HIROSHIMA MATH. J.
11 (1981), 443–456

Kaplansky's radical and Hilbert Theorem 90

Daiji KIJIMA and Mieo NISHI

(Received January 19, 1981)

§ 1. Introduction

In [7], Kaplansky introduced the notion of the radical for a field F as the subgroup $R(F)=\{a \in \dot{F};\ D_F\langle 1, -a\rangle=\dot{F}\}$ of the multiplicative group $\dot{F}=F-\{0\}$, where $D_F\langle 1, -a\rangle$ is the subgroup of all elements of $\dot{F}$ which are represented by a 1-fold Pfister form $\langle 1, -a\rangle$. An interesting result concerning the radical $R(F)$ was given in [2] as follows: Let $\varphi=\langle a_1,\dots, a_n\rangle$, $n\geqq 2$, be a quadratic form over a field F and let $r_1,\dots, r_n$ be elements of $R(F)$. Then $D_F(\varphi)=D_F\langle r_1a_1,\dots, r_na_n\rangle$. This fact suggests us that the radical would play a rôle of the group $\dot{F}^2$ to some extent.

On the other hand, in case when K is a quadratic extension field of F, Hilbert Theorem 90 says that $N^{-1}(\dot{F}^2)=\dot{F}\cdot\dot{K}^2$, where $N: \dot{K}\to\dot{F}$ is the norm map. Replacing groups of squares $\dot{F}^2$ and $\dot{K}^2$ by radicals $R(F)$ and $R(K)$, we can set up a conjecture: $N^{-1}(R(F))=\dot{F}\cdot R(K)$. This conjecture is valid if F is a pre-Hilbert field and $|\dot{F}/R(F)|<\infty$ ([5]). In case when $|\dot{F}/R(F)|=\infty$, we shall introduce topologies on the groups $\dot{F}/\dot{F}^2$, $\dot{K}/\dot{K}^2$ so that the norm map $N: \dot{F}/\dot{F}^2\to\dot{K}/\dot{K}^2$ is continuous and $R(F)$ is closed. Therefore the conjecture, which we call '*H-conjecture*', must be of the form: $N^{-1}(R(F))=(\dot{F}\cdot R(K))^-$, where the bar means the topological closure of $\dot{F}\cdot R(K)$. In case when $\dot{F}/R(F)$ is finite, the topology can be neglected.

The main purpose of this paper is to show that if F is a pre-Hilbert field and $K=F(\sqrt{a})$, $a\notin R(F)$, then $N^{-1}(R(F))=(\dot{F}\cdot R(K))^-$.

In the forthcoming paper, part II, we shall discuss the case of a quadratic extension $K=F(\sqrt{a})$, $a\in R(F)$, where F is not necessarily assumed to be a pre-Hilbert field.

§ 2. Definitions and preliminaries

In this section, we set up the definitions and notations to be used in this paper, and state some basic facts about quadratic forms.

By a field F, we shall always mean a field of characteristic different from two. Let $\dot{F}$ denote the multiplicative group of F. Diagonalized quadratic forms over F are denoted by $\varphi_F=\langle x_1,\dots, x_n\rangle$, and we define $D_F(\varphi)=\{a\in\dot{F}\mid\varphi_F \text{ represents } a\}$. If $D_F(\varphi)=\dot{F}$, φ is called universal. To simplify the notation, we denote $D_F(\langle x_1,$

$\dots, x_n\rangle)$ by $D_F\langle x_1,\dots,x_n\rangle$. A subgroup of central importance throughout will be the radical $R(F)=\{x\in \dot{F} \mid D_F\langle 1, -x\rangle=\dot{F}\}$. Another formulation is $R(F)=\bigcap_{x\in\dot{F}} D_F\langle 1, -x\rangle$. The fields with a unique nonsplit quaternion algebra were called pre-Hilbert fields by L. Berman [1], instead of generalized Hilbert fields. We also use the term pre-Hilbert.

The following propositions are stated in [2], [3] respectively.

PROPOSITION 2.1. *Let φ be a quadratic form over a field F with diagonalization $\langle a_1,\dots,a_n\rangle$, $n\geqq 2$. And let $r_1,\dots,r_n\in R(F)$. Then $D(\varphi)=\langle r_1a_1,\dots,r_na_n\rangle$.*

PROPOSITION 2.2. *Let F be a pre-Hilbert field. For $a, b\in\dot{F}$,*

$$D_F\langle 1, -a\rangle = D_F\langle 1, -b\rangle \text{ if and only if } ab\in R(F).$$

REMARK. The if part is valid for any field from Proposition 2.1.

In [2], Proposition 2.1 is stated under the assumption that F is a non-formally real field, and in [3] Proposition 2.2 is stated under the assumption that F is a non-formally real field with $|\dot{F}/F^2|<\infty$. However, Proposition 2.1 is valid for any field, and Proposition 2.2 is valid for any pre-Hilbert field.

PROPOSITION 2.3. *A field F is a pre-Hilbert field if and only if $D_F\langle 1, -b\rangle$ has index 1 or 2 for every $b\in\dot{F}$ and has 2 for at least one $b\in\dot{F}$.*

The if part of this well known result was first observed by Kaplansky [7].
The following three lemmas will be used frequently in this paper.

LEMMA 2.4 ([4], Lemma in § 2). *Let F be a field. Then for any $a, b\in\dot{F}$,*

$$D_F\langle 1, -a\rangle \cap D_F\langle 1, -b\rangle \subseteq D_F\langle 1, -ab\rangle.$$

LEMMA 2.5 ([1], Lemma 3.5). *Let F be a field, and $K=F(\sqrt{a})$, $a\in\dot{F}-\dot{F}^2$. If $x\in\dot{F}$, then*

$$D_K\langle 1, -x\rangle \cap \dot{F} = D_F\langle 1, -x\rangle\cdot D_F\langle 1, -ax\rangle.$$

LEMMA 2.6 ([6], Norm Principle 2.13). *Let φ be a form over F, and $K=F(\sqrt{a})$, $a\in\dot{F}-\dot{F}^2$. Let $N=N_{K/F}$ denote the norm map from K to F, and $x\in\dot{K}$. Then, $N(x)\in D_F(\varphi)\cdot D_F(\varphi)$ if and only if $x\in\dot{F}\cdot D_K(\varphi)$.*

In particular, if φ is a 1-fold Pfister form $\langle 1, -b\rangle$, $D_F(\varphi)$ is a subgroup of $\dot{F}$. Then Norm Principle says that $N(x)\in D_F\langle 1, -b\rangle$ if and only if $x\in\dot{F}\cdot D_K\langle 1, -b\rangle$, i.e. $N^{-1}(D_F\langle 1, -b\rangle)=\dot{F}\cdot D_K\langle 1, -b\rangle$.

