MONOGRAFIAS DE MATEMÁTICA N.º 29

HEREDITARILY-PYTHAGOREAN FIELDS AND ORDERINGS OF HIGHER LEVEL

EBERHARD BECKER

INSTITUTO DE MATEMÁTICA PURA E APLICADA

RIO DE JANEIRO
1978

MONOGRAFIAS DE MATEMÁTICA

1) Alberto Azevedo & Renzo Piccinini - Introdução à Teoria dos Grupos
2) Nathan M. Santos - Vetores e Matrizes (esgotado)
3) Manfredo P. Carmo - Introdução à Geometria Diferencial Global
4) Jácob Palis Jr. - Sistemas Dinâmicos
5) João Pitombeira de Carvalho - Introdução à Álgebra Linear (esgotado)
6) Pedro J. Fernandez - Introdução à Teoria das Probabilidades
7) R.C. Robinson - Lectures on Hamiltonian Systems
8) Manfredo P. do Carmo - Notas de Geometria Riemanniana
9) Chain S. Hönig - Análise Funcional e o Problema de Sturn-Liouville
10) Welington de Melo - Estabilidade Estrutural em Variedades de Dimensão 2
11) Jaime Lesmes - Teoria das Distribuições e Equações Diferenciais
12) Clóvis Vilanova - Elementos da Teoria dos Grupos e da Teoria dos Anéis
13) Jean Claude Douai - Cohomologie des Groupes,
14) H. Blaine Lawson Jr. - Lectures on Minimal Submanifolds, Vol.1
15) Elon L. Lima - Variedades Diferenciáveis
16) Pedro Mendes - Teoremas de Ω-estabilidade e Estabilidade Estrutural em Variedades Abertas.
17) Herbert Amann - Lectures on Some Fixed Point Theorems
18) Exercícios de Matemática - IMPA
19) Djairo G. de Figueiredo - Números Irracionais e Transcendentes
20) C.E. Zeeman - Uma Introdução Informal à Topologia das Superfícies
21) Manfredo P. do Carmo - Notas de um curso de Grupos de Lie
22) A. Prestel - Lectures on Formally Real Fields
23) Aron Simis - Introdução à Álgebra
24) Jaime Lesmes - Seminário de Análise Funcional
25) Fred Brauer - Some Stability and Perturbation Problem for Differential and Integral Equations
26) Lucio Rodríguez - Geometria das Subvariedades
27) Mario Miranda - Frontiere Minime
28) Fernando Cardoso - Resolubilidade Local de Equações Diferenciais Parciais
29) Eberhard Becker - Hereditarily-Pythagorean Fields and Orderings of Higher Level

Contents

Introduction

Artins solution of the 17^{th} problem of Hilbert is based on the theory of formally real fields which he and O.Schreier created [1]-[4]. One essential idea of his proof consists of a new characterization of sums of squares. Let k be a field, Q(k) the subset of all sums of squares. If char k = 2, then $Q(k) = k^2$, if char $k \neq 2$ but $-1 \in Q(k)$, then $Q(k) = k$ since we have an identity $a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2$ Fields in which -1 is not a sum of squares were called formally real (real for short) by E.Artin and O.Schreier, and for these fields they developed a theory. Every real field has (in a fixed algebraic closure) maximal real algebraic extensions called its real closures. The following fundamental results were proved by Artin and Schreier where k is a real field, Ω its algebraic closure and R an intermediate field of $\Omega|k$:

1) R is a real closure of k iff the absolute Galoisgroup $G(\Omega/R)$ is a nontrivial finite group. If R is a real closure, then $\Omega = R(\sqrt{-1})$.
2) If R is a real closure of k, then $P := R^2$ is an ordering, i.e. satisfies the following conditions:
   i) $P+P \subset P$ ii) $PP \subset P$ iii) $R = P \cup -P$, $\{0\} = P \cap -P$.
3) k admits orderings, and every ordering P of k is induced by a real closure R of k: $P = R^2 \cap k$. Two real closures

of k are isomorphic over k iff they induce the same ordering on k.

Based on these results Artin was able to prove that Q(k) is the intersection of all orderings of k and finally to answer Hilbert's problem in the affirmative.

Besides these applications the results 1) - 3) are significant from a different point of view. Thex are examples of some general principles in field theory; for the base field k which is the proper object of investigation is investigated only via certain field-extensions. These extensions admit some structures - orderings in this case - which in a wider sense can be regarded as arithmetical ones. The problem to characterize these extensions up to isomorphy can be solved by the induced structures in the base field k. One sees a clear analogy with the local-global-principle in algebraic number theory as well as with the classfield theory of global or local fields.

The present work is founded on these aspects of the Artin-Schreier theory. Hence we proceed in the following way:

we shall single out real algebraic extensions by properties of their absolute Galoisgroup, investigate such extensions especially with respect to arithmetical structures, characterize isomorphic extensions by the induced arithmetical structures in the base field.

One starting point was a result of W.D. Geyer. He investigated in [27] all algebraic number fields whose absolute Galois groups are not only pro-solvable but even solvable as an abstraot group. A real number field of this type has a rather special absolute Galois group: it is a semi-direct product of an abelian group with an involution operating on the abelian group by taking the inverse.

The second starting point was the observation that there exist relative versions of the original Artin-Schreier theory. Besides the algebraic closure Ω of the real field k one can find further extensions $\Omega|k$ such that the results 1) - 3) remain valid: one has only to replace the real closures by the relative real closures of k in Ω. The smallest extension is $\Omega = k_2$, the maximal 2-extension of k. A further example is given by the maximal solvable extension.

In chapter II we introduce these suitable extensions $\Omega|k$. These extensions are to be regarded as the universe for the theory to be developed. The results of chapter III and IV refer to the real intermediate fields K of a fixed extension $\Omega|k$. In §1 of chapt. III we prove the following main theorem:

K is hereditarily-pythagorean in Ω (i.e. every real extension of K in Ω is pythagorean) iff the Galois group $G(\Omega|K(i))$ $i = \sqrt{-1}$, is abelian.

This theorem extends the result of W.D. Geyer mentioned above. In view of the result 1) it furthermore shows that the hereditarily-pythagorean fields (= h.p. fields) can be viewed as generalized real-closed fields.

The h.p. fields have many remarkable field-theoretical properties, as will be proved in chap. III. It is not only possible to describe the construction of the algebraic extensions (in Ω) but one can explicitely compute the Galois group $G(\Omega|K)$ and the Brauer group $Br(\Omega|K)$ in terms of simple invariants. Furthermore they admit a nontrivial Ω-henselian valuation (L.Bröcker). In addition to our main theorem the h.p. fields can be characterized by the Haar-measure of the set of involutions in $G(\Omega|K)$ (L.Bröcker), by the existence of a Kummer Theory for the intermediate extensions of $\Omega|K$ (F.P. Halter-Koch) or by torsion-properties of the Wittring of K(X) (in case Ω = algebraic closure).

The investigation of h.p. fields has led to the discovery of the orderings of higher level of a field. Orderings of higher level are new examples of infinite Harrison-primes and are generalizations of orderings. In chap. I we initiate a theory of orderings of higher level. This is done by an extensive use of the theory of Krull-valuation. Based on the extension-theory for orderings of higher level we prove the following theorem.

