

On the local theory of quaternionic anti-hermitian forms

By Takashi TSUKAMOTO*

(Received June 24, 1961)

The purpose of this paper is to give a theory of the anti-hermitian forms over a p -adic quaternion algebra \mathfrak{D} , i. e. the unique quaternion division algebra over a given p -adic number field. We shall determine in §2 the types (in the sense of Witt) of such anti-hermitian forms, showing that the type of an anti-hermitian form over \mathfrak{D} is uniquely determined by the parity of the number of variables and by its discriminant, and that these two invariants can be given arbitrarily (Theorem 3). §3 is concerned with the ‘maximal integral lattice’; we shall prove the Witt decomposition theorem for such lattices, and using this, obtain some results on the structure of the group of automorphisms (or of similitudes) of an anti-hermitian form over \mathfrak{D} , which are quite analogous to those obtained by Tamagawa for other classical groups. §1 is of preliminary nature and contains some definitions and known results indispensable for our considerations.

§1. Quaternionic anti-hermitian forms and the associated sesquilinear forms.

1.1. Let k be a field of characteristic different from 2, and let \mathfrak{D} be a quaternion division algebra over k , i. e. a division algebra with a basis $(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ over k such that

$$\begin{aligned}\varepsilon_0 &= \text{identity element,} \\ \varepsilon_1^2 &= \varepsilon_0 c_1, \quad \varepsilon_2^2 = \varepsilon_0 c_2 \quad (c_1, c_2 \in k), \\ \varepsilon_1 \varepsilon_2 &= -\varepsilon_2 \varepsilon_1 = \varepsilon_3.\end{aligned}$$

For $\xi = \sum_{i=0}^3 \varepsilon_i \xi_i \in \mathfrak{D}$, the canonical involution $\xi \rightarrow \bar{\xi}$ of \mathfrak{D} is given by

$$\bar{\xi} = \varepsilon_0 \xi_0 - \sum_{i=1}^3 \varepsilon_i \xi_i$$

and the reduced norm of ξ from \mathfrak{D} to k , denoted by $n(\xi)$, is equal to $\xi \bar{\xi}$. We

*) T. Tsukamoto died on August 9, 1960, at the age of 23, by an accident in the mountain climbing. This paper was written originally in Japanese as a report to a seminar led by Professor T. Tamagawa and published in provisional form in “Sugaku”, vol. 12 (1961). This English version was edited by I. Satake.

denote by \mathfrak{D}^- the set of all 'pure quaternions', i. e. those elements ξ in \mathfrak{D} such that $\bar{\xi} = -\xi$. We usually identify k with $\varepsilon_0 k \subset \mathfrak{D}$.

Let V be a finite-dimensional right vector space over \mathfrak{D} . A mapping Φ from $V \times V$ into \mathfrak{D} is called a *sesquilinear form* on $V \times V$, if it satisfies the following conditions:

$$(1) \quad \Phi(x, y+y') = \Phi(x, y) + \Phi(x, y'),$$

$$(2) \quad \Phi(x, y\alpha) = \Phi(x, y)\alpha,$$

$$(1') \quad \Phi(x+x', y) = \Phi(x, y) + \Phi(x', y),$$

$$(2') \quad \Phi(x\alpha, y) = \bar{\alpha}\Phi(x, y),$$

for any $x, x', y, y' \in V$, $\alpha \in \mathfrak{D}$. It is called *anti-hermitian* if in addition it satisfies the condition

$$(3) \quad \Phi(y, x) = -\overline{\Phi(x, y)}$$

for all $x, y \in V$. A mapping H from V into \mathfrak{D}^- is called an *anti-hermitian form* on V , if the following conditions are satisfied:

$$(4) \quad H(x\alpha) = \bar{\alpha}H(x)\alpha.$$

There exists a sesquilinear form Φ on $V \times V$ such that

$$(5) \quad H(x+y) - H(x) - H(y) = \Phi(x, y) - \overline{\Phi(x, y)}.$$

PROPOSITION 1. *For an anti-hermitian form H on V the sesquilinear form Φ satisfying the condition (5) is uniquely determined.*

PROOF. It is enough to show that $H=0$ implies $\Phi=0$. If $H=0$, we have for any $x, y \in V$, $\lambda \in \mathfrak{D}$

$$\Phi(x, y)\lambda - \overline{\Phi(x, y)\lambda} = H(x+y\lambda) - H(x) - H(y\lambda) = 0.$$

Hence

$$\Phi(x, y)\lambda = \bar{\lambda}\overline{\Phi(x, y)}.$$

Putting $\lambda=1$, we see that $\Phi(x, y)$ is in k . If $\Phi \neq 0$, it would follow that $\lambda = \bar{\lambda}$ for all $\lambda \in \mathfrak{D}$, which is a contradiction. q. e. d.

Since in (5) we may replace $\Phi(x, y)$ by $-\overline{\Phi(y, x)}$, it follows that the sesquilinear form Φ in (5) is anti-hermitian, and since the characteristic is different from 2, we have $H(x) = \Phi(x, x)$. Conversely, given an anti-hermitian sesquilinear form Φ on $V \times V$, $H(x) = \Phi(x, x)$ becomes an anti-hermitian form on V . Thus the anti-hermitian forms on V and the anti-hermitian sesquilinear forms on $V \times V$ are in one-to-one correspondence. The sesquilinear form Φ satisfying the condition (5) (viz. anti-hermitian and such that $\Phi(x, x) = H(x)$) is called the sesquilinear form *associated with H* .

From now on we shall fix once for all an anti-hermitian form H on V (and the associated anti-hermitian sesquilinear form Φ on $V \times V$). With this

structure, V is called an *anti-hermitian space* over \mathfrak{D} . The relation of orthogonality is defined with respect to Φ . For a vector subspace W of V , we denote by W^\perp the subspace formed of all the vectors in V which are orthogonal to W . We assume in the following that Φ is ‘non-degenerate’, i. e. that $V^\perp = \{0\}$.

PROPOSITION 2. V has an orthogonal basis.

PROOF. By virtue of Proposition 1, there exists a vector x_1 in V such that $H(x_1) \neq 0$. Then, denoting by $\{x_1\}_\mathfrak{D}$ the subspace generated by x_1 over \mathfrak{D} and putting $V' = \{x_1\}_\mathfrak{D}^\perp$, we have

$$V = \{x_1\}_\mathfrak{D} + V' \quad (\text{orthogonal sum}).$$

Since the restriction of Φ on $V' \times V'$ is again non-degenerate, the Proposition follows by induction on the dimension of V . q. e. d.