Let A be a set. Then we denote the cardinality of A by $|A|$. Let A_i, $i\in I$, be a family of subsets in A. We say that the intersection $\bigcap_{i\in I} A_i$, is irredundant if $A_i \not\supseteq \bigcap_{j\neq i} A_j$ for every $i\in I$. Let G be a group and A be a subset of G. Then we denote by $\langle A\rangle$ the subgroup of G generated by the set A.

§3. Properties of a pre-Hilbert field

In this section, we investigate some characterizations and properties of a pre-Hilbert field.

LEMMA 3.1. *Let V be an n-dimensional vector space over $\boldsymbol{Z}_2=\boldsymbol{Z}/2\boldsymbol{Z}$. Then the number of $(n-1)$-dimensional subspaces of V is 2^n-1.*

The proof is elementary and omitted.

DEFINITION 3.2. *We put $U_F=\dot{F}/R(F)$. A subgroup A of U_F is called a P-group if there exists an $a\in\dot{F}-R(F)$ such that $A=D_F\langle 1, -a\rangle/R(F)$.*

PROPOSITION 3.3. *Let F be a field with $\dim_{\boldsymbol{Z}_2}U_F=n<\infty$. Then the following statements are equivalent:*

(1) *F is a pre-Hilbert field.*

(2) *$n\geqq 1$ and any $(n-1)$-dimensional subspace of U_F is a P-group.*

PROOF. (1)⇒(2): Let L be the set of P-groups in U_F, and let f be the map from $\dot{F}-R(F)$ to L, defined by $f(a)=D_F\langle 1, -a\rangle/R(F)$. Then, using Proposition 2.2, we have the induced map $\bar{f}$ from the set $U_F-\{1\}$ to L; namely, $\bar{f}(\bar{a})=f(a)$, where $\bar{a}$ means a mod $R(F)$. The map $\bar{f}$ is injective. The surjectivity of $\bar{f}$ is clear, and so $|L|=2^n-1$. Now Lemma 3.1 and Proposition 2.3 show that any $(n-1)$-dimensional subspace of U_F is a P-groups.

(2)⇒(1): In this case, $\bar{f}$ is well-defined and surjective from Remark of Proposition 2.2. So $|L|\leqq 2^n-1$. The statement (2) and Lemma 3.1 imply that any P-group has index 2 in U_F. Now apply Proposition 2.3. q.e.d.

In order to analyse some conditions which characterize a pre-Hilbert field F with $|U_F|<\infty$, we need some lemmas on a vector space over $\boldsymbol{Z}_2$.

LEMMA 3.4. *Let V be a vector space over $\boldsymbol{Z}_2$, and W_i $(i=1,\dots, t)$ be subspaces of index 2 in V. If $\bigcap_{1\leqq i\leqq t}W_i$ is irredundant, then $V/\cap W_i$ is a t-dimensional vector space.*

PROOF. We use induction on t. By the induction hypothesis, we can see that $V/\bigcap_{1\leqq i\leqq t-1}W_i$, is $(t-1)$-dimensional. Since $W_t\not\supseteq\bigcap_{1\leqq i\leqq t-1}W_i$, we have $W_t+\bigcap_{1\leqq i\leqq t-1}W_i=V$. So $V/W_t\cong\bigcap_{1\leqq i\leqq t-1}W_i/\bigcap_{1\leqq j\leqq t}W_j$ is a 1-dimensional vector space. q.e.d.

LEMMA 3.5. *Let V be an n-dimensional vector space over $\boldsymbol{Z}_2$, and W_i $(i=1,\dots, t)$ be subspaces of V such that for any $j=2,\dots, t$, $\bigcap_{1\leqq i\leqq j-1}W_i\not\subseteq W_j$.*

If $\dim V/W_1 \geqq 2$, *then* $t<n$.

LEMMA 3.6. *Let* V *be a vector space over* $\mathbf{Z}_2$, *and* W_i $(i=1,\dots, t)$ *be subspaces of* V such that $\cap_{1\leqq i\leqq t} W_i$ *is irredundant. If* $\dim V/\cap_{1\leqq i\leqq t} W_i=t$, *then for any* i, $\dim V/W_i=1$.

The proofs of these two lemmas are easy and omitted.

From now on, for a subset B of F, $\cap_{b\in B} D_F\langle 1, -b\rangle$ will be sometimes denoted by $I_F(B)$, or simply by $I(B)$ if there is no fear of confusion. For a subset C of U_F, we also write $I(C)=I_F(C)=\cap_{d\in D} D_F\langle 1, -d\rangle$ where D is the inverse image of C by the canonical homomorphism φ: $\dot{F}\to U_F=\dot{F}/R(F)$. If $C=\{x\}$, $I(x)$ stands for $I(\{x\})$. By Remark of Proposition 2.2, for any $a\in\varphi^{-1}(x)$, $I(x)=I(a)=D_F\langle 1, -a\rangle$.

PROPOSITION 3.7. *For any field* F *and* $x\in U_F$, $B\subseteq U_F$, *the following statements hold*:

(1) *If* $x\in\langle B\rangle$, *then* $I(x)\supseteq I(B)$.

(2) *If* $\langle B\rangle=U$, *then* $I(B)=R(F)$.