Let K be an infinite field, char K $\neq$ 2, let n,m be natural numbers, then for arbitrary elements $x_1, \ldots, x_r \in K$ there exist $y_1, \ldots, y_s \in K$ such that the following holds:

$$(x_1^{2^n} + \ldots + x_r^{2^n})^{2^m} = y_1^{2^{n+m}} + \ldots + y_s^{2^{n+m}}$$

This theorem extends in a certain sense an identity of D.Hilbert used in his solution of the Waring-problem.

In the last chapter we deal with h.p. extensions of a given real field. The extension theory for orderings of higher level leads to a solution of the problem of isomorphy. In particular we succeeded in characterizing the isomorphyclasses of the real closures for an ordering of higher level. As opposed to the case of ordinary orderings there exist infinitely many classes in general.

These notes are based on the author's Habilitationsschrift, Köln (Federal Republic of Germany), 1976. I would like to express my gratitude to the Instituto de Mathemâtica Pura et Aplicada, especially to Prof.Dr. O. Endler, that it was rendered possible to publish the results in the IMPA lecture notes series.

Köln, 1977.

Chapter I Orderings of Higher Level

§1 Basic notions

Let K be a (commutative) field, $n \in \mathbb{N}$. A subset $T \subset K$ is called a preordering of level n of K if it satisfies

(P1) $K^{2^n} \subset T$

(P2) $T+T \subset T$

(P3) $TT \subset T$.

For any $t \in T^{\times} := T \setminus \{0\}$ the inverse $t^{-1} = (t^{-1})^{2^n} t^{2^n-1}$ belongs to $T^{\times}$ as follows from (P1), (P3). $T^{\times}$ is therefore a subgroup of $K^{\times}$. Set

$$Q_n(K) = Q_n = \{a \in K \mid \bigvee_{k \in \mathbb{N}} \ \bigvee_{b_1,\ldots,b_k \in K} \ a = \sum_1^k b_i^{2^n} \} .$$

Q_n is obviously a preordering of level n, and in view of (P1), (P2), Q_n is contained in any preordering of level n. Let T be a preordering of level n. Since $T^{\times}$ is a group it follows that

$$T = -T \quad \text{or} \quad T \cap -T = \{0\} .$$

We have $T = -T$ iff T is a subfield of K, but we shall not be concerned about this case here. $T \subseteq K$ is called a proper preordering of level n if it satisfies (P1), (P2), (P3) and

(P4) $T \cap -T = \{0\}$.

Condition (P4) is equivalent to

(P4') $-1 \notin T$.

If char (k) = $p > 0$ then $-1 = (p-1)\times 1 \in Q_n$ holds. Consequently, proper preorderings only exist in fields of characteristic 0. In §2 we shall even prove that they can occur in real fields only.

LEMMA 1. <u>Let K be an infinite field with char (k) $\neq 2$, $T \subset K$ a preordering of level n, then</u>

$$\underline{T - T = K}.$$

<u>Proof</u>. $F := T - T$ is a subfield of k, because of $a^{-1} = (a^{-1})^{2^n} a^{2^n-1}$ for $a \neq 0$. In case $K \neq F$, we find $a \in K \setminus F$ with $a^2 \in F$ since $K^{2^n} \subset F$ holds. In K[X] there is an identity

$$(X + a)^{2^n} - (X - a)^{2^n} = 2^{n+1}\, a\, g(X)$$

where g(X) is a monic polynomial of degree 2^n-1. From $a^2 \in F$ it follows that $g(X) \in F[X]$. Hence $g(\alpha)=0$ for $\alpha \in F$. This implies that F is finite, and hence K must be finite too.

I.R. Joly [38; S.46] proved a general theorem about the subfield which is generated by the powers x^d, d a fixed exponent. If char(K) = 0 the proof could have been carried out by means of the following identiy, too [32, S.235]:

$$d!X = \sum_{h=o}^{d-1} (-1)^{d-1-h} \binom{d-1}{h} [(X + h)^d - h^d]$$

As a consequence of Lemma 1 we have:

i) char (K) > 2 , $|K| = \infty$: $Q_n = K$,

ii) char (K) = 2 : $Q_n = K^{2^n}$,∇

iii) $|K| < \infty$, $K = \mathbb{F}(p^r)$: $Q_n = \mathbb{F}(p^{r_n})$,

where r_n is the smallest divisor of r such that $(p^r - 1)/(p^{r_n} - 1)$ divides 2^n.

LEMMA 2. For a preordering T of level n of K the following statements are equivalent:

i) T is proper , ii) $-1 \notin T$,

iii) char (K) = 0 , $T \neq K$.

The proof follows from the definition and Lemma 1.

Using (P4'), an easy application of Zorn's Lemma shows that any proper preordering is contained in a maximal proper one. The maximal proper preorderings of level n are called orderings of level n denoted in general by P, P'....

For a more convenient manner of speaking we introduce the notion "ordering (preordering) of higher level" to name orderings (preorderings) of some level; as already done the attributes "higher level","level n" will often be dropped. In the same way we shall deal with the subgroup and semiorderings of type n to be introduced later.

Of course, orderings of higher level can only exist in field of characteristic zero; by Lemma 2 they are characterized in such fields as the maximal preorderings $T \neq K$.

Furthermore we deduce from Lemma 2:

COROLLARY. For any field K the following statements are equivalent:

i) K has orderings of level n ,

ii) $-1 \notin Q_n$,

iii) char K = 0 , $Q_n \neq K$.

In particular (n = 1), a field is real iff it admits orderings of level 1. This result is due to Artin- Schreier since the orderings of level 1 are just the usual orderings as we shall see in a moment.

Until the end of §1 we assume all fields to be of characteristic zero.

Let T be a preordering of level n and set

$$T_o = \bigcap_{P \text{ ordering}, T \subset P} P .$$

We want to show $T = T_o$. To this end assume the contrary. Pick $a \in T_o \setminus T$; since $a^{2^n} \in T$ we find $r \in \mathbb{N}$ with $a^{2^{r-1}} \notin T$ but $a^{2^r} \in T$. Set $T' := T - Ta^{2^{r-1}}$; then T' is preordering of level n. If T' were proper, there would exist an ordering P with $T \subset T' \subset P$. P would contain a and $-a^{2^{r-1}}$ and we would get the contradiction $-1 \in P$.

Therefore $T' = K$, and we get a representation $a^{2^{r-1}} = t - t' a^{2^{r-1}}$, $t, t' \in T$; hence $a^{2^{r-1}} \in T$.

We have proved:

THEOREM 1 i) Every proper preordering is contained in an ordering of level n.

ii) Every preordering is the intersection of all orderings in which it is contained.

A preordering T of level n is likewise of level m for $m \geq n$. We call T of exact level n if

$$K^{2^n} \subset T \ , \quad K^{2^{n-1}} \not\subset T.$$

THEOREM 2. The orderings of exact level n are precisely the subsets of K with the following properties:

$$0 \in P \ , \ P+P \subset P \ , \quad P^{\times} \text{ is a subgroup of } K^{\times},$$
$$K^{\times}/P^{\times} \text{ is cyclic, } [K^{\times}:P^{\times}] = 2^n.$$

If P is an ordering of exact level n then $K^{\times}/P^{\times}$ is generated by every class $\omega P^{\times}$ where $\omega^{2^{n-1}} \in -P$.