1.2. The following two propositions are special cases of Witt’s theorems. For the proofs, we refer to Bourbaki [1] or Dieudonné [2].

PROPOSITION 3. Let W_1, W_2 be two subspaces of V . Then any linear isomorphism ρ from W_1 onto W_2 such that $H(\rho(x)) = H(x)$ for all $x \in W_1$ can be extended to an automorphism of the anti-hermitian space V .

PROPOSITION 4. V can be decomposed in the following form:

$$(6) \quad V = V_0 + \sum_{i=1}^\nu \{e_i, e_i'\}_\mathfrak{D} \quad (\text{orth. sum}),$$

where

$$H(e_i) = H(e_i') = 0, \quad \Phi(e_i, e_i') = 1 \quad (1 \leq i \leq \nu)$$

and V_0 is ‘anisotropic’ (i. e. $x \in V_0, H(x) = 0$ imply $x = 0$). Moreover this decomposition is unique up to an automorphism of the anti-hermitian space V .

The decomposition (6) is called a *Witt decomposition* and ν the *index* of V (or of H). The (unique) isomorphism class of V_0 is called the *type* of V . We write $V \sim V'$ if V, V' belong to the same type. We define an addition of types by calling the type of the direct sum $V_1 + V_2$ the sum of the types of V_1 and V_2 ; the ‘zero type’ is given by the type of the space of dimension 0, and the inverse of the type of V with the anti-hermitian form H is given by the type of the same space V with $-H$. Thus the set of all the types of the anti-hermitian spaces over \mathfrak{D} forms a commutative group, called the *Witt group* and denoted by \mathcal{T} .

It is clear that, if V is of dimension n , the ‘parity’ of n (viz. $(-1)^n$) depends only on the type of V . We denote by \mathcal{T}^+ the subgroup of \mathcal{T} formed of all the ‘even’ types, i. e. the types of the spaces of even dimension.

1.3. We define the *discriminant* $\delta(V)$ of an anti-hermitian space V as follows. Let (x_1, \dots, x_n) be a basis of V over \mathfrak{D} . Denoting by N the reduced norm from

$M_n(\mathfrak{D})^{*})$ to k , we put

$$(7) \quad \delta(V) = (-1)^n N((\Phi(x_i, x_j))) \pmod{(k^*)^2},$$

where k^* is the multiplicative group of the non-zero elements in k . Clearly $\delta(V)$ does not depend on the choice of the basis (x_i) and actually depends only on the type of V , as we have $\delta(V) = \delta(V_0)$. Also it is clear that

$$\delta(V+V') = \delta(V)\delta(V')$$

for the direct sum $V+V'$. Thus we have the following

PROPOSITION 5. *The mapping $V \rightarrow \delta(V)$ is a homomorphism from the Witt group \mathcal{I} into $k^*/(k^*)^2$.*

§ 2. Determination of the types in the case of local fields.

2.1. Throughout this paper we keep the notations in § 1. For $a, a' \in k^*$, we write $a \sim a'$ if a'/a is a square in k^* . In this section, k is assumed to satisfy the following condition:

(C) *The local class field theory for quadratic extensions holds in k ; i. e. there exists a one-to-one correspondence between the classes in $k^*/(k^*)^2$ of the elements $a \not\sim 1$ and the subgroups M of k^* of index 2 by the relation $M = N(k(\sqrt{a})^*)$, N denoting the norm from $k(\sqrt{a})$ to k .*

We exclude the trivial case where $k^* = (k^*)^2$. Then it can easily be shown that there exists one and only one quaternion division algebra \mathfrak{D} over k (up to an isomorphism) and that every element a in k^* is a square of some element in \mathfrak{D} . (If $a \not\sim 1$, a is a square of some element in \mathfrak{D}^- .) We distinguish two cases.

Case (I): $[k^* : (k^*)^2] = 2$. In this case, k has a unique quadratic extension K and we have $n(\mathfrak{D}^*) = N(K^*) = (k^*)^2$, \mathfrak{D}^* denoting the multiplicative group of the non-zero elements in \mathfrak{D} . 'Real closed fields' belong to this case.

Case (II): $[k^* : (k^*)^2] > 2$. In this case, we have $n(\mathfrak{D}^*) = k^*$. 'p-adic number fields' belong to this case.

LEMMA 1. *Under the above assumptions, \mathfrak{D} satisfies the following property.*

(N) *For non-zero elements ξ, η in \mathfrak{D}^- , there exists an element α in \mathfrak{D}^* such that $\eta = \bar{\alpha}\xi\alpha$, if and only if $n(\xi) \sim n(\eta)$.*

PROOF. The 'only if' part of (N) is trivial. To prove the 'if' part, let ξ, η be non-zero elements in \mathfrak{D}^- such that $n(\eta) = n(\xi)a^2$ with $a \in k^*$. Since every element in k^* is a square of some element in \mathfrak{D}^* , there exists $\alpha \in \mathfrak{D}^*$ such that $a = \alpha^2$. Then it follows that

$$(\bar{\alpha}\xi\alpha)^2 = -n(\bar{\alpha}\xi\alpha) = -n(\alpha)^2 n(\xi) = -a^2 n(\xi) = -n(\eta) = \eta^2,$$

*) For any ring R , $M_n(R)$ denotes the ring of all $n \times n$ matrices with components in R .