(3) *If* $\cap_{x\in B} I(x)$ *is irredundant, then* B *is linearly independent in* U_F.

PROOF. (1) Since $x\in\langle B\rangle$, there exist $y_1,\dots, y_n\in B$ such that $x=y_1\cdot\cdots\cdot y_n$. Then by Lemma 2.4, $I(x)\supseteq\cap_{1\leqq i\leqq n} I(y_i)\supseteq I(B)$.

(2) Using (1), we have $I(B)=I(U_F)=R(F)$.

(3) If B is linearly dependent, then there exist x, $y_1,\dots, y_n\in B$ such that $x=y_1\cdot\cdots\cdot y_n$ and $x\neq y_i$ for any i. The assertion (1) implies that $I(x)\supseteq\cap_{1\leqq i\leqq n} I(y_i)$ which contradicts the assumption of (3). q.e.d.

We now consider the following three conditions which are the converse of the statements (1), (2) and (3) in Proposition 3.7.

(*A*–1) *If* $I(x)\supseteq I(B)$, *then* $x\in\langle B\rangle$.

(*A*–2) *If* $I(B)=R(F)$, *then* $\langle B\rangle=U$.

(*A*–3) *If* B *is linearly independent in* U_F, *then* $\cap_{x\in B} I(x)$ *is irredundant.*

PROPOSITION 3.8. *Let* F *be a pre-Hilbert field, and* B *be a finite subset of* U_F. *Then for* $x\in U$, (*A*–1) *holds.*

PROOF. There exists a subset $B'\subseteq B$ such that $I(B)=I(B')=\cap_{y\in B'} I(y)$ is irredundant. Let $B'=\{y_1,\dots, y_n\}$. By (3) of Proposition 3.7, $\{y_1,\dots, y_n\}$ is linearly independent. Since $U/I(y_i)$ is a 1-dimensional vector space, it follows from Lemma 3.4 that $U/\cap_{y\in B'} I(y)$ is an n-dimensional vector space. Let K be the set of P-groups $I(x)$, $x\in\langle B'\rangle$. Let L be the set of P-groups which contain $I(B)$, and M be the set of subspaces of index 2, containing $I(B)$, in U. Then $K\subseteq L\subseteq M$. The first inclusion is clear and the second one follows from Proposition 2.3. Using Proposition 2.2, we see that $|K|=2^n-1$ and $|M|=2^n-1$, because $U_F/I(B)$ is an n-dimensional vector space by Lemma 3.4. Hence $K=L$ and the proof is completed. q.e.d.

COROLLARY 3.9. *Let F be a pre-Hilbert field with $|U_F|<\infty$. Then the following statements are satisfied.*

(1) *For any $x\in U$ and any $B\subseteq U$, $(A-1)$ holds.*

(2) *For any $B\subseteq U$, $(A-2)$ holds.*

(3) *For any $B\subseteq U$, $(A-3)$ holds.*

PROOF. The assertion (1) follows immediately from Proposition 3.8. Moreover we can readily see that (1) implies (2) and that (1) implies (3). q.e.d.

Conversely, if $|U_F|<\infty$, then the statements (1), (2) and (3) of Corollary 3.9 characterize a pre-Hilbert field.

PROPOSITION 3.10. *Let F be a field with $1\neq|U_F|<\infty$. If any one of the statements in Corollary 3.9 holds, then F is a pre-Hilbert field.*

PROOF. It is enough to show that (2) or (3) characterizes F being a pre-Hilbert field.

(2): For $B\subseteq U_F$, $I(B)=R(F)$ implies $\langle B\rangle=U$. Suppose F is not a pre-Hilbert field. Then we can find $a_1\in U$ such that $\dim U/\langle a_1\rangle\geqq 2$. We can construct a sequence $\{a_1, a_2,\dots, a_t\}$ inductively, such that $I(a_1,\dots, a_j)\nsubseteq I(a_{j+1})$ for any $j=1,\dots, t-1$, and $I(a_1,\dots, a_t)=R(F)$. By Lemma 3.5, $t<\dim U$. Hence $\langle a_1,\dots, a_t\rangle\neq U$. But this contradicts the hypothesis of (2).

(3): For $B\subseteq U$, if B is linearly independent, then $\bigcap_{x\in B} I(x)$ is irredundant. Let $\{a_1,\dots, a_t\}$ be a free base of U over $\boldsymbol{Z}_2$; then by (3), $\bigcap_{1\leqq i\leqq t} I(a_i)$ is irredundant. Since $\dim U/I(a_i)\geqq 1$ for any i, $\dim U/\bigcap_{1\leqq i\leqq t} I(a_i)\geqq t$, and hence is equal to t. By Lemma 3.6, $\dim U/I(a_i)=1$ for any i. Now any non-unit element can be chosen as a member of a free base, and therefore for any $x\in U$, $\dim U/I(x)\leqq 1$. Apply Proposition 2.3. q.e.d.

We end this section with the following proposition.

PROPOSITION 3.11. *Let F be a pre-Hilbert field, and B be a subspace of U such that* $\dim U/B=1$. *If B contains a finite intersection of P-groups, then B is a P-group.*

PROOF. We can assume that B contains an irredundant intersection $\bigcap_{1\leqq i\leqq n} I(a_i)$. Then $\{a_1,\dots, a_n\}$ is linearly independent in U. By Proposition 2.2, the number of P-groups which contain $\bigcap_{1\leqq i\leqq n} I(a_i)$ is at least 2^n-1. Since any P-group has index 2 in U, Lemma 3.1 yields that B is a P-group. q.e.d.

§ 4. Applications of $I(A)$

By abuse of notation, we also denote $I(A)/R(F)$ by $I(A)$, where A is a subset of U.

LEMMA 4.1. *Let F be a field. Let x and y be elements of U. Then, $x \in I(y)$ if and only if $y \in I(x)$.*

PROOF. Let x' and y' be representatives of x and y in F, respectively. Then $x \in I(y)$ if and only if $x' \in D_F\langle 1, -y'\rangle$, and similarly, $y \in I(x)$ if and only if $y' \in D_F\langle 1, -x'\rangle$. The assertion follows immediately from these observations.

q.e.d.