Proof. Let P be an ordering of exact level n. We first show for $a \in K^{\times}$: $a^2 \in P \Rightarrow a \in P \cup -P$. For if $a \notin P$ then $P+Pa$ is a preordering properly containing P, and hence $P+Pa = K$. Therefore $-1 = u + va$ for some $u,v \in P$, and we see $a \in -P$. By assumption we have $K^{2^{n-1}} \not\subset P$. Let ω be an element with $\omega^{2^n} \in P$, $\omega^{2^{n-1}} \notin P$; hence $\omega^{2^{n-1}} \in -P$. As already remarked, $P^{\times}$ is a group. For $a \in K^{\times}$, $a^{2^r} \in P^{\times}$ we prove by induction on r: $a \in P_o := \bigcup\limits_i \omega^i P^{\times}$. In case $r = 0$

we have $a \in P_o$. If $r \geq 1$, then $(a^{2^{r-1}})^2 \in P$ implies that $a^{2^{r-1}} \in P \cup -P$ and further that $a^{2^{r-1}} \in P$ or $(\omega^{2^{n-r}} a)^{2^{r-1}} \in P^{\times}$. In either case it follows that $a \in P_o$.

For the converse we take a subset $P \subset K$ satisfying the quoted conditions. P is obviously a proper preordering of level n for $K^{2^n} \subset P$, $K \neq P$, therefore

$$P = \cap P'$$

where P' ranges over all orderings containing P. Suppose $P \subsetneqq P'$ for all $P' \supset P$. Then we conclude $[K^{\times}:P'^{\times}] | 2^{n-2}$ implying $K^{2^{n-1}} \subset P'$ and finally $K^{2^{n-1}} \subset P$: a contradiction. Thus P has to be an ordering, obviously of exact level n.

In view of Lemma 2 one concludes from theorem 2: <u>orderings of level 1</u> are those subsets P of K satisfying:

$$P+P \subset P,\ PP \subset P,\ P \cup -P = K,\ P \cap -P = \{0\},$$

i.e. they are just the usual orderings. It is rather convenient to have a special name for orderings of level 1 and we call them <u>orders</u>.

With help of the orders of a field E.Artin [2 ; Satz 1] characterized the sums of quares, and this characterization was an important step toward his solution of the 17[th] problem of Hilbert. Pfister [45; Satz 21] extended this characterization to sums of the type $\Sigma\, x^2_{i_1 \ldots i_k}\, a_1^{i_1} \ldots a_k^{i_k}$ with given $a_1, \ldots, a_k \in K$. We shall obtain an analogous result replacing the sums of squares by sums of 2^n-th powers. For a generalization to semilocal rings see [41].

For a preordering $T \subset K$, $a_1,\ldots,a_k \in K$, we define $T[a_1,\ldots,a_k]$ to be the set of all polynomial expressions in $a_1,\ldots,a_k$ with coefficients from T:

$$a = \Sigma\, t_{i_1\ldots i_k}\, a_1^{i_1}\ldots a_k^{i_k}$$

$T[a_1,\ldots,a_k]$ is the smallest preordering containing T and $a_1,\ldots,a_k$. Theoerem 1, ii) implies that $T[a_1,\ldots,a_k]$ is the intersection of all orderings P where $T \subset P$, $a_1,\ldots,a_k \in P$. Restricting to $T = Q_n$ we obtain:

THEOREM 3. <u>$Q_n[a_1,\ldots,a_k]$ is the set of all elements which lie precisely in those orderings of level n which contain $a_1,\ldots,a_k$.</u>

Elements of the form $a = \sum_1^k x_i^2 a_i$ can be characterized in a similar manner [46], [12], [8], [41]. In order to extend this result to sums $\sum_1^k x_1^{2^n} a_i$ we make use of the notion of "T-module" [8].

Let T be a proper preordering of higher level of K. We call every non-empty subset M a T-module if the following conditions hold :

(M1) $M+M \subset M$ (M2) $TM \subset M$.

$M = \{0\}$, $M = T$, $M = K$ are the most simple examples of T-modules.

Suppose M is a T-module and $M^{\times}$ is not additively closed. Pick $m \in M^{\times}$ with $m, -m \in M^{\times}$. Since $Km = K$ we obtain from lemma 1: $K = KM = (T - T)m = Tm + T(-m) \subset M$, hence $M = K$.

We have proved

LEMMA 3. For a T-module M, $M \neq 0$, the following statements are equivalent:

i) $M^{\times} + M^{\times} \subset M^{\times}$, ii) $M \neq K$,

iii) $M \cap -M = \{0\}$.

Zorn's lemma shows the existence of maximal elements among all T-modules different from K; they are called maximal T-modules. Every T-module is contained in a maximal T-module. Let M be a maximal T-module and $a \in K \setminus M$. Since $M + Ta$ is a T-module properly containing M we have $M + Ta = K$. In particular there is an $m \in M$ with $m + ta = -a$ and hence $K^{\times} = M^{\times} \cup -M^{\times}$. Then M must be maximal (lemma 3). Therefore we obtain (compare [8, Satz 1]):

THEOREM 4. Let T be a proper preordering of higher level. Then

i) every T-module $M \neq K$ is contained in a maximal T-module,

ii) every T-module is the intersection of the maximal T-modules in which it is contained,

iii) <u>the maximal T-modules are precisely those subsets M of K satisfying</u>

$$\underline{M+M \subset M,\ TM \subset M,\ K = M \cup (-M),\ M \cap (-M) = \{0\}}.$$

It is a remarkable consequence of this theorem that an ordering of exact level $n \geq 2$ has indeed no oversets which are additively <u>and</u> multiplicatively closed but admits additively closed oversets having, in contrast to $P^{\times}$, the "index" 2. Here, for the first time, we find out a difference between orders and orderings of exact level $n \geq 2$.

We adopt the terminology of [46] (not of [47]) and call a maximal T-module S a <u>T-semiordering</u>; S shall be called <u>normed</u> if $1 \in S$. In case $T = Q_n$ we say semiordering of level n.

Let T be a preordering, $a_1,\ldots,a_k \in K$, then

$$T(a_1,\ldots,a_k) := \{\sum_{i=1}^{k} t_i a_i \mid t_1,\ldots,t_k \in T\}$$

is the smallest T-module containing $T \cup \{a_1,\ldots,a_k\}$. By theorem 4 it is the intersection of all T-modules M with $a_1,\ldots,a_k \in M$. In particular we get in the case of $T = Q_n$:

THEOREM 5. <u>$Q_n(a_1,\ldots,a_k)$ is the set of all elements which lie precisely in those semiorderings of level n which contain $a_1,\ldots,a_k$.</u>

Let P be an ordering of level n. Since $K^{\times}/P^{\times}$ is a cyclic group every subgroup U of $K^{\times}$, for which $P^{\times} \subsetneq U$ holds, contains -1. $P^{\times}$ is therefore maximal among the subgroups of $K^{\times}$ not containing -1. In short, $P^{\times}$ is a maximal subgroup without -1.