so that $k(\bar{\alpha}\xi\alpha)$, $k(\eta)$ are mutually isomorphic quadratic extensions of k contained in \mathfrak{D} . Therefore they must be transformed to each other by an inner automorphism of \mathfrak{D} , i. e. there exists $\beta \in \mathfrak{D}^*$ such that $\bar{\alpha}\xi\alpha = \beta\eta\beta^{-1}$ or

$$n(\beta)^{-1}\bar{\alpha}\beta\xi\alpha\beta = \eta.$$

If $n(\beta) \in n(k(\eta))$, then, by replacing β by $\beta\eta$ with a suitable η in $k(\eta)$, we may assume that $n(\beta) = 1$, finishing the proof. This is surely the case in Case (I). In Case (II), every element in k^* being a norm of some element in \mathfrak{D}^* , we can find $\alpha, \alpha' \in \mathfrak{D}^*$ such that $n(\alpha) = a$, $n(\alpha') = -a$. Then quite similarly as above, we see that there exist $\beta, \beta' \in \mathfrak{D}^*$ such that $\bar{\alpha}\xi\alpha = \beta\eta\beta^{-1}$, $\bar{\alpha}'\xi\alpha' = \beta'\eta\beta'^{-1}$, and that the Lemma holds if $n(\beta)$ or $n(\beta')$ is in $n(k(\eta))$. Therefore it remains only to consider the case where $n(\beta), n(\beta') \notin n(k(\eta))$. In this case, we have, from the local class field theory, $n(\beta)^{-1}n(\beta') \in n(k(\eta))$. On the other hand, we have

$$n(\alpha)^{-1}\alpha\beta\eta(\alpha\beta)^{-1} = \xi = n(\alpha')^{-1}\alpha'\beta'\eta(\alpha'\beta')^{-1}.$$

Hence, putting $\gamma = \beta^{-1}\alpha^{-1}\alpha'\beta'$, we have

$$n(\gamma) = -n(\beta)^{-1}n(\beta') \in -n(k(\eta)),$$

$$\gamma^{-1}\eta\gamma = -\eta.$$

It follows that $(1, \eta, \gamma, \eta\gamma)$ forms a basis of \mathfrak{D} over k and that γ^2 , commuting with both η and γ , belongs to k . Hence γ belongs to \mathfrak{D}^- . But then we have $\gamma^2 = -n(\gamma) \in n(k(\eta))$, contradicting the fact that \mathfrak{D} is a division algebra. q. e. d.

2.2. Let a_1, \dots, a_n be n elements in k^* such that $a_i \not\sim 1$ and let α_i be n elements in \mathfrak{D}^- such that $\alpha_i^2 = -n(\alpha_i) = a_i$ ($1 \leq i \leq n$). Call V an n -dimensional anti-hermitian space over \mathfrak{D} with an orthogonal basis (x_1, \dots, x_n) such that $H(x_i) = \alpha_i$. It follows from Lemma 1 that the structure of the anti-hermitian space V depends only on the classes of the a_i modulo $(k^*)^2$. Hence we shall write $V = V(a_1, \dots, a_n)$. By Proposition 2 all anti-hermitian spaces are obtained in this manner. It is clear from (7) that

$$(8) \quad \delta(V(a_1, \dots, a_n)) = a_1 \cdot \dots \cdot a_n.$$

We shall make a free use of these notations in the rest of this section.

THEOREM 1. *If k satisfies the condition (C), any anti-hermitian space over \mathfrak{D} of dimension ≥ 4 contains an isotropic vector (i. e. a non-zero vector x such that $H(x) = 0$).*

PROOF. It is enough to consider the case $V = V(a_1, a_2, a_3, a_4)$. Then, since the dimension of \mathfrak{D}^- over k is 3, we have, in the above notations, a non-trivial linear relation $\sum_{i=1}^4 \alpha_i l_i = 0$ with $l_i \in k$. As $n(\alpha_i l_i) = n(\alpha_i) l_i^2$, there exist by Lemma 1 $\lambda_i \in \mathfrak{D}$ ($1 \leq i \leq 4$) such that $\alpha_i l_i = \bar{\lambda}_i \alpha_i \lambda_i$. Then the λ_i are not all zero and we get $H(\sum_{i=1}^4 x_i \lambda_i) = \sum_{i=1}^4 \bar{\lambda}_i \alpha_i \lambda_i = 0$. q. e. d.

REMARK. As is seen from the above proof, Theorem 1 holds whenever \mathfrak{D} satisfies the condition (N).

THEOREM 2. *In Case (I), the Witt group \mathfrak{I} is a group of order 2 consisting of the zero type and the type of $V(c)$ with $c \not\sim 1$.*

PROOF. Since $[k^* : (k^*)^2] = 2$, there exists only one type of the space of dimension 1. Hence by Proposition 4 it is enough to show that any anti-hermitian space V of dimension ≥ 2 contains an isotropic vector. Let $V = V(a_1, a_2)$. Then, in the above notations, we have $a_1 a_2 = n(\alpha_1) \cdot n(-\alpha_2) \sim 1$, so that by Lemma 1 there exists λ in \mathfrak{D}^* such that $H(x_1 \lambda + x_2) = \bar{\lambda} \alpha_1 \lambda + \alpha_2 = 0$.
 q. e. d.

LEMMA 2. *In Case (II), the mapping δ is an isomorphism from \mathfrak{I}^+ onto $k^*/(k^*)^2$.*

PROOF. Let $V = V(a_1, a_2)$. If $\delta(V) = a_1 a_2 \sim 1$, then V is shown to contain an isotropic vector just as in the proof of Theorem 2. This, combined with Theorem 1, proves that δ is injective on \mathfrak{I}^+ . On the other hand, since we are in Case (II), $k^*/(k^*)^2$ contains more than three elements. Hence, for any $c \in k^*$, we can find $a_1, a_2 \in k^*$ such that $a_i \not\sim 1$ ($i = 1, 2$) and $a_1 a_2 \sim c$. We have then $\delta(V(a_1, a_2)) = a_1 a_2 \sim c$. This proves that δ restricted on \mathfrak{I}^+ is surjective.
 q. e. d.

THEOREM 3. *In Case (II), the type of an anti-hermitian space V over \mathfrak{D} is completely determined by the parity of $\dim V$ and by the discriminant $\delta(V)$, which can be prescribed arbitrarily. The list of all the anisotropic anti-hermitian spaces V_0 over \mathfrak{D} is as follows:*

$\dim V_0$	$\delta(V_0)$
0	1
1	$c \not\sim 1$
2	$c \not\sim 1$
3	1

PROOF. The existence of V of dimension 1 with given $\delta(V) \not\sim 1$ is obvious and the corresponding statement for dimension 2 was shown in the proof of Lemma 2. The existence of V of dimension 3 with $\delta(V) = 1$ is shown as follows. Call V_1, V_2 respectively the spaces of dimension 1 and 2 with $\delta(V_1) = \delta(V_2)$, and put $V = V_1 + V_2$ (direct sum). Then we have $\delta(V) = \delta(V_1) \delta(V_2) \sim 1$. Therefore, since the maximal anisotropic subspace of V can not be of dimension 1, V itself must be anisotropic. Finally, if V, V' have the same parity and discriminant, then, the type $V - V'$ belonging to \mathfrak{I}^+ and having the

discriminant 1, we have $V \sim V'$ by Lemma 2.

q. e. d.