PROPOSITION 4.2. *Let F be a field. For a subset A of U, we have*

$$I(A) = \{x \in U \mid A \subseteq I(x)\}.$$

PROOF. The assertion $x \in I(A)$ is equivalent to saying that $x \in I(a)$ for every $a \in A$, and the latter statement is equivalent to the fact $a \in I(x)$ for every $a \in A$ by Lemma 4.1. This observation implies that $x \in I(A)$ if and only if $A \subseteq I(x)$.

q.e.d.

For a subset A of U, we put $E(A) = I(I(A))$.

PROPOSITION 4.3. *Let F be a field. Then for subsets $A, B \subseteq U$, the following statements hold:*

(1) *If $A \subseteq B$, then $E(A) \subseteq E(B)$.*

(2) *$A \subseteq E(A)$.*

(3) *$E(E(A)) = E(A)$.*

PROOF. Suppose that $x \in E(A)$. Then, by Proposition 4.2, we have $I(A) \subseteq I(x)$, and therefore $I(B) \subseteq I(x)$. Again by Proposition 4.2, we see that $x \in E(B)$. Thus the assertion (1) is settled.

The assertion (2) follows immediately from the definition.

As for the assertion (3), we first show that $I(E(A)) = I(A)$. In fact, if $x \in E(A)$, then $I(A) \subseteq I(x)$ and so $I(A) \subseteq I(E(A))$; conversely, since $A \subseteq E(A)$, $I(E(A)) \subseteq I(A)$. Suppose now that $x \in E(E(A))$. Then $I(E(A)) \subseteq I(x)$ and so $I(A) \subseteq I(x)$, which implies that $x \in E(A)$. Conversely, if $x \in E(A)$, then we can show that $x \in E(E(A))$ similarly. q.e.d.

COROLLARY 4.4. *For a subset A of U, $E(A)$ is the intersection of all P-groups which contain A.*

PROOF. From (2) of Proposition 4.3, it is clear that $E(A)$ is an intersection of some P-groups which contain A. So it is enough to show that any P-group which contains A also contains $E(A)$. If $I(x)\supseteq A$, then $x\in I(A)=I(E(A))$ and hence $I(x)\supseteq E(A)$. q.e.d.

PROPOSITION 4.5. *Let F be a field. The following statements are equivalent*:

(1) *For any $x\in U$, $E(x)=\langle x\rangle$.*

(2) *If for $a, b\in U$, $I(a)=I(b)$, then $ab=1\in U$. Moreover any two P-groups are incomparable.*

PROOF. (1)⇒(2): We assume that $I(a)=I(b)$. Then $a\in E(b)$ by Proposition 4.2. So $a\in\langle b\rangle$, and so $ab=1$. We now assume that $I(a)$ and $I(b)$ are P-groups (i.e. $a\neq 1$, $b\neq 1$) and $I(a)\subsetneqq I(b)$. Then we have $b=a$ by the fact $b\in E(a)=\langle a\rangle$. But this contradicts the assumption $I(a)\subsetneqq I(b)$.

The implication: (2)⇒(1) is similar and the proof is omitted. q.e.d.

COROLLARY 4.6. *Let F be a pre-Hilbert field. Then for any $x\in U$, $E(x)=\langle x\rangle$.*

PROOF. It follows from Proposition 2.3 that F satisfies the statement (2) in Proposition 4.5. q.e.d.

Let F be a field, and $K=F(\sqrt{a})$, $a\in\dot{F}-\dot{F}^2$. Then there is an interesting characterization of $R(K)\cap\dot{F}$.

PROPOSITION 4.7. *Let F be a field and $K=F(\sqrt{a})$, $a\in\dot{F}-\dot{F}^2$. For $b\in\dot{F}$, the following statements are equivalent*:

(1) $b\in R(K)$.

(2) $I_F(b)\supseteq I_F(a)$ *and* $I_F(b)\cdot I_F(ab)=\dot{F}$.

PROOF. (1)⇒(2): By Lemma 2.6 (Norm Principle), $N(D_K\langle 1, -b\rangle)\subseteq D_F\langle 1, -b\rangle$. Let b be an element of $R(K)$. Then $D_K\langle 1, -b\rangle=\dot{K}$. Hence, $D_F\langle 1, -a\rangle=N(\dot{K})=N(D_K\langle 1, -b\rangle)\subseteq D_F\langle 1, -b\rangle$, hence $I_F(b)\supseteq I_F(a)$. By Lemma 2.5, $D_F\langle 1, -b\rangle\cdot D_F\langle 1, -ab\rangle=D_K\langle 1, -b\rangle\cap\dot{F}=\dot{F}$, i.e. $I_F(b)\cdot I_F(ab)=\dot{F}$.

(2)⇒(1): We must show that $D_K\langle 1, -b\rangle$ is universal. The fact $I_F(b)\cdot I_F(ab)=\dot{F}$ shows that $D_K\langle 1, -b\rangle\supseteq\dot{F}$. Hence $D_K\langle 1, -b\rangle=\dot{F}\cdot D_K\langle 1, -b\rangle$. By the corollary to Lemma 2.6, $N^{-1}(D_F\langle 1, -b\rangle)=\dot{F}\cdot D_K\langle 1, -b\rangle$. The another assumption $I_F(b)\supseteq I_F(a)$ shows that $N(\dot{K})\subseteq D_F\langle 1, -b\rangle$. So $\dot{K}=N^{-1}(D_F\langle 1, -b\rangle)=\dot{F}\cdot D_K\langle 1, -b\rangle=D_K\langle 1, -b\rangle$. q.e.d.