More generally, let U be an arbitrary maximal subgroup without -1. One easily sees that $K^{\times}/U$ is 2-primary and that every finitely generated subgroup of $K^{\times}/U$ is cyclic. If $[K^{\times}:U]$ is assumed to be finite, $K^{\times}/U$ must therefore be a cyclic group of order say 2^n, and it follows that $K^{2^n} \subset U$, $K^{2^{n-1}} \not\subset U$.

We call a subgroup U of $K^{\times}$ a subgroup of level n if $-1 \notin U$ and $K^{\times 2^n} \subset U$ holds; U has the exact level n if furthermore $K^{\times 2^{n-1}} \subset U$.

The following theorem is valid for $\mathrm{char}(K) \neq 2$; its proof is analogous to those of theorems 1, 2.

THEOREM 6. i) Every subgroup of level n is contained in such a maximal subgroup.

ii) a subgroup of level n is the intersection of all maximal subgroups in which it is contained,

iii) if U is a maximal subgroup of exact level n, then $K^{\times}/U$ is cyclic of order 2^n, and $K^{\times}/U = \langle\omega U\rangle$ for every ω with $\omega^{2^{n-1}} \in -U$.

Now let T be a proper preordering of level n of the field K, char (K) = 0. For every ordering $P \supset T$, $P^{\times}$ is a maximal subgroup of level n. The converse does not hold in general. In fact, there may exist maximal subgroups U (without -1) over T such that $P := U \cup \{0\}$ is not an ordering of level n. But there are preorderings for which the converse holds. They seem to play an important role in the theory of real fields [8], [13], in particular, they occur in the investigation of hereditarily-pythagorean fields. According to [8] a preordering T of higher level is called a <u>fan</u> (in German: Fächer) if for every maximal subgroup U over $T^{\times}$ the set $U \cup \{0\}$ is an ordering. In view of the theorems 2 and 6 one has only to require that <u>every maximal subgroup over T is additively closed</u>.

THEOREM 7. <u>For a proper preordering of level n the following statements are equivalent</u>:

i) <u>T is a fan</u>

ii) $$\bigwedge_{\substack{a \in K^{\times} \\ a^i \notin -T \text{ for } i \in \mathbb{N}}} T[a] = \bigcup_{i=o}^{2^n-1} Ta^i$$

<u>Proof</u>. i) ⇒ ii) Obviously $Ta^i \subset T[a]$. Since $-1 \notin V := \cup T^{\times} a^i$, the subgroup V is the intersection of maximal subgroups by theorem 6. These subgroups contain $T^{\times}$, and, since T is a fan, $V \cup \{0\} = \cup Ta^i$ turns out to be a preordering. Hence $T[a] \subset \cup Ta^i$. ii) ⇒ i) Let U be a maximal subgroup, $U \supset T^{\times}$. For $a \in U$ we obtain $a^i \notin -T$ for $i \in \mathbb{N}$ since $-1 \notin U$. Therefore $1+a = ta^i \in U$, and U is additively closed.

Every preordering above a fan T is again a fan. Furthermore, for every subgroup U without -1 and $U \supset T^{\times}$ it follows from theorem 6 that $U \cup \{0\}$ is likewise a preordering, hence a fan.

§2. Orderings of higher level and valuation rings

The connection between orders and valuation rings has been known since Baer and Krull [5], [42]. It was already implicitly contained in the fundamental paper of Artin and Schreier [4]. Some years ago Prestel [46] discovered that semiorderings of level 1 lead to valuation rings, too. Now we are going to investigate the analogous relations between orderings of higher level and valuation rings. Then we shall give some applications of Prestel's result.

For valuation theory we refer to [26], [49]. Let A be a valuation ring of a field K. We denote by I, U or $A^{\times}$, $U^{(1)}$, k its maximal ideal, group of units, group 1+I of 1-units, the residue field A/I, respectively. For $a \in A$ we often write $\bar{a}$ for $a + I \in k$. The group $K^{\times}/U =: \Gamma$ is called the value group of A and $v: K \to \Gamma \cup \infty$, $v(a) = aU$ if $a \in K^{\times}$, $v(0) = \infty$, its valuation. In order to avoid ambiquities concerning value groups we only deal with valuation arising in this way. If we start with a valuation $v: K \to \Gamma_v$ we denote the corresponding objects by A_v, I_v, U_v, U_v^1, k_v (or often by A, I,...) and assume $\Gamma_v = K^\times/U_v$. A valuation ring A of K is called a real valuation ring if $k = A/I$ is a real field. The real valuation rings are just the valuation rings of real places, i.e. the places $\lambda: K \to F \cup \infty$ where F is a real field. If K admits a real valuation ring, then K must be real itself.

Let P be an ordering of level n of the valued field (K,v). We already know char $(K) = 0$. Set $P_v := \{a + I_v \mid a \in P \cap A_v\} \subset k_v$. One easily verifies: $k_v^{2^n} \subset P_v$, $P_v + P_v \subset P_v$, $P_v P_v \subset P_v$. P is called compatible with v, denoted by $P \sim v$ or $P \sim A_v$, if P_v is a proper preordering of k_v. In this case we must have $\text{char}(k_v) = 0$.

LEMMA 4. The following statements are equivalent:
i) $P \sim v$, ii) P_v is an ordering, iii) $U_v^1 \subset P$,
iv) $\bigwedge_{a,b \in K^\times} [v(a) > v(b),\ a \in P \Rightarrow a-b \in P]$.

Proof. iii) and iv) are obviously equivalent. i) $\Rightarrow$ iii) Take $a \in I$ and assume $\varepsilon = 1+a \notin I$, then $-\varepsilon^{2^k} \in P$ for some $k \in \mathbb{N}$. But this implies $-1 = -\bar{\varepsilon}^{2^k} \in P_v$. iii) $\Rightarrow$ ii) The valuation v induces an epimorphism $K^\times/P^\times \to \Gamma/v(P^\times)$ with $\ker(v) = P^\times U/P^\times \cong U/U \cap P^\times$. Since $U^1 \subset P^\times$ we get an isomorphism $U/U \cap P^\times \simeq k^\times/P_v^\times$ and an exact sequence

$$1 \to k^\times/P_v^\times \to K^\times/P^\times \to \Gamma/v(P^\times) \to 1.$$

Hence $k^\times/P_v^\times$ is seen to be cyclic, and we have $P_v^\times \neq k^\times$. Now apply theorem 2. ii) $\Rightarrow$ i) is obvious.

COROLLARY. <u>If P is compatible with v, then</u>

$$\underline{[K^\times:P] = [k^\times:P_v^\times][\Gamma:v(P^\times)]}.$$

If $P \sim v$ we call P_v the ordering induced by P. We often write $\bar{P}$ for P_v. The exact level of $\bar{P}$ is related to P by the index formula of the corollary. In particular the exact level of $\bar{P}$ is less than, or equal to the exact level of P. Later we shall see, that all values compatible with the index-formula can occur for the exact level of $\bar{P}$.

We now want to prove that every ordering of higher level is compatible with a <u>real</u> valuation ring. For this purpose we make use of a representation theorem for "Stone-rings" proved by Dubois [21]. A partially ordered ring (R,P) is an associative ring with unity together with the positive cone of an order-relation:

(α) $P+P \subset P$, $PP \subset P$, $0,1 \in P$, $-1 \notin P$.