§ 3. **Maximal lattices in an anti-hermitian spaces over a p-adic quaternion algebra.**

3.1. In this section, k is a p-adic number field. We denote by \mathfrak{D} , $\mathfrak{P} = \Pi\mathfrak{D} = \mathfrak{D}\Pi$ the unique maximal order in \mathfrak{D} and the unique prime ideal in \mathfrak{D} , respectively, Π denoting a generator of \mathfrak{P} . Then any ideal \mathfrak{Q} in \mathfrak{D} (with respect to the maximal order \mathfrak{D}) is a power of \mathfrak{P} and thus two-sided and principal. $\mathfrak{o} = \mathfrak{D} \cap k$, $\mathfrak{p} = \mathfrak{P} \cap k$ are the ring of p-adic integers in k and the unique prime ideal in \mathfrak{o} , respectively; we may write $\mathfrak{p} = \pi\mathfrak{o}$, $\pi = \Pi^2$. For $\alpha \in \mathfrak{D}^*$ (resp. $a \in k^*$) we indicate that $\alpha\mathfrak{D} = \mathfrak{P}^m$ (resp. $a\mathfrak{o} = \mathfrak{p}^m$) by writing $\text{ord}_{\mathfrak{p}}\alpha = m$ (resp. $\text{ord}_{\mathfrak{p}}a = m$). In the following, we fix once for all an ideal $\mathfrak{Q} = \mathfrak{P}^m = \omega\mathfrak{D}$ in \mathfrak{D} and put $\mathfrak{Q}^- = \{\xi - \bar{\xi} \mid \xi \in \mathfrak{Q}\}$.

A subset M of an anti-hermitian space V over \mathfrak{D} is called a *lattice* in V if it is a right \mathfrak{D} -module with finite generators containing a basis of V over \mathfrak{D} . A lattice M is called \mathfrak{Q} -integral if we have

$$(9) \quad H(x) \in \mathfrak{Q}^-$$

for all $x \in M$. A lattice M is called *maximal \mathfrak{Q} -integral* if it is \mathfrak{Q} -integral and maximal in the class of lattices with this property.

PROPOSITION 6. *If M is a \mathfrak{Q} -integral lattice in V , we have*

$$(10) \quad \Phi(x, y) \in \mathfrak{Q}$$

for all $x, y \in M$.

PROOF. As is seen from the formula

$$H(x+y\lambda) - H(x) - H(y\lambda) = \Phi(x, y)\lambda - \bar{\lambda}\overline{\Phi(x, y)},$$

it is sufficient to show that the set \mathfrak{X} defined by

$$\mathfrak{X} = \{\xi \mid \xi \in \mathfrak{D}, \xi\lambda - \bar{\lambda}\bar{\xi} \in \mathfrak{Q}^-, \text{ for all } \lambda \in \mathfrak{D}\}$$

is contained in \mathfrak{Q} . It is clear that \mathfrak{X} is an ideal (with respect to \mathfrak{D}) containing \mathfrak{Q} . We shall first show that $\mathfrak{X} \cap k = \mathfrak{Q} \cap k$. In fact, if $\xi \in \mathfrak{X} \cap k$ we have $\xi\lambda - \bar{\lambda}\bar{\xi} = \xi(\lambda - \bar{\lambda}) \in \mathfrak{Q}^-$. As the residue class field $\mathfrak{D}/\mathfrak{P}$ is a quadratic extension of $\mathfrak{o}/\mathfrak{p}$, there exists $\lambda \in \mathfrak{D}$ such that $\lambda - \bar{\lambda}$ is a unit in \mathfrak{D} . Therefore, we have $\xi \in \mathfrak{Q}$, as desired. In case m is odd, this shows already that $\mathfrak{X} = \mathfrak{Q}$. If m is even, we may write $m = 2m'$, $\mathfrak{Q} = \pi^{m'}\mathfrak{D}$, and it suffices to show that $\pi^{m'}\Pi^{-1} \in \mathfrak{X}$. If this were not the case, we would have $\pi^{m'}\Pi^{-1}\lambda - \overline{\pi^{m'}\Pi^{-1}\lambda} \in \mathfrak{Q}^-$ for any $\lambda \in \mathfrak{D}$, which means (for $\lambda = 1$) that there exists an element a in k such that $a + \pi^{m'}\Pi^{-1} \in \mathfrak{Q}$. Since $\text{ord}_{\mathfrak{p}}a$ is even and $\text{ord}_{\mathfrak{p}}(\pi^{m'}\Pi^{-1})$ is odd, we must have $\pi^{m'}\Pi^{-1} \in \mathfrak{Q}$, which contradicts $\mathfrak{Q} = \pi^{m'}\mathfrak{D}$. q. e. d.

LEMMA 3. *Let M be an \mathfrak{Q} -submodule in V generated by a subset S of V .*

Then, in order that M be a \mathfrak{D} -integral lattice, it is necessary and sufficient that the following conditions be satisfied:

- 1) S contains a basis of V over \mathfrak{D} ,
- 2) $H(x) \in \mathfrak{D}^-$, $\Phi(x, y) \in \mathfrak{D}$ for all $x, y \in S$.

This is an immediate consequence of the formulas (4), (5) and Prop. 6.

3.2. THEOREM 4. *If V is anisotropic, the subset M of V defined by*

$$(11) \quad M = \{x \in V \mid H(x) \in \mathfrak{D}^-\}$$

is a \mathfrak{D} -integral lattice in V . (Hence M is a unique maximal \mathfrak{D} -integral lattice in V .)