COROLLARY 4.8. *Let F be a field and $K=F(\sqrt{a})$, $a\in\dot{F}-\dot{F}^2$. Let $\bar{a}$ be the image of a in U. If $E(\bar{a})=\langle\bar{a}\rangle$, then $R(K)\cap\dot{F}=\langle R(F), a\rangle$.*

PROOF. The fact that $N^{-1}(D_F\langle 1, -b\rangle)=\dot{F}\cdot D_K\langle 1, -b\rangle$ implies $R(F)\subseteq$

$R(K)$. Thus it is obvious that $R(K) \cap \dot{F} \supseteq \langle R(F), a\rangle$. Conversely, it follows from Proposition 4.7 that $I_F(a) \subseteq I_F(b)$ for any $b \in R(K) \cap \dot{F}$. Let $\bar{b}$ be the canonical image of b in U. Then $\bar{b} \in I(I(\bar{a})) = E(\bar{a}) = \langle \bar{a}\rangle$. Hence $\bar{b} = 1$ or $\bar{a}$; hence $R(K) \cap F \subseteq \langle R(F), a\rangle$. q.e.d.

LEMMA. *Let V be a finite dimensional vector space over $\boldsymbol{Z}_2$. Then any subspace of V can be expressed as a finite intersection $\cap W_i$ of subspaces of W_i's such that* $\dim V/W_i = 1$ *for any i.*

The proof of this lemma is easy and omitted.

PROPOSITION 4.9. *Let F be a pre-Hilbert field, and X be a subspace of U_F containing a finite intersection of P-groups. Then $E(X) = X$.*

PROOF. By Proposition 3.11, any subspace of index 2 in U_F, which contains a finite intersection of P-groups, is a P-group. By the above lemma, X can be expressed as an intersection of P-groups. Apply Corollary 4.4. q.e.d.

§5. The relation between U_F and U_K

Throughout this section, we let F be a field, and $K = F(\sqrt{a})$ be a quadratic extension of F.

LEMMA 5.1. $N^{-1}(R(F)) \supseteq \dot{F} \cdot R(K)$.

PROOF. From Norm Principle, $N^{-1}(D_F\langle 1, -b\rangle) = \dot{F} \cdot D_K\langle 1, -b\rangle$ for any $b \in \dot{F}$. Let $f\alpha$ be an element of $\dot{F} \cdot R(K)$, where $f \in \dot{F}$ and $\alpha \in R(K)$. Since $f\alpha \in \dot{F} \cdot D_K\langle 1, -b\rangle$ for any $b \in \dot{F}$, $N(f\alpha) \in D_F\langle 1, -b\rangle$ for any $b \in \dot{F}$. Hence $N(f\alpha) \in R(F)$. q.e.d.

LEMMA 5.2 ([2], Corollary to Proposition 3). $R(K) \cap \dot{F} \supseteq \langle R(F), a\rangle$.

By Hilbert Theorem 90, there is an exact sequence (A);

$$\text{(A)} \quad 1 \longrightarrow \dot{F}/\langle \dot{F}^2, a\rangle \xrightarrow{\varepsilon} \dot{K}/\dot{K}^2 \xrightarrow{N} \dot{F}/\dot{F}^2.$$

From (A), we get a sequence (B);

$$\text{(B)} \quad 1 \longrightarrow U_F/\langle a\rangle \xrightarrow{\bar{\varepsilon}} U_k \xrightarrow{\bar{N}} U_F$$

where, x (resp. y) being a representative of $\bar{x}$ in $\dot{F}/\langle \dot{F}^2, a\rangle$ (resp. $\bar{y}$ in $\dot{K}/\dot{K}^2$), $\bar{\varepsilon}(\bar{x}) = \varepsilon(x) \bmod R(K)$ and $\bar{N}(\bar{y}) = N(y) \bmod R(F)$. Here note that $\bar{\varepsilon}$ and $\bar{N}$ are well-defined by Lemma 5.1 and Lemma 5.2.

PROPOSITION 5.3. *The following statements hold:*
(1) (B) *is exact at $U_F/\langle a\rangle$ if and only if $R(K) \cap \dot{F} = \langle R(F), a\rangle$.*

(2) (B) *is exact at* U_K *if and only if* $N^{-1}(R(F))=\dot{F}\cdot R(K)$.

PROOF. We consider the following commutative diagram, where $\tilde{\varepsilon}$ and $\tilde{N}$ are the restriction maps of ε and N respectively. It is clear that the sequences (2), (4), (5) and (6) are exact.

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \langle a, R(F)\rangle/\langle a\rangle \arrow[r, "\tilde{\varepsilon}"] \arrow[d] & R(K) \arrow[r, "\tilde{N}"] \arrow[d] & R(F) \arrow[d] & \cdots\cdots(1) \\
1 \arrow[r] & \dot{F}/\langle a, \dot{F}^2\rangle \arrow[r, "\varepsilon"] \arrow[d] & \dot{K}/\dot{K}^2 \arrow[r, "N"] \arrow[d] & \dot{F}/\dot{F}^2 \arrow[d] & \cdots\cdots(2)=(A) \\
1 \arrow[r] & U_F/\langle a\rangle \arrow[r, "\bar{\varepsilon}"] \arrow[d] & U_K \arrow[r, "\bar{N}"] \arrow[d] & U_F \arrow[d] & \cdots\cdots(3)=(B) \\
 & 1 \arrow[d, dotted, no head] & 1 \arrow[d, dotted, no head] & 1 \arrow[d, dotted, no head] & \\
 & (4) & (5) & (6) &
\end{tikzcd}$$

Then, (B) is exact at $U_F/\langle a\rangle \Leftrightarrow \bar{\varepsilon}$ is injection

$$\begin{aligned}
&\Leftrightarrow R(K)\cap \dot{F}/\langle a, \dot{F}^2\rangle=\langle a, R(F)\rangle/\langle a\rangle \\
&\Leftrightarrow R(K)\cap \dot{F}=\langle a, R(F)\rangle \\
&(\Leftrightarrow (1) \text{ is exact at } R(K)).
\end{aligned}$$

(B) is exact at $U_K \Leftrightarrow N^{-1}(R(F))=\langle R(K), \dot{F}/\langle a, F^2\rangle\rangle \Leftrightarrow N^{-1}(R(F))=\dot{F}\cdot R(K)$ ($\Leftrightarrow \tilde{N}$ is onto). q.e.d.