(R,P) is called a <u>Stone-ring</u> [21] if furthermore the following holds:

(β) $P \cap -P = \{0\}$,

(γ) $\bigwedge_{a\in R} \bigvee_{n\in\mathbb{N}} n\cdot 1 - a \in P$,

(δ) $\bigwedge_{a\in R} [\bigwedge_{n\in\mathbb{N}} 1+na \in P \Rightarrow a \in P]$.

Typical examples are given by compact Hausdorff spaces X if one takes $R = C(X) = C(X,\mathbb{R})$ and $P = C(X)^+ = \{f \in C(X) \mid \bigwedge_{x\in X} f(x) \geq 0\}$. Dubois proved in [21] that every Stone-ring admits an embedding $\varphi: R \to C(X)$ with $P = \varphi^{-1}C(X)^+$ for some compact Hausdorff space X. The representation theorem has the important consequence:

<u>in every Stone-ring the squares are positive</u>;

<u>a Stone-ring has no nilpotent elements</u>.

Now let P be an ordering of K, because of $char(K) = 0$ we have $\mathbb{Q} \subset K$. Set $\mathbb{Q}^+ = \{r \in \mathbb{Q} \mid r > 0\}$; then from $N \subset P^x$ we deduce $\mathbb{Q}^+ \subset P$. Assume $P \sim v$, v a valuation of K. Since $char\,(k_v) = 0$ we have $\mathbb{Q} \subset A_v$. From $\mathbb{Q}^+ \subset P$, $1+I_v \subset P$ we see for $a \in I_v$, $r \in \mathbb{Q}^+$: $r \pm a = r(1 \pm r^{-1}a) \in P$. Therefore, the ideal I is contained in the following set.

$$I(P) = \{a \in K \mid \bigwedge_{r\in\mathbb{Q}^+} r \pm a \in P\}.$$

A_v is a valuation ring, hence A_v encloses any ring $A \subset K$ in which I(P) is an ideal. Set

$$A(P) = \{a \in K \mid \bigvee_{r\in\mathbb{Q}^+} r \pm a \in P\},$$

$$Arch(P) = \{a \in A(P) \mid \bigwedge_{n\in\mathbb{N}} 1 + na \in P\}.$$

Considering $\mathbb{Q}^+ \subset P$, one verifies that A(P) is a ring and I(P) an ideal of A(P). To look for valuations v with $P \sim v$ therefore leads to the investigation of A(P) and I(P). For $Arch(P) \subset A(P)$ the conditions (α), (γ), (δ) are easily checked, and since $\mathrm{Arch}(P) \cap -\mathrm{Arch}(P) = I(P)$ we get [22], [23]

$$(A(P)/I(P),\ \mathrm{Arch}(P)/I(P)) \text{ is a Stone-ring,}$$

and consequently:

(*) $\bigwedge_{a \in A(P)} \bigwedge_{n \in \mathbb{N}} \frac{1}{n} + a^2 \in P$,

(**) $I(P) = \sqrt{I(P)}$.

Now all is prepared for the proof that A(P) is a valuation ring with maximal ideal I(P) and that $\bar{P}$ is moreover an order of $A(P)/I(P)$. The proof has three parts:

I. $a \in A(P),\ a \notin P \cup -P \Rightarrow a \in I(P)$, II. A(P) is a local ring with maximal ideal I(P), III. A(P) is a valuation ring, $\bar{P}$ an order.

ad I.) For $a \in A(P)$ with $a \notin P \cup -P$ we have $a^{2^k} \in -P$ for some $k \geq 1$ and hence $\frac{1}{n} - a^{2^k} \in P$ for $n \in \mathbb{N}$. (*) shows $\frac{1}{n} + a^{2^k} \in P$; therefore $a^{2^k} \in I(P)$. Finally $a \in I(P)$ because of (**).

ad II.) For $a \in A(P)$, $a \in I(P)$ we have to show $a^{-1} \in A(P)$. By I. we know $a \in P \cup -P$, say $a \in P$. Since $a \notin I(P)$ there is an $m \in N$ with $\frac{1}{m} - a \notin P$; hence $\frac{1}{2m} - a \notin P$. Suppose $\frac{1}{2m} - a \notin -P$, then $\frac{1}{2m} - a \in I(P)$, and finally $\frac{1}{m} - a = \frac{1}{2m} + (\frac{1}{2m} - a) \in P$. Therefore $\frac{1}{2m} - a \in -P$. Division by $-\frac{a}{2m}$ yields $2m - \frac{1}{a} \in P$ which proves $a^{-1} \in A(P)$ ($2m + \frac{1}{a} \in P$ is obvious).

ad III.) For $a \in P^{\times}$ we first show: $a \in A(P)$ or $a^{-1} \in I(P)$.

Since $\frac{a}{1+a}, \frac{1}{1+a} \in P$ we have $1 \pm \frac{a}{1+a}$, $1 \pm \frac{1}{1+a} \in P$, i.e. $\frac{1}{1+a}, \frac{a}{1+a} \in A(P)$. In case $\frac{1}{1+a}$ is a unit in A(P), then $a \in A(P)$, otherwise $\frac{1}{1+a} \in I(P)$ by II. The identity $1 = \frac{1}{1+a} + \frac{a}{1+a}$ shows $\frac{a}{1+a} \notin I(P)$ in this case. By II we get $\frac{1+a}{a} \in A(P)$ and hence $a^{-1} \in A(P)$.

By $\widetilde{A(P)}$ we denote the integral closure of A(P) in K. Taking $a \in K^{\times}$, we have $a^{2^n} \in P$. Therefore $a^{2^n} \in A(P)$ or $a^{-2^n} \in A(P)$ which proves $a \in \widetilde{A(P)}$ or $a^{-1} \in \widetilde{A(P)}$. We see that $\widetilde{A(P)}$ is a valuation ring and denote its maximal ideal by $\mathfrak{m}$. Since $\widetilde{A(P)}$ is integral over A(P) we have $I(P) \subset \mathfrak{m}$. Assume $a \in \widetilde{A(P)}$ but $a^{2^n} \notin A(P)$, then, as already proved, $a^{-2^n} \in I(P)$ which implies the contradiction $1 \in \mathfrak{m}$. Hence $a^{2^n} \in A(P)$ holds for every $a \in \widetilde{A(P)}$. With help of the identity

$$(2^n)!\ X = \sum_{h=o}^{2^n-1} \pm \binom{2^n-1}{h}[(X+h)^{2^n} - h^{2^n}]$$

we conclude $A(P) = \widetilde{A(P)}$. It remains to prove that the induced ordering $\bar{P}$ (P is compatible with A(P)) in $k = A(P)/I(P)$ is an order. But $k = \bar{P} \cup -\bar{P}$ is a direct consequence of I. $\bar{P}$ is moreover an archimedean order.

Taking into account that the overrings of a valuation ring are totally ordered by inclusion we have just proved:

THEOREM 8. Let P be an ordering of higher level of the field K and A(P), I(P) be defined as above. Then

i) A(P) is a real valuation ring with maximal ideal I(P),

ii) P induces an archimedean order in A(P)/I(P),

iii) a valuation ring A is compatible with P iff $A(P) \subset A$.