PROOF. By Lemma 3 it is enough to show that $H(x), H(y) \in \mathfrak{D}^-$ imply $\Phi(x, y) \in \mathfrak{D}$. Suppose that $\beta = \Phi(x, y) \notin \mathfrak{D}$. Then, putting $H(x) = \xi - \bar{\xi}$, $H(y) = \eta - \bar{\eta}$ with $\xi, \eta \in \mathfrak{D}$, we have

$$H(x+y\lambda) = (\xi - \bar{\xi}) + (\beta\lambda - \bar{\beta}\bar{\lambda}) + \bar{\lambda}(\eta - \bar{\eta})\lambda.$$

Making a substitution $\lambda = -\beta^{-1}\xi + \lambda_1$, we get

$$H(x+y\lambda) = (\xi_1 - \bar{\xi}_1) + (\beta_1\lambda_1 - \bar{\beta}_1\bar{\lambda}_1) + \bar{\lambda}_1(\eta_1 - \bar{\eta}_1)\lambda_1,$$

where

$$\xi_1 = \bar{\beta}^{-1}\bar{\xi}\eta\beta^{-1}\xi,$$

$$\beta_1 = \beta - \bar{\beta}^{-1}\bar{\xi}(\eta - \bar{\eta}) \equiv \beta \pmod{\mathfrak{D}}.$$

Hence if we define $\xi_i, \beta_i, \lambda_i$ successively by

$$\xi_i = \bar{\beta}_{i-1}^{-1}\bar{\xi}_{i-1}\eta\beta_{i-1}^{-1}\xi_{i-1},$$

$$\beta_i = \beta_{i-1} - \bar{\beta}_{i-1}^{-1}\bar{\xi}_{i-1}(\eta - \bar{\eta}),$$

$$\lambda_i = \lambda_{i-1} + \beta_{i-1}^{-1}\xi_{i-1},$$

we have

$$H(x+y\lambda) = (\xi_i - \bar{\xi}_i) + (\beta_i\lambda_i - \bar{\beta}_i\bar{\lambda}_i) + \bar{\lambda}_i(\eta - \bar{\eta})\lambda_i,$$

$$\xi_i \in \mathfrak{D}\mathfrak{P}^{2i}, \quad \beta_i \equiv \beta \pmod{\mathfrak{D}}.$$

Hence putting $\lambda_i = 0$, we get

$$H(x+y\mu_i) = \xi_i - \bar{\xi}_i,$$

where $\mu_i = -\beta^{-1}\xi - \dots - \beta_{i-1}^{-1}\xi_{i-1}$. Making i tend to infinity, we have $\xi_i \rightarrow 0$, $\mu_i \rightarrow \mu \in \mathfrak{P}$, so that $H(x+y\mu) = 0$. Hence by the assumption, $x = -y\mu$. But then we get $\beta = \Phi(x, y) = -\bar{\mu}H(y) \in \mathfrak{D}$, which is a contradiction. q. e. d.

THEOREM 5. *Let V be an anti-hermitian space over \mathfrak{D} with index ν and M a maximal \mathfrak{D} -integral lattice in V . Then M can be decomposed in the following form:*

$$(12) \quad M = M_0 + \sum_{i=1}^{\nu} \{e_i, e_i'\} \quad (\text{orthogonal sum}),$$

where M_0 is the unique maximal \mathfrak{D} -integral lattice in a maximal anisotropic subspace V_0 of V and the e_i, e_i' are such that

$$H(e_i) = H(e_i') = 0, \quad \Phi(e_i, e_i') = \omega,$$

and where $\{e_i, e_i'\}_{\mathfrak{D}}$ denotes the \mathfrak{D} -submodule generated by $\{e_i, e_i'\}$. Conversely, any lattice decomposable in the form (25) with M_0, e_i, e_i' ($1 \leq i \leq \nu$) as described above is a maximal \mathfrak{D} -integral lattice in V .

PROOF. We prove the Theorem by induction on ν . If $\nu = 0$, it is trivial. Assume $\nu > 0$. Let e_1 be any 'primitive' isotropic vector in M . (That $x \in M$ is primitive means that $x\Pi^{-1} \notin M$.) Consider the set

$$\{\Phi(e_1, x) \mid x \in M\}.$$

By Proposition 6 it is clear that this is an ideal contained in \mathfrak{D} . We shall show that this is actually equal to \mathfrak{D} . Let x_1 be an element in M such that $\Phi(e_1, x_1)$ generates this ideal. For any $x \in M$, putting $\alpha = \Phi(e_1, x_1)^{-1} \Phi(e_1, x) \in \mathfrak{D}$, we have $x = x' + x_1\alpha$, $\Phi(e_1, x') = 0$. This shows that $M = (M \cap \{e_1\}_{\mathfrak{D}}^{\perp}) + \{x_1\}_{\mathfrak{D}}$. Hence, if $\text{ord}_{\mathfrak{p}} \Phi(e_1, x_1) > m$, the set $S = M \cup \{e_1\Pi^{-1}\}$ would satisfy the condition of Lemma 3 and thus generate a \mathfrak{D} -integral lattice containing M and $e_1\Pi^{-1}$, contradicting the maximality of M . This proves our assertion. It follows that we may choose x_1 in such a way that $\Phi(e_1, x_1) = \omega$. Put $H(x_1) = \xi_1 - \bar{\xi}_1$. Then, putting $e_1' = e_1\beta + x_1$, $\beta = \bar{\omega}^{-1}\xi_1 \in \mathfrak{D}$, we get $H(e_1') = \bar{\beta}\omega - \omega\beta + H(x_1) = 0$. Thus we have proved that there exists in M a pair of isotropic vectors e_1, e_1' such that $\Phi(e_1, e_1') = \omega$. Now, let $\{e_1, e_1'\}$ be any such pair and put

$$V' = \{e_1, e_1'\}_{\mathfrak{D}}^{\perp}, \quad M' = M \cap V'.$$

Then, as M is maximal \mathfrak{D} -integral in V , so is M' in V' . Any $x \in V$ can be written uniquely in the form

$$x = e_1\gamma + e_1'\delta + x' \quad \text{with } x' \in V',$$

where we have $\gamma = -\bar{\omega}^{-1}\Phi(e_1', x)$, $\delta = \omega^{-1}\Phi(e_1, x)$. Hence $x \in M$, if and only if $\alpha, \beta \in \mathfrak{D}$, $x' \in M'$. Thus we have

$$M = \{e_1, e_1'\}_{\mathfrak{D}} + M' \quad (\text{orthogonal sum}),$$

which proves, by the induction assumption on M' , that M is decomposed in the form (12). Conversely, if M is of the form (12), M is a \mathfrak{D} -integral lattice by Lemma 3 and $M' = M \cap V'$ is a maximal \mathfrak{D} -integral lattice in V' by the induction assumption. If x is any element contained in a \mathfrak{D} -integral lattice \tilde{M} containing M , we get, in the above notation, $\gamma, \delta \in \mathfrak{D}$ so that x' is in a \mathfrak{D} -integral lattice $\tilde{M} \cap V'$ containing M' , hence in M' itself by the maximality of M' . Therefore we have $x \in M$, proving the maximality of M . This completes our proof by induction.