COROLLARY 5.4. *Let F be a pre-Hilbert field. Then $\bar{\varepsilon}$ is an injection.*

PROOF. The assertion follows immediately from Corollary 4.6, Corollary 4.8 and Proposition 5.3. q.e.d.

Let $K=F(\sqrt{a})$, $a\in\dot{F}-\dot{F}^2$, be a quadratic extension of F. We say that K is a radical extension if $a\in R(F)$, and a non-radical extension otherwise.

COROLLARY 5.5. *Let K be a radical extension of F. Suppose that* $\dim U_F=n<\infty$. *Then,* $N^{-1}(R(F))=\dot{F}\cdot D(K)$ *if and only if* $\dim U_K=2n$.

PROOF. By Proposition 5.3, it is enough to show that $R(K)\cap\dot{F}=R(F)$. By Lemma 2.5, $D_K\langle 1, -x\rangle\cap\dot{F}=D_F\langle 1, -x\rangle$ for any $x\in\dot{F}$, and the assertion follows from Lemma 5.2. q.e.d.

COROLLARY 5.6. *If* $\dim U_F/I_F(a)=1$ (*K must be a non-radical extension*) *and* $\dim U_F=n<\infty$, *then* $N^{-1}(R(F))=\dot{F}\cdot D(K)$ *if and only if* $\dim U_K=2(n-1)$.

PROOF. It is easy to show that $E(\langle a\rangle)=\langle a\rangle$, where $\langle a\rangle$ is considered as a subgroup of U_F. Hence $\bar{\varepsilon}$ is injective, and the assertion is obvious. q.e.d.

§ 6. H-conjecture when $|U_F| < \infty$

Throughout this section we assume that F is a pre-Hilbert field and $K = F(\sqrt{a})$ is a non-radical quadratic extension, i.e. $a \notin R(F)$, unless otherwise stated. We need several results in [5], and so we borrow them here. We shall give a proof of one of them, Proposition 6.5, which is based on a different idea from that in [5], as a preliminary step to § 7, the main part of this paper.

LEMMA 6.1 ([5], Proposition 2.6). *For $x \in \dot{K} - N^{-1}(R(F))$, we have $\dot{F} \cdot D_K\langle 1, -x\rangle = \dot{K}$.*

Lemma 6.1 does not need the assumption that $a \notin R(F)$.

LEMMA 6.2 ([5], Corollary 3.4). *If $x \in K$, then $\dot{F} \cap D_K\langle 1, -x\rangle = D_F\langle 1, -N(x)\rangle$.*

LEMMA 6.3. *For $x \in N^{-1}(R(F))$, we have $D_K\langle 1, -x\rangle \supseteq N^{-1}(R(F))$.*

Lemma 6.3 is given in the proof of [5], Proposition 3.7, by using a transfer method.

LEMMA 6.4 ([5], Theorem 3.8). *If F is non-formally real, then K is a pre-Hilbert field.*

PROPOSITION 6.5 ([5], Proposition 3.9). *If $|U_F| < \infty$, then $N^{-1}(R(F)) = \dot{F} \cdot R(K)$.*

PROOF. By Lemma 5.1, $N^{-1}(R(F)) \supseteq \dot{F} \cdot R(K)$. Conversely we take an element $x \in N^{-1}(R(F)) - R(K)$. Then by Lemma 6.3 and Lemma 6.4, $N(D_K\langle 1, -x\rangle)/R(F)$ has index 2 in $N(\dot{K})/R(F) = I_F(a)$. By Proposition 4.9 and Corollary 4.4, $N(D_K\langle 1, -x\rangle)/R(F) = I_F(a) \cap I_F(b)$ for some $b \in \dot{F} - \langle a, R(F)\rangle$. Then $D_K\langle 1, -x\rangle = N^{-1}(D_F\langle 1, -b\rangle) = D_K\langle 1, -b\rangle$, and hence $bx \in D(K)$ by Proposition 2.2. q.e.d.

The following Lemma 6.6 is valid for any field F and any quadratic extension K.

LEMMA 6.6. $N^{-1}(R(F)) = \bigcap_{b \in \dot{F}} \dot{F} \cdot I_K(b)$.

PROOF. Let x be an element of $\dot{K}$. Then $x \in N^{-1}(R(F))$ if and only if $N(x) \in I_F(b)$ for any $b \in \dot{F}$, and the latter statement is equivalent to the fact that $x \in \dot{F} \cdot I_K(b)$ for any $b \in \dot{F}$ (Norm Principle). q.e.d.

In particular, by Lemma 6.2, $I_K(b) \supseteq \dot{F}$ for any $b \in \dot{F}$; therefore $N^{-1}(R(F)) = \bigcap_{b \in \dot{F}} I_K(b)$.

We can generalize Proposition 6.5 as follows.

LEMMA. *Let V and V' be vector spaces over $\boldsymbol{Z}_2$, and $f\colon V\to V'$ be a linear map. Let W_i, $i=1,\ldots,n$, be subspaces of V such that* $\dim V/W_i=1$ *for any i and* $\operatorname{Ker} f\subseteq \cap W_i$. *If $\cap W_i$ and $\cap f(W_i)$ are both irredundant, then $f(\cap W_i)=\cap f(W_i)$.*

PROOF. It is clear that $f(\cap W_i)\subseteq \cap f(W_i)$. It follows from Lemma 3.4 that $\dim V/\cap W_i=n$. So $\dim f(V)/f(\cap W_i)=n$ by the assumption that $\operatorname{Ker} f\subseteq \cap W_i$. Since $\dim f(V)/f(W_i)=1$ for any i, $\dim f(V)/\cap f(W_i)=n$, again by Lemma 3.4. This implies that $f(\cap W_i)=\cap f(W_i)$. q.e.d.