This theorem immediately yields

THEOREM 9. For $n \in \mathbb{N}$ and a field K, the following are equivalent:

i) K admits orderings of level n,

ii) -1 is not a sum of 2^n-th powers,

iii) -1 is not a sum of squares, i.e. K is real.

Proof. i) and ii) are equivalent by the corollary to lemma 2. iii) ⇒ ii) obvious. i) ⇒ iii) K has by theorem 8 a real valuation ring and hence is real itself.

This result also shows that proper preorderings of higher level can only exist in a real field because every one is contained in an ordering.

Let K be an infinite field, char (K) ≠ 2; if K is not a real field, then $K = Q_n$ holds for any $n \in N$. This follows from lemma 1 and the last theorem. A more comprehensive result is due to Joly [38; Théorème 6.15].

A valuation v of K is called 2-henselian, [20], [13] or chapt. II, if it has a unique extension to the quadratic closure of K. An equivalent property is the validity of Hensel's lemma for quadratic polynomials [20; §1]. By the result of [20] we see that a non-dyadic valuation is 2-henselian iff the group $U_v^{(1)}$ is 2-divisible, i.e. iff we have $1 + I = (1 + I)^{2^n}$ for all $n \in N$.

COROLLARY 1. <u>An ordering is compatible with any 2- henselian valuation</u>.

<u>Proof</u>. By theorem 9 K must be a real field and therefore k_v too [20; Satz 4]. v is seen to be non-dyadic; furthermore $U_v^{(1)} \subset P$ because of the 2-divisibility of $U_v^{(1)}$. Now apply lemma 4.

COROLLARY 2. <u>If a valuation ring is compatible with an ordering it must be real</u>.

<u>Proof</u>. The residue field admits an ordering.

So far, we have obtained an explicite description for the smallest valuation ring A(P) compatible with a given ordering P. We are now going to derive an analogous result for <u>all</u> valuation rings A, A~P. This is known in the case of orders, i.e. of orderings of level 1 [16], [40], [47; §7].

Let P be an ordering of higher level of K, F a subfield of K; we set

$$A(P,F) := \{a \in K \mid \bigvee_{r \in F \cap P^{\times}} r \pm a \in P\},$$

$$I(P,F) := \{a \in K \mid \bigwedge_{r \in F\cap P^\times} r \pm a \in P\}.$$

Then $A(P) = A(P,\mathbb{Q})$, $I(P) = I(P,\mathbb{Q})$ hold.

LEMMA 5. <u>$A(P,F)$ is a valuation ring compatible with P; $I(P,F)$ is its maximal ideal, and $F \subset A(P,F)$ holds.</u>

<u>Proof</u>. $A(P,F)$ and $I(P,F)$ are additively closed. To prove that $A(P,F)$ is a ring with ideal $I(P,F)$ we use the fact $1/2 \in P$ and the identity $2(rs + xy) = (r + x)(s +x) + (r - x)(s - y)$. $A(P,F)$ is surely an overring of $A(P)$, hence a valuation ring with maximal ideal , say, $\mathfrak{m}$. Since $I(P,F)$ is a proper ideal, $I(P,F) \subset \mathfrak{m}$. To show $I(P,F) = \mathfrak{m}$ we first prove $F^\times \subset A(P,F) \setminus \mathfrak{m}$. For it holds that $P\cap F \subset A(P,F)$, hence $F = P\cap F - P\cap F \subset A(P,F)$ since $P\cap F$ is an ordering of F. Pick $a \in \mathfrak{m}$, $r \in F\cap P^\times$; then $r \pm a = r(1 \pm r^{-1}a) \in P(1 + \mathfrak{m})$. But $1 + \mathfrak{m} \subset 1 + I(P) \subset P$. Therefore $r \pm a \in P$ proving $\mathfrak{m} \subset I(P,F)$.

Let $k = k(P,F)$ be the residue field of $A(P,F)$. k is an extension of $\bar{F} = \{a + I(P,F) \mid a \in A(P,F)\}$ and carries the ordering $\bar{P} = \{a + I(P,F) \mid a \in P\, A(P,F)\}$. Moreover

$$\bigwedge_{a \in k} \bigvee_{r \in \bar{F}\cap\bar{P}^\times} r \pm a \in \bar{P} \quad \text{holds.}$$

This gives rise to the following definition: Let $L|M$ be a field extension, P an ordering of L, $L|M$ is called

<u>archimedean relative to P</u> if

$$\bigwedge_{a \in L} \bigvee_{r \in M \cap P^{\times}} r \pm a \in P$$

holds or, equivalent, if $A(P,M) = L$.

LEMMA 6. <u>Algebraic extensions are archimedean relative to any ordering</u>.

<u>Proof</u>. Assume $L|M$ is an algebraic extension, P an ordering of L. Since $M \subset A(P,M)$ we have $A(P,M) \cap M = M$ and therefore $A(P,M) = L$ by [26; (9.8) Corollary].

Let v be a valuation of the field L. For any subgroup $\Sigma \triangleleft \Gamma = \Gamma_v$ set

$$\bar{\Sigma} := \{\alpha \in \Gamma \mid \bigvee_{\gamma,\gamma' \in \Sigma} \gamma \leq \alpha \leq \gamma'\} .$$

$\bar{\Sigma}$ is the convex (= isolated) subgroup generated by Σ.
We further set:

$$A_\Sigma := \{a \in K \mid a = 0 \vee \bigvee_{\gamma \in \Sigma} v(a) \leq \gamma\}$$

where $A = A_v$ is the valuation ring of v. A_Σ is a valuation overring of A and we have $A_\Sigma = A_{\bar{\Sigma}}$, $v(U_\Sigma) = \bar{\Sigma}$. Every (valuation) overring A_1 of A is of this type; for instance, $A_1 = A_\Sigma$ where $\Sigma = v(U_1)$. Hence the correspondence $\Sigma \mapsto A_\Sigma$ yields a bijection between the set of all overrings of A and the set of all convex subgroups of Γ [26; §7]. In case $A_1 = A_\Sigma$, Σ convex, we say: Σ belongs to A_1.

LEMMA 7. Let P be an ordering of K, $F_1 \subset F_2$ two subfields, and v the valuation associated with $A(P,F_1)$. Then $A(P,F_1) \subset A(P,F_2)$, and $A(P,F_2)$ belongs to the convex subgroup generated by $v(F_2^{\times})$.

Proof. Obviously, $A(P,F_1) \subset A(P,F_2)$. Put $\Sigma = v(F_2^{\times})$, $A_1 = A(P,F_1)_{\Sigma}$. If $a \in R_1$, $a \neq 0$ we find $b \in F_2^{\times}$ with $v(a) \leq v(b)$, i.e. $ab^{-1} \in A(P,F_1)$. Let P be of level n, then it follows with $r := b^{2^n} \in F_2 \cap P$ that $s \pm a^{2^n} r^{-1} \in P$ for some $s \in F_1 \cap P^{\times}$. Since $r \in P^{\times}$, we see $rs \pm a^{2^n} \in P$ and $a^{2^n} \in A(P,F_2)$. But $A(P,F_2)$ is integrally closed so $a \in A(P,F_2)$, i.e. $A_1 \subset A(P,F_2)$. Now take $a \in A(P,F_2)$, then $a^{2^n} \in P$ and $r - a^{2^n} \in P$ for some $r \in F_2 \cap P^{\times}$. Part iv) of lemma 4 shows $v(a^{2^n}) \leq v(r)$ since $v \sim P$. This means $a^{2^n} \in A_1$ and, as before, $a \in A_1$.

