v_m) = h_2(w_m, w_m)$). Let $T : V \to V$ be defined by $v_i \mapsto w_i$. Then for $x, y \in V$:

$$\begin{aligned} h_1(x, y) &= \sum_{i=1}^{m} h_1(v_i x_i, v_i y_i) \\ &= \sum_{i=1}^{m} x_i^* y_i h_i(v_i, v_i) \\ &= \sum_{i=1}^{m} x_i^* y_i h_2(Tv_i, Tv_i) \\ &= \sum_{i=1}^{m} h_2(Tv_i x_i, Tv_i y_i) \\ &= h_2(Tx, Ty) \end{aligned}$$

and h_1 and h_2 are equivalent.

□

Example 3.9. Let $h_1 = h$ as defined in previous examples (where $h(v_i, v_i) = 1$ for basis $v_1, \ldots, v_m$) and define h_2 similarly for some basis $u_1, \ldots, u_m$. Let $T : V \to V$ be defined by $u_i \mapsto v_i$. Then h_1 and h_2 are equivalent, with $h_2(Tu_i, Tu_i) = h_2(v_i, v_i) = 1 = h_1(v_i, v_i)$ for all i. Similarly, the reductions of h_1 and h_2 modulo $\mathfrak{r}$ are equivalent, because each has a gram matrix of the identity matrix with respect to the basis they are defined by. This also implies that their discriminants are the same. In fact, in our example, because A is commutative, we can see that h_1 and h_2 have the same discriminant by taking the determinant of the Gram matrix with respect to $v_1, \ldots, v_m$ and $u_1, \ldots, u_m$.

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 $\text{diag}\{r_1, \ldots, r_m\}$. Note that because these matrices contain only elements of R^*, which is commutative, the notion of a determinant is well defined.

Lemma 3.10. *h is of type $\{r_1, \ldots, r_m\}$ and $\{s_1, \ldots, s_m\}$ 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 R 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 where $h(v_i, v_i) \in R^*$ for $v_i \in B$, 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, $k \leqslant m - 1$. Without loss of generality, assume that $h(v_i, v_i) = s_i$ when $i \leqslant m - k$ and $h(v_i, v_i) = d_i s_i$ where $d_i \neq 1 \pmod{Q(A^*)}$ when $i > m - k$. Because h is of type $\{h(v_i, v_i) : 1 \leq i \leq m\}$, and $\det(h)$ is invariant under choice of basis,

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

and by assumption,

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

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 proposition 3.5 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 $d_i = 1 \pmod{Q(A^*)}$ for all i, and for some basis V, h is of type $\{s_1, s_2, \ldots, s_m\}$. □

Lemma 3.11. *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 3.6, 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 $k = \frac{m+1}{2}$ if m is odd. By the previous result, if $r(-1)^k\delta^{-1} \in Q(A^*)$, for some $\delta \in R^*$, 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.

□

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 3.12. *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 $\Lambda = R^* \backslash R^{*2}$.*

(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 $h(u_1a^*, u_1a^*) = aa^* = r$. Thus $R^{*2} \subseteq \Lambda$. Now let $v \in V$ be primitive. Because $m = 1$, $v = u_1a$ 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 $v = u_1a_1 + u_2a_2$ is primitive and $h(v, v) \in \mathfrak{m}$. That is, $a_1a_1^* - \varepsilon a_2a_2^* = f \in \mathfrak{m}$. 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 $\varepsilon a_2a_2^* \neq 0$ in $A/\mathfrak{r}$. Because $Q(A) = R^{*2}$, $a_1a_1^* = b_1^2$ and $a_2a_2^* = b_2^2$ for some $b_1, b_2 \in R^*$. Then $b_1^2 - \varepsilon b_2^2 = f$. Let $c_1 = b_1 + \mathfrak{r}, c_2 = b_2 + \mathfrak{r}, \delta = \varepsilon + \mathfrak{r} \in A/\mathfrak{r}$ Then $c_1^2 - \delta c_2^2 = 0$ in $A/\mathfrak{r}$ with $c_1, c_2, \delta \neq 0$. But $\delta = c_1^2(c_2^{-1})^2 = (c_1c_2^{-1})^2$, 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 3.5, there exists a primitive vector $v \in u_1A \oplus u_2A$ 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 $\Lambda = R$. □

Example 3.13. Continue with h as defined previously. In our example, the involution that $*$ induces on $A/\mathfrak{r}$ is the identity. Then h is of type $\{1\}$ with respect to the basis $v_1, \ldots, v_m$.

(a) If $m = 1$, then v_1a is primitive for all $a \notin \mathfrak{r}$. Then $h(v_1a, v_1a) = a^*a \in Q(A^*)$. Then $\Lambda = Q(A^*) = R^{*2}$

(b) If $m = 2$, then by lemma 3.11, h is of type $\{1, -\varepsilon\}$. Then h is also of type $\{-1, \varepsilon\}$ and there exist primitive vectors u and v such that $h(u, u) = 1$ and $h(v, v) = \varepsilon$. Then for $x \in R^{*2}, x = Q(a)$ for some $a \in A^*$ and $x = aa^* = h(va^*, va^*)$. Thus $R^{*2} \subset \Lambda$. Similarly, if $y \notin R^{*2}$, then $y = \varepsilon b^2$ for some $b \in R^*$ (note this is because $[R^* : R^{*2}] = 2$). Then $y = h(vb, vb)$ and $R^* \backslash R^{*2} \subset \Lambda$, implying that $\Lambda = R^*$.

(c) By assumption, $h(v_3, v_3) = 1$. Applying proposition 3.5, there exists a primitive $u \in v_1A \oplus v_2A$ such that $h(u, u) = -1$. Then $u + v_3$ is primitive and $h(u + v_3, u + v_3) = 0$, allowing lemma 3.2 to be applied and shows that $\Lambda = R$.

References

[1] J. Cruickshank, A. Herman, R. Quinlan, and F. Szechtman. Unitary groups over local rings. *Journal of Algebra and Its Applications*, 13, 9 2013.

[2] Thomas W. Hungerfor. *Algebra*. Springer-Verlag, New York, United States, 1974.

[3] D. A. Jordan. Some examples of noncommutative local rings. *Glasgow Mathematical Journal*, 32:79–86, 1 1990.

[4] Svetlana Katok. *p-adic Analysis Compared with Real*. American Mathematical Society, Providence, Rhode Island, 2007.

[5] Max-Albert Knus. *Quadratic and Hermitian Forms over Rings*. Springer-Verlag, Berlin, Germany, 1991.

[6] James S. Milne. Algebraic number theory (v3.01), 2008. Available at www.jmilne.org/math/.

[7] Pierre Samuel. *Algebraic Theory of Numbers*. Hermann, Paris, France, 1970.

[8] Jean-Pierre Serre. *Local Fields*. Springer-Verlag, New York, United States, 1979.