PROPOSITION 6.7. *Suppose that, for any $x\in N^{-1}(R(F))$, there exists a finite subset B of $\dot{F}$ such that $I_K(x)\supseteq I_K(B)$. Then $N^{-1}(R(F))=\dot{F}\cdot D(K)$.*

PROOF. We may assume that $I_K(B)=\bigcap_{y\in B} I_K(y)$ is irredundant. Then B is linearly independent in U_K by Proposition 3.7 (2). Hence B is linearly independent in $U_F/\langle a, R(F)\rangle$. By Proposition 3.8, for a finite subset $B\subseteq U_F$, $(A\text{–}3)$ holds. This shows that $\bigcap_{y\in B} I_F(y)\cap I_F(a)$ is irredundant, because $B\cup\{a\}$ is linearly independent in U_F. On the other hand, $N(I_K(y))=I_F(y)\cap I_F(a)$ for any $y\in\dot{F}$ by Norm Principle. Then the above lemma says that $N(I_K(B))=I_F(B)\cap I_F(a)$. Hence $N(D_K\langle 1, -x\rangle)\supseteq I_F(B)\cap I_F(a)$, and by Proposition 4.9, $E(N(D_K\langle 1, -x\rangle)/R(F))=N(D_K\langle 1, -x\rangle)/R(F)$. By Corollary 4.4, there exists $b\in\dot{F}-\langle a, R(F)\rangle$ such that $N(D_K\langle 1, -x\rangle)/R(F)=I_F(a)\cap I_F(b)$. Then $D_K\langle 1, -x\rangle= N^{-1}(D_F\langle 1, -b\rangle)=D_K\langle 1, -b\rangle$, which implies that $bx\in R(K)$ by Proposition 2.2. q.e.d.

§7. Topologies on U induced by P-groups

In what follows, we let K be a non-radical quadratic extension of a pre-Hilbert field F, namely $K=F(\sqrt{a})$ with $a\notin R(F)$.

Let G be an abelian group and $\{P_i\}_{i\in I}$ be a non-empty family of subgroups of G. Let $\{R_j\}_{j\in J}$ be the set of all finite intersections of P_i's. We first state the following two propositions based on the theory of topological groups.

PROPOSITION 7.1. *There exists a unique topology S of G so that G becomes a topological group under S and $\{R_j\}_{j\in J}$ is a complete neighbourhood system of the unity of G.*

PROPOSITION 7.2. *Let M be a subset of G. Then we have $\overline{M}=\{x\in G\mid xR_j\cap M\neq\phi$ for any $j\in J\}$, where the bar means the topological closure.*

DEFINITION 7.3. *We consider the following three kind of topologies S_1, S_2 and S_3 on $\dot{K}$:*

(1) *S_1 is defined by* $\{P_i\}=\{I_K(x) \mid x \in \dot{K}\}$.
(2) *S_2 is defined by* $\{P_i\}=\{I_K(x) \mid x \in N^{-1}(R(F))\}$.
(3) *S_3 is defined by* $\{P_i\}=\{I_K(x) \mid x \in \dot{F}\}$.

PROPOSITION 7.4. *The following statements are equivalent:*
(1) $N^{-1}(R(F)) = \dot{F} \cdot R(K)$.
(2) *The topology S_2 coincides with the topology S_3.*

PROOF. We first assume the equality (1). Since $I_K(x)=I_K(xy)$ for any $x \in \dot{K}$ and any $y \in R(F)$, we have $\{I_K(x) \mid x \in N^{-1}(R(F))\}=\{I_K(x) \mid x \in \dot{F}\}$.

Conversely, suppose that the assertion (2) holds. Then, for any $x \in N^{-1}(R(F))$, we can find a finite subset B of $\dot{F}$ such that $I_K(x) \supseteq I_K(B)$. Apply Proposition 6.7. q.e.d.

LEMMA 7.5. *Let G be an abelian group with the unity e. Assume that for any $x \in G$, $x^2=e$. Let $\{P_i\}_{i\in I}$ be a family of subgroups of G and S be the topology defined by $\{P_i\}_{i\in I}$. Then for a subset M of G, $\overline{M}=\cap R_jM$. In particular $\{\bar{e}\}=\bigcap_{i\in I} P_i$.*

The assertion follows immediately from Proposition 7.2.

PROPOSITION 7.6. *If F is not formally real, then the topologies S_1 and S_2 are different to each other.*

PROOF. Suppose, on the contrary, that the topologies S_1 and S_2 coincide. Then for any $x \in \dot{K}-N^{-1}(R(F))$, we have $I_K(x) \supseteq I_K(B)$ for some finite subset B of $N^{-1}(R(F))$. Since K is a pre-Hilbert field by Lemma 6.4, it follows from Proposition 3.8 that $x \in \langle B, R(K)\rangle \subseteq N^{-1}(R(F))$. This is a contradiction. q.e.d.

We define the topology on $\dot{F}$ by $\{P_i\}=\{I_F(x) \mid x \in \dot{F}\}$. By Lemma 7.5, we see that $R(F)=\cap P_i=\{\bar{e}\}$ is a closed subgroup.

LEMMA 7.7. *For any topology S_i, $1 \leqq i \leqq 3$, on $\dot{K}$, the norm map $N: \dot{K} \to \dot{F}$ is continuous.*

PROOF. We have only to show that N is continuous at the unity 1 of $\dot{K}$. Let V be a neighbourhood of the unity 1 of $\dot{F}$, namely $V=\bigcap_{x\in B} I_F(x)$ for some finite subset B of $\dot{F}$. Since $N(I_K(x)) \subseteq I_F(x)$ by Norm Principle ([8], VII, Theorem 4.3), we see that $N(I_K(B)) \subseteq I_F(B)=V$. We can readily see that $I_K(B)$ is a neighbourhood of $1 \in \dot{K}$ for any topology S_i. Thus the assertion is settled. q.e.d.