Now let P be an ordering, A a valuation ring of K compatible with P, and k its residue field. The valuation of $A(P) = A(P,\mathbb{Q})$ will be denoted by $v_{\mathbb{Q}}$. Let Σ be the convex subgroup of $v_{\mathbb{Q}}(K^{\times})$ belonging to $A \supset A(P)$. Furthermore let F be a subfield of R. Under this assumption we shall prove

THEOREM 1o. If F is a maximal subfield of A, then $A = A(P,F)$. More generally, the following statements are equivalent:

i) $A = A(P,F)$,

ii) $k/\bar{F}$ is archimedean relative to $\bar{P}$,

iii) $\underline{\Sigma = \overline{v_{\mathbb{Q}}(F^{\times})}}$.

From $\mathbb{Q} \subset A$ the existence of maximal subfields follows by Zorn's lemma. Therefore

COROLLARY. <u>Every valuation ring compatible with P is of the type A(P,F) for some subfield F.</u>

<u>Proof of theorem 1o</u>. Because of $\mathbb{Q} \subset F$ the statements i) and iii) are equivalent. That i) implies ii) has already been observed. ii) $\Rightarrow$ i) Let I be the maximal ideal of A and $a \in I$. For an element $r \in F \cap P^{\times}$ it follows from $F^{\times} \subset A^{\times}$, $1 + I \subset P$ that $r \pm a = r(1 \pm r^{-1}a) \in P$, i.e. $I \subset I(P,F)$ holds. Hence $I \subset A(P,F) \subset A$. For an element $a \in A$ there exists an element $r \in F \cap P^{\times}$ with $\bar{r} \pm \bar{a} \in \bar{P}$. If $\bar{r} = \bar{a}$ or $\bar{r} = -\bar{a}$, say $\bar{r} = \bar{a}$, we see that $a = r + u$, $u \in I$ holds, which implies $a \in A(P,F)$. We now assume $r \pm a \in A^{\times}$; in this case the result $r \pm a \in P$, i.e. $a \in A(P,F)$ follows from $\bar{r} \pm \bar{a} \in \bar{P}$ and the compatibility of P and A. If F is a maximal subfield of A, then for any $a \in A \setminus F$ $F(a) \not\subset A$ holds; hence we find a polynomial $f \in F[X]$, $f \neq 0$ with $f(a) \in I$. This shows that $k|\bar{F}$ is an algebraic extension, in particular archimedean relative to $\bar{P}$ by lemma 6.

So far we have investigated those valuation rings which are compatible with a given ordering of higher level. Now we fix a <u>valuation v with real valuation ring A</u> and we construct all orderings of an exact level n which are compatible with this valuation.

The value group Γ of v is torsion-free, from which one deduces (for example by induction) that Γ/Γ^{2^n} is a free $\mathbb{Z}/2^n\mathbb{Z}$-module; we have $\dim_{\mathbb{Z}/2^n\mathbb{Z}}(\Gamma/\Gamma^{2^n}) = \dim_{\mathbb{Z}/2\mathbb{Z}}(\Gamma/\Gamma^2)$. The epimorphism $v: K^\times/K^{\times 2^n} \longrightarrow \Gamma/\Gamma^{2^n}$, induced by the valuation $v: K^\times \to \Gamma$, therefore admits a homomorhpic section μ. For the subgroup $\bar{\mathfrak{A}} = \mu(\Gamma/\Gamma^{2^n}) \subset K^\times/K^{\times 2^n}$ we choose a system of representatives $\mathfrak{A} \subset K$, assuming $1 \in \mathfrak{A}$, without loss of generality,. For $a,b \in \mathfrak{A}$ there exists $x \in K^\times$ with $abx^{2^n} \in \mathfrak{A}$; each $\alpha \in \Gamma$ has a unique representation: $\alpha = v(a)\beta^{2^n}$, $\beta \in \Gamma$, $a \in \mathfrak{A}$.

The construction (relative to $\mathfrak{A}$) depends on some data subject to certain conditons. We start with

a subgroup $\Gamma_o \subset \Gamma$, an ordering $\bar{P}$ of k and a character $\chi: \Gamma_o \to k^\times/\bar{P}^\times$

satisfying the following conditions:

Γ/Γ_o is a cyclic group of order 2^r, $[k^\times:\bar{P}^\times] = 2^s$, $n = r + s$ and if $r > 0$: $\chi(\Gamma^{2^{n-1}}) \neq 1$.

Note that $\Gamma^{2^{n-1}} \subset \Gamma_o$ holds, since $s \geq 1$ and $r \leq n-1$. For $\bar{\mathfrak{A}}_o := \mu(\Gamma_o/\Gamma^{2^n})$ we denote by $\mathfrak{A}_o \subset A$ the according set of representatives. If $a \in \mathfrak{A}_o$, we write

$$M_a = \{\varepsilon \in A^\times \mid \bar{P}^\times\bar{\varepsilon} = \chi(v(a))\}.$$

Then we set

$$P := \bigcup_{a \in \mathfrak{A}_o} aM_a K^{2^n} .$$

THEOREM 11. (See [42; § 12] for n = 1) i) P is an ordering of exact level n, P is compatible with v and induces the given ordering $\bar{P}$ on k,

ii) every ordering of exact level n results in this way from the induced ordering of the residue field.

Proof. The cosets $\bar{P}^{\times}\bar{\eta}$ are additively closed, therefore $M_a + M_a \subset M_a$. $M_1 = \{\varepsilon \in A^{\times} \mid \bar{\varepsilon} \in \bar{P}^{\times}\} \supset 1+I$, hence $K^{2^n} \subset P$; moreover, this yields $P \sim v$, once P will have been proved to be an ordering. For $a,b \in \mathfrak{A}_o, \varepsilon \in M_a, \eta \in M_b$, $x,y \in K^{\times}$, we have to show: $t := a\varepsilon x^{2^n} + b\eta y^{2^n} \in P$, $s := ab\varepsilon\eta(xy)^{2^n} \in P$. If $v(a\varepsilon x^{2^n}) \neq v(b\eta y^{2^n})$, say $v(a\varepsilon x^{2^n}) > v(b\eta y^{2^n})$, then it follows that $t = a\varepsilon\varepsilon' x^{2^n}$, $\varepsilon' \in 1+I$, hence $t \in P$, since $\varepsilon\varepsilon' \in M_a$ holds. If $v(a\varepsilon x^{2^n}) = v(b\eta y^{2^n})$, then $a = b$ and $(yx^{-1})^{2^n} \in (A^{\times})^{2^n}$. Thus, $t = ax^{2^n}(\varepsilon + \eta(yx^{-1})^{2^n}) \in aM_a K^{2^n}$, because $M_a + M_a \subset M_a$. In order to prove $s \in P$, one first notices that there are $c \in \mathfrak{A}$, $z \in K$ with $ab = cz^{2^n}$. It remains to show: $\varepsilon\eta \in M_c$; from $v(a)v(b) = v(c)v(z)^{2^n}$ it follows that $\chi(v(a))\chi(v(b)) = \chi(v(c))$, as we have $\Gamma^{2^n} \subset (\Gamma_o)^{2^s}$, $[k^{\times}:\bar{P}^{\times}] = 2^s$; therefore $\bar{\varepsilon}\bar{\eta} \in \chi(v(c))$ and $\varepsilon\eta \in M_c$ holds and P is proved to be a preordering. By the choice of $\mathfrak{A}_o$, $v(P^{\times}) = \Gamma_o$ holds. Using $1+I \subset P$ and $\bar{P} = \overline{A \cap P}$, one obtains, as in the proof of lemma 3, the following exact sequence

$$1 \to k^\times/\bar{P}^\times \to K^\times/P^\times \to \Gamma/\Gamma_o \to 1.$$

Obviously $[K^\times:P^\times] = 2^n$ follows. Now we are going to show that the following statements are equivalent:

1) P is not an ordering,

2) $n > 1$ and $K^{2^{n-1}} \subset P$,

3) $r > 0$ and $\chi(\Gamma^{2^{n-1}}) = 1$.