REMARK. From the above proof, we note that as e_1 we may take any

primitive isotropic vector in M and that as $\{e_1, e_1'\}$ we may take any pair of isotropic vectors in M satisfying the relation $\Phi(e_1, e_1') = \omega$. We call a decomposition of M of the form (12) a *Witt decomposition* of M . By Proposition 4 and Theorem 4, it is clear that the Witt decomposition of M is unique up to an automorphism of M (i.e. an automorphism of the anti-hermitian space V leaving M fixed). In particular, it follows from what we have stated above that any two primitive isotropic vectors (resp. any two pairs of isotropic vectors satisfying the above condition) are mutually conjugate with respect to the automorphisms of M .

3.3. By a *similitude* of the anti-hermitian space V over \mathfrak{D} we mean a linear transformation ρ of V over \mathfrak{D} such that

$$(13) \quad H(\rho(x)) = aH(x)$$

for all $x \in V$, a denoting an element in k^* depending only on ρ , called the ‘multiplicator’ of ρ . If ρ is a similitude of V with multiplicator a , we have from Proposition 1

$$(14) \quad \Phi(\rho(x), \rho(y)) = a\Phi(x, y)$$

for all $x, y \in V$.

We shall now determine the general form of a similitude of V leaving fixed an isotropic line.

LEMMA 4. Let $\{e_1, e_1'\}$ be a pair of isotropic vectors in V such that $\Phi(e_1, e_1') = \omega$ and let $V' = \{e_1, e_1'\}^\perp_{\mathfrak{D}}$. Then, for any similitude ρ of V with multiplicator a leaving $\{e_1\}_{\mathfrak{D}}$ invariant, we have

$$(15) \quad \begin{cases} \rho(e_1) = e_1\alpha, \\ \rho(e_1') = e_1\gamma + e_1'a\omega^{-1}\bar{\alpha}^{-1}\omega + \rho'(x_0), \\ \rho(x') = e_1\xi + \rho'(x'), \quad \xi = \alpha\bar{\omega}^{-1}\Phi(x_0, x') \quad \text{for } x' \in V', \end{cases}$$

where $\alpha, \gamma \in \mathfrak{D}$, $x_0 \in V'$ satisfying the relation

$$(16) \quad H(x_0) = \bar{\omega}\alpha^{-1}\gamma - \overline{\alpha^{-1}\gamma}\omega,$$

and where ρ' is a similitude of V' with multiplicator a . Conversely, for any $\alpha, \gamma \in \mathfrak{D}$, $x_0 \in V'$ and ρ' satisfying the above conditions, the linear transformation ρ of V over \mathfrak{D} defined by (15) is a similitude with multiplicator a .

PROOF. Let ρ be a similitude of V with multiplicator a such that $\rho(e_1) = e_1\alpha$ and put

$$\begin{aligned} \rho(e_1') &= e_1\gamma + e_1'\delta + y_0, \\ \rho(x') &= e_1\xi + e_1'\eta + \rho'(x') \quad \text{for } x' \in V' \end{aligned}$$

with $\gamma, \delta, \xi, \eta \in \mathfrak{D}$, $y_0, \rho'(x') \in V'$. Then, from $\Phi(\rho(e_1), \rho(e_1')) = a\Phi(e_1, e_1') = a\omega$, we obtain $\delta = a\omega^{-1}\bar{\alpha}^{-1}\omega$. From $\Phi(\rho(e_1), \rho(x')) = a\Phi(e_1, x') = 0$, we obtain $\eta = 0$.

From $H(\rho(e_1')) = aH(e_1') = 0$, we obtain $\bar{\gamma}\omega\delta - \overline{\omega\delta}\gamma + H(y_0) = 0$, i. e. $H(y_0) = a(\overline{\omega\alpha^{-1}\gamma} - \overline{\alpha^{-1}\gamma}\omega)$. From $\Phi(\rho(e_1'), \rho(x')) = a\Phi(e_1', x') = 0$, we obtain $-\overline{\omega\delta}\xi + \Phi(y_0, \rho'(x')) = 0$, i. e. $\xi = a^{-1}\alpha\overline{\omega^{-1}}\Phi(y_0, \rho'(x'))$. From $H(\rho(x')) = aH(x')$, we see that ρ' is a similitude with multiplier a (in particular, ρ' is non-singular). Putting $x_0 = \rho'^{-1}(y_0)$, we obtain (15), (16). The converse is clear. q. e. d.

LEMMA 5. *The notations being as in Lemma 4, let M be a maximal \mathfrak{D} -integral lattice in V containing e_1, e_1' and put $M' = M \cap V'$. Then, for a similitude ρ of V with multiplier a given by (15), we have $\rho(M) \subset M\alpha$, if and only if the following conditions are satisfied:*

$$(17) \quad \begin{aligned} a &\in n(\alpha)\mathfrak{D}, & \gamma &\in \alpha\mathfrak{D}, \\ x_0 &\in M', & \rho(M') &\subset M'\alpha. \end{aligned}$$

PROOF. As in the proof of Theorem 5, we have the direct decomposition

$$M = \{e_1, e_1'\}_{\mathfrak{D}} + M'.$$

Hence, if $\rho(M) \subset M\alpha$, we obtain from (15)

$$\begin{aligned} \gamma &\in \alpha\mathfrak{D}, & a\omega^{-1}\bar{\alpha}^{-1}\omega &\in \alpha\mathfrak{D}, & \rho'(x_0) &\in M'\alpha, \\ \xi &\in \alpha\mathfrak{D}, & \rho'(x') &\in M'\alpha & \text{for } x' &\in M', \end{aligned}$$

whence we get $a \in n(\alpha)\mathfrak{D}$, $\rho'(M') \subset M'\alpha$. Moreover we obtain from (15), (16)

$$\begin{aligned} \Phi(x_0, x') &= \overline{\omega\alpha^{-1}}\xi \in \mathfrak{D} & \text{for } x' &= M', \\ H(x_0) &= \overline{\omega\alpha^{-1}}\gamma - \overline{\alpha^{-1}\gamma}\omega \in \mathfrak{D}^-. \end{aligned}$$

Hence, by Lemma 3 and by the maximality of M' we get $x_0 \in M'$. The converse is clear. q. e. d.