In order to prove our main theorem (Theorem 7.9), we need the following

LEMMA 7.8. *Let V be a vector space over $\boldsymbol{Z}_2$, and W_i $(i=1,\dots,n)$ be subspaces of V such that $\dim V/W_i=1$ for any i. Suppose that $\bigcap_{1\leqq i\leqq n} W_i$ is ir-*

redundant and let I be a subset of $\{1,\dots, n\}$. Then we can find an element x of V so that $x \in W_i$ for $i \in I$ and $x \notin W_j$ for $j \notin I$.

PROOF. We see that $|V/\bigcap_{1 \leqq i \leqq n} W_i| = 2^n$ by Lemma 3.4. Let L be the set of all subsets of $\{1,\dots, n\}$. We define a map φ: $V/\cap W_i \to L$ by $\varphi(\bar{x}) = \{i \mid x \in W_i\}$, where x is a representative of $\bar{x}$ in V. We can readily see that the following two statements concerning elements x and y of V are equivalent: (1) $x+y \in \cap W_i$, (2) For any i, $x \in W_i$ if and only if $y \in W_i$. This equivalence implies that φ is well-defined and that φ is injective. Since $|V/\cap W_i| = |L| = 2^n$, φ is surjective. Thus the proof is completed.

THEOREM 7.9. *Let K be a non-radical quadratic extension of a pre-Hilbert field F. Then we have $N^{-1}(R(F)) = (\dot{F} \cdot R(K))^-$, where the bar means the topological closure with respect to the topology S_1.*

PROOF. Since $N^{-1}(R(F)) \supseteq \dot{F} \cdot R(K)$, $R(F)$ is closed in $\dot{F}$ and N is continuous, it is clear that $N^{-1}(R(F)) \supseteq (\dot{F} \cdot R(K))^-$. Conversely, we take an element α of $N^{-1}(R(F))$. By virtue of Lemma 7.5, we have to show that for any finite subset X of $\dot{K}$, $\alpha \in I_K(X) \cdot \dot{F}$.

Step 1. First we show that we may assume $X \cap N^{-1}(R(F)) = \phi$. Let $X = X_1 \cup X_2$ be the partition of X such that $X_1 \cap N^{-1}(R(F)) = \phi$ and $X_2 \subseteq N^{-1}(R(F))$. Then, since $\dot{F} \subseteq I_K(X_2)$ by Lemma 6.2, we see that $I_K(X) \cdot \dot{F} = (I_K(X_1) \cap I_K(X_2)) \cdot \dot{F} = I_K(X_1) \cdot \dot{F} \cap I_K(X_2)$. Lemma 6.3 implies that $N^{-1}(R(F)) \subseteq I_K(X_2)$. Therefore, to show that $\alpha \in I_K(X) \cdot \dot{F}$, we have only to prove that $\alpha \in I_K(X_1) \cdot \dot{F}$.

Step 2. In this step we prove our theorem under the additional assumption that $I_F(N(X)) = \bigcap_{x \in X} D_F\langle 1, -N(x)\rangle$ is irredundant. What we have to do is to find an element $f \in \dot{F}$ such that $f\alpha \in I_K(x)$ for any $x \in X$. Note first that $I_K(x) \cap \dot{F} = I_F(N(x))$ by Lemma 6.2 and $I_K(x)$ has index 2 in $\dot{K}$ by Lemma 6.4 for any $x \in X$. It follows from these observations that, x being an element of X, if $\alpha \in I_K(x)$, then $f\alpha \in I_K(x)$ for any $f \in I_F(N(x))$ and if $\alpha \notin I_K(x)$, then $f\alpha \in I_K(x)$ for any $f \notin I_F(N(x))$. Therefore it is sufficient to show that there exists $f \in \dot{F}$ such that for any $x \in X$, $\alpha \in I_K(x)$ if and only if $f \in I_F(N(x))$. Let I be the subset of X such that $I = \{x \in X \mid \alpha \in I_K(x)\}$. Apply now Lemma 7.8.

Step 3. Finally we consider the general case. Let Y be a subset of X such that $I_F(N(x)) = \bigcap_{y \in Y} I_F(N(y))$ is irredundant. Then, by Step 2, we can find an element $f \in \dot{F}$ such that $f\alpha \in I_K(Y)$. We then show that $f\alpha \in I_K(x)$ for any $x \in X$. It follows from Proposition 3.8 that $N(x) \in \langle N(Y), R(F)\rangle$ because of the fact $I_F(N(x)) \supseteq \cap I_F(N(Y))$. Therefore $x = g \cdot y_1 \cdot \cdots \cdot y_n$, where $g \in N^{-1}(R(F))$ and $y_1,\dots, y_n \in Y$. Then, $f\alpha$ is an element of $I_K(g) \cap (\bigcap_{1 \leqq i \leqq n} I_K(y_i))$, which is contained in $I_K(x)$ by Lemma 2.4. Thus we see that $f\alpha \in I_K(x)$ and the proof is completed.

References

[1] L. Berman, Pythagorean fields and the Kaplansky radical, J. Algebra **61** (1979), 497–507.

[2] C. M. Cordes, Kaplansky's radical and quadratic forms over non real fields, Acta. Arith. **28** (1975), 253–261.

[3] C. M. Cordes, Quadratic forms over non formally real fields with a finite number of quaternion algebras, Pacific J. Math. **63** (1976), 357–365.

[4] C. M. Cordes and J. R. Ramsey, Jr., Quadratic forms over fields with $u=q/2<\infty$, Fundamenta Math. **99** (1978), 1–10.

[5] C. M. Cordes and J. R. Ramsey, Jr., Quadratic forms over quadratic extensions of fields with two quaternion algebras, Can. J. Math. **31** (1979), 1047–1058.

[6] R. Elman and T. Y. Lam, Quadratic forms under algebraic extensions, Math. Ann. **219** (1976), 21–42.

[7] I. Kaplansky, Fröhlich's local quadratic forms, J. Reine Angew. Math. **239** (1969), 74–77.

[8] T. Y. Lam, The algebraic theory of quadratic forms, W. A. Benjamin, Reading, Mass., 1973.

Eishin Senior High School,
Hiroshima, Japan
and
Department of Mathematics,
Faculty of Science,
Hiroshima University