LEMMA 6. *Any maximal \mathfrak{D} -integral lattice M of index > 0 is generated by isotropic vectors contained in M .*

PROOF. Take a pair of isotropic vectors e_1, e_1' in M such that $\Phi(e_1, e_1') = \omega$. Then any $x \in M$ can be written in the following form:

$$x = e_1\alpha + e_1'\beta + x', \quad \text{with } \alpha, \beta \in \mathfrak{D}, x' \in M'.$$

Let $H(x') = \xi' - \bar{\xi}'$ with $\xi' \in \mathfrak{D}$ and put $\gamma = \omega^{-1}\xi' \in \mathfrak{D}$. Then

$$H(x' + e_1 - e_1'\gamma) = H(x') - \omega\gamma + \overline{\omega\gamma} = 0.$$

Therefore, M is generated over \mathfrak{D} by isotropic vectors contained in M . q. e. d.

THEOREM 6. *Let M be a maximal \mathfrak{D} -integral lattice in V . ($\mathfrak{D} = \Pi^m\mathfrak{D}$). Then, for any similitude ρ of V with multiplier a , there exists an automorphism υ of M , a Witt decomposition*

$$M = M_0 + \sum_{i=1}^{\nu} \{e_i, e_i'\} \quad (\Phi(e_i, e_i') = \Pi^m)$$

of M and a system of rational integers r_i ($1 \leq i \leq \nu$) such that

$$(18) \quad \rho\nu(e_i) = e_i\Pi^{r_i}, \quad \rho\nu(e_{i'}) = e_{i'}a\bar{\Pi}^{-r_i} \quad (1 \leq i \leq \nu),$$

$$(19) \quad r_1 \leq r_2 \leq \dots \leq r_\nu \leq \text{ord}_p a.$$

PROOF. The Theorem being vacant for $\nu = 0$, we assume that $\nu > 0$ and proceed by induction on ν . Since $V = \bigcup_{r \in \mathbb{Z}} M\Pi^r$, there exists the largest integer r_1 such that $M\Pi^{r_1} \supset \rho(M)$. Then by Lemma 6 there exists a primitive isotropic vector e_1 in M which is contained in $\rho(M)\Pi^{-r_1}$. Then e_1 is also primitive in $\rho(M)\Pi^{-r_1}$, so that $\rho^{-1}(e_1)\Pi^{r_1}$ is primitive in M . Hence, by the remark after Theorem 5, there exists an automorphism ν of M such that $\nu(e_1) = \rho^{-1}(e_1)\Pi^{r_1}$ or $\rho\nu(e_1) = e_1\Pi^{r_1}$. Taking any isotropic vector $e_{1'}$ in M such that $\Phi(e_1, e_{1'}) = \Pi^m$ and applying Lemma 4, 5 to $\rho\nu$ with $\alpha = \Pi^{r_1}$, $\omega = \Pi^m$, we get

$$\rho\nu(e_{1'}) = e_1\gamma + e_{1'}a\bar{\Pi}^{-r_1} + \rho'(x_0),$$

where γ, \dots satisfy the condition (17); in particular, we have $\text{ord}_p a \geq r_1$. Hence, replacing $e_{1'}$ by $e_{1'} - e_1(\alpha^{-1}\gamma - \bar{\omega}^{-1}H(x_0)) - x_0 \in M$, we get from (15), (16)

$$H(e_{1'}) = 0, \quad \Phi(e_1, e_{1'}) = \Pi^m,$$

$$\rho\nu(e_{1'}) = e_{1'}a\bar{\Pi}^{-r_1}.$$

Since $\rho\nu(M') \subset M'\Pi^{r_1}$, we can apply the induction assumption on the restriction of $\rho\nu$ on M' , and in doing so, we get $r_1 \leq r_2$. This completes our proof by induction on ν .

3.4. We now fix a maximal \mathfrak{O} -integral lattice M in V and put as follows:

G = group of all automorphisms of V ,

\tilde{G} = group of all similitudes of V ,

U = group of all automorphisms of M (viz. all automorphisms of V leaving M fixed),

\tilde{U} = group of all similitudes of V leaving M fixed,

\mathcal{M} = group of all multipliers of the similitudes belonging to \tilde{G} .

With their natural topology, G, \tilde{G} are locally compact topological groups, U, \tilde{U} are open compact subgroups of G, \tilde{G} , respectively, and we have $U = \tilde{U} \cap G$; we have also a canonical homomorphism from \tilde{G} onto \mathcal{M} whose kernel is G .

LEMMA 7. Let W_1, W_2 be two non-isotropic subspaces of V (i.e. such that $W_i \cap W_i^\perp = \{0\}$). If there exists $\rho \in \tilde{G}$ such that $\rho(W_1) = W_2$, then there exists $\rho' \in G$ such that $\rho'(W_1) = W_2$.

PROOF. If a is the multiplier of ρ and if r is the common dimension of W_1 and W_2 , we have $\delta(W_2) = a^{2r} \delta(W_1) \sim \delta(W_1)$. Hence, by Theorem 3, W_1, W_2 are isomorphic anti-hermitian spaces over \mathfrak{D} , and the Lemma follows from Proposition 3. q. e. d.

It follows, in particular, that for any $\rho \in \tilde{G}$ there exists $\rho' \in G$ such that $\rho'^{-1}\rho$ leaves invariant a given Witt decomposition of V . Therefore, if V is

$\neq 1$, \mathcal{M} coincides with the group of all multipliers of the similitude of a maximal anisotropic subspace V_0 of V . In this case, call a_0 an element of \mathcal{M} such that, for any $a \in \mathcal{M}$, $\text{ord}_p a$ is a rational integral multiple of $\text{ord}_p a_0$, and call ρ_0 a similitude of V_0 with multiplier a_0 . In case $V \sim 1$, we have clearly $\mathcal{M} = k^*$, and so we put $a_0 = \pi$.

Now let us fix furthermore a Witt decomposition

$$M = M_0 + \sum_{i=1}^{\nu} \{e_i, e_i'\}_{\mathfrak{D}} \quad (\Phi(e_i, e_i') = \Pi^m)$$

of M ; any other Witt decomposition of M is then given by

$$M = v(M_0) + \sum_{i=1}^{\nu} \{v(e_i), v(e_i')\}_{\mathfrak{D}} \quad \text{with } v \in U.$$

Call \check{D} the group of all linear transformations of V of the form

$$(20) \quad \begin{cases} \rho(e_i) = e_i \Pi^{r_i}, \\ \rho(e_i') = e_i' a_0^{r_i} \bar{\Pi}^{-r_i} \quad (1 \leq i \leq \nu), \\ \rho(x) = \rho_0^{r_0}(x) \quad \text{for } x \in V_0, \end{cases}$$

where a_0, ρ_0 are as defined above. We denote the transformation (20) by $\delta(r_0, r_1, \dots, r_\nu)$, which is clearly a similitude of V with multiplier a_0 . Put

$$D = \{\delta(0, r_1, \dots, r_\nu) \mid r_i \in \mathbf{Z}\} = \check{D} \cap G.$$

Furthermore, denote by N the group of all automorphisms ρ of V of the following form:

$$(21) \quad \begin{cases} \rho(e_i) = \sum_{j < i} e_j \alpha_{ji} + e_i, \\ \rho(e_i') = \sum_{j=1}^{\nu} e_j \beta_{ji} + e_i' + \sum_{j > i} e_j' \gamma_{ji} + y_i \quad (y_i \in V_0), \\ \rho(x) = \sum_{j=1}^{\nu} e_j \delta_j + x \quad \text{for } x \in V_0. \end{cases}$$

Then we obtain the following theorem:

THEOREM 7. *In the above notations, we have*

$$(22) \quad \begin{aligned} \check{G} &= \check{U} \check{D} \check{U}, & G &= U D U, \\ \check{G} &= \check{U} \cdot \check{D} N = \check{D} N \cdot \check{U}, & G &= U \cdot D N = D N \cdot U. \end{aligned}$$

PROOF. Let ρ be any similitude of V . Then, by Theorem 6, there exist $v, v' \in U$ such that

$$\begin{aligned} \rho v v'(e_i) &= v'(e_i) \Pi^{r_i}, \\ \rho v v'(e_i') &= v'(e_i') a \bar{\Pi}^{-r_i} \quad (1 \leq i \leq \nu). \end{aligned}$$

Hence, if $\text{ord}_p a = r_0 \cdot \text{ord}_p a_0$, $v'' = \delta(r_0, r_1, \dots, r_\nu)^{-1} v'^{-1} \rho v v'$ is a similitude of V with a multiplier which is a unit of \mathfrak{D} , leaving all $\{e_i, e_i'\}_{\mathfrak{D}}$ fixed. Hence v'' leaves V_0 fixed and consequently, by Theorem 4, v'' leaves also M_0 fixed.

Thus $v'' \in \tilde{U}$ and we have $\tilde{G} = \tilde{U}\tilde{D}\tilde{U}$. If $\rho \in G$, we have by the same reason: $v'' = \delta(0, r_1, \dots, r_\nu)^{-1}v'^{-1}\rho vv' \in U$, so that $G = UDU$.

Next we prove (23) by induction on ν . If $\nu = 0$, we have $N = \{1\}$ and the proof is already contained in the above argument. Let $\nu > 0$ and let ρ be any similitude of V with multiplier a . Take r_1 such that $\rho(e_1)\Pi^{-r_1}$ is primitive in M . Then there exists $v_1 \in U$ such that $v_1^{-1}(e) = \rho(e_1)\Pi^{-r_1}$. From Lemma 4, we have

$$\begin{cases} v_1\rho(e_1) = e_1\Pi^{r_1}, \\ v_1\rho(e_1') = e_1 * + e_1'a\Pi^{-r_1} + \tau'(x_0), \\ v_1\rho(x') = e_1 * + \tau'(x') \quad \text{for } x' \in V' = \{e_1, e_1'\}_{\mathbb{Q}}^{\perp}, \end{cases}$$

where $x_0 \in V'$ and τ' is a similitude of V' with multiplier a . Hence, if we denote by τ a similitude of V defined by

$$\begin{cases} \tau(e_1) = e_1\Pi^{r_1}, \\ \tau(e_1') = e_1'a\Pi^{-r_1}, \\ \tau(x') = \tau'(x') \quad \text{for } x' \in V', \end{cases}$$

we have

$$\begin{cases} \tau^{-1}v_1\rho(e_1) = e_1, \\ \tau^{-1}v_1\rho(e_1') = e_1 * + e_1' + x_0, \\ \tau^{-1}v_1\rho(x') = e_1 * + x', \end{cases}$$

which is an automorphism belonging to N . Applying the induction assumption on τ' , we see that $\tau \in \tilde{U}\cdot\tilde{D}N$. Therefore $\rho \in \tilde{U}\cdot\tilde{D}N$, as desired. If $\rho \in G$, we have $\tau \in U\cdot DN$ and so $\rho \in U\cdot DN$. Since \tilde{D} normalizes N , we have $\tilde{D}N = N\tilde{D}$, $DN = ND$, so that we have $\tilde{G} = N\cdot\tilde{D}\cdot\tilde{U} = \tilde{D}N\cdot\tilde{U}$, $G = N\cdot D\cdot U = DN\cdot U$.
q. e. d.

REMARK. It follows easily from (22) that \tilde{U} (resp. U) is a maximal compact subgroup of \tilde{G} (resp. G) and from (23) that N is a maximal 'unipotent' subgroup of \tilde{G} and G (viewed as linear algebraic groups over k).

Bibliography

- [1] N. Bourbaki, *Eléments de mathématique*, Livre II Algèbre, Chap. 9, Formes sesquilinéaires et formes quadratiques. Herman, 1959.
- [2] J. Dieudonné, *La géométrie des groupes classiques*. Ergebnisse der Math. und ihre Grenzgebiete. Springer, 1955.
- [3] K. G. Ramanathan, Quadratic forms over involutorial division algebras, *J. Ind. Math. Soc.*, 20 (1956), 227-257.

NOTE: It was noticed in the course of the proof reading that the contents of § 2 of this paper had already been obtained in [3].