With this we have also proved theorem 11 i); this equivalence will be used in the proof of ii), too. We shall make use of the following fact, which is a consequence of $[\bar{\mathfrak{A}}:\bar{\mathfrak{A}}_o] = [\Gamma:\Gamma_o] = 2^{n-s} | 2^{n-1}$: for $a \in \mathfrak{A}$ there is $a_o \in \mathfrak{A}_o$, $x \in K^\times$, with $a^{2^{n-1}} = a_o x^{2^n}$ (*).

1) $\Rightarrow$ 2). Obviously $n > 1$. P is the intersection of all orderings P' with $P \subset P'$. If P is not an ordering, then each P' must be of level $n - 1$, since $[K^\times:P^\times] = 2^n$ holds. In this case $K^{2^{n-1}} \subset P$ follows. 2) $\Rightarrow$ 3) In addition to (*) we find for $a \in \mathfrak{A}$ elements $a_1 \in \mathfrak{A}_o$, $\varepsilon \in M_{a_1}$, $y \in K^\times$ with $a^{2^{n-1}} = a_1 \varepsilon y^{2^n}$. Then it must follow that $a_o = a_1$ and $\varepsilon \in (A^\times)^{2^n}$, yielding $\bar{P}^\times = \varepsilon\bar{P}^\times = \chi(v(a_1)) = \chi(v(a^{2^{n-1}}))$. From $\Gamma = v(\mathfrak{A})\Gamma^2$ we deduce $\Gamma^{2^{n-1}} = v(\mathfrak{A}^{2^{n-1}})\Gamma^{2^n}$ and $\chi(\Gamma^{2^{n-1}}) = 1$. If $r = 0$, the above sequence would show that $K^\times/P^\times$ were cyclic of order 2^n. 3) $\Rightarrow$ 1) We have $n = r+s > s \geq 1$; therefore $\bar{\varepsilon}^{2^{n-1}} \in \bar{P}^\times$ and $\varepsilon^{2^{n-1}} \in M_1 \subset P$ for any

$\varepsilon \in A$. By (*) there is an element $y \in K^\times$ with $a^{2^{n-1}} y^{2^n} \in \mathfrak{a}_o$ for every $a \in A$. Because of $\chi(v(a^{2^{n-1}}))=1$, we conclude $1 \in M_{a^{2^{n-1}} y^{2^n}} = \{\varepsilon \mid \bar{\varepsilon} \in \bar{P}^\times\}$, hence $a^{2^{n-1}} \in P$. Each $x \in K$ is representable by $x = a\varepsilon y^2$, where $\varepsilon \in A^\times$, $y \in K$. Therefore $K^{2^{n-1}} \subset P$ holds, and in view of $[K^\times : P^\times] = 2^n$, $K^\times/P^\times$ cannot be cyclic.

Now we prove ii). Denote $\Gamma_o := v(P^\times)$, $\bar{P} := \overline{A \cap P}$; the character $\chi: \Gamma_o \to k^\times/\bar{P}^\times$ is to be defined as follows: for $u \in P$ set $\chi(v(u)) := \bar{\varepsilon}\bar{P}^\times$, where $u = a\varepsilon x^{2^n}$, $a \in \mathfrak{a}$, $\varepsilon \in A^\times$ holds. That χ proves to be a character is due to the above mentioned property: for $a,b \in \mathfrak{a}$ there exists $y \in K^\times$ with $aby^{2^n} \in \mathfrak{a}$. As the proof of lemma 3 shows, the first three of the required conditions are satified by Γ_o, $\bar{P}$, χ. One obtains $\mathfrak{a}_o = \{a \in \mathfrak{a} \mid v(a) \in \Gamma_o\}$. For $a \in \mathfrak{a}_o$ set $M_a := \{\varepsilon \mid \bar{\varepsilon} \in \chi(v(a))\}$. There is $u \in P$ with $v(u) = v(a)$, hence $a\eta = u$, where $\eta \in A^\times$. By definition of χ, we have $\bar{\eta}\bar{P}^\times = \chi(v(u)) = \chi(v(a))$. If $\bar{\varepsilon} \equiv \bar{\eta} \mod \bar{P}$, then $\varepsilon = \eta\lambda + z$ holds, where $\lambda \in P^\times \cap A^\times$, $z \in I$. The equations $\varepsilon = \eta\lambda'$, $\lambda' \in P$, and $aM_m \subset P$ follow from $1+I \subset P$. Therefore the inclusion $\bigcup_{a \in \mathfrak{a}_o} aM_a K^{2^n} \subset P$ is proved. Conversely, for $u \in P$, we find elements $a \in \mathfrak{a}_o$, $\varepsilon \in A$, $x \in K$ with $u = a\varepsilon x^{2^n}$. Because of $\bar{\varepsilon}\bar{P} = \chi(v(a))$ one gets $u \in aM_a K^{2^n}$, hence $P = \bigcup aM_a K^{2^n}$. Since P is an ordering, the equivalence 1) $\leftrightarrow$ 3) yields that if $r > 0$, then $\chi(\Gamma^{2^{n-1}}) \neq 1$

holds.

REMARK. The proof just given seems to suggest the conclusion that the assumption on the structure of Γ/Γ_o is not necessary at all. But it is easy to see that any character χ satisfies $\chi(\Gamma^{2^{n-1}}) = 1$, if $r > 0$ holds and Γ/Γ_o is not cyclic.

We shall now attend to the compatibility of preorderings of higher level and valuation rings. Let T be a proper preordering of higher level of the real field K, A a valuation ring of K with maximal ideal I, residue field k, and let $\pi: A \to k$ be the canonical epimorphism. T induces the preordering $\bar{T} := \overline{A \cap T} = \pi(A \cap T)$ of k. We define as with orderings: A is compatible with T, $A \sim T$, if $\bar{T}$ is a proper preordering. In that case k is necessarily a real field, and consequently A a real valuation ring.

LEMMA 8. The following statements are equivalent:

i) $A \sim T$, ii) $T[1 + I] \neq K$

iii) $A \sim P$ for some ordering $P \supset T$.

Proof. i) ⇒ ii) We have $-1 \notin \bar{T}$, which shows $T \cap -(1+I) = \emptyset$. We shall prove $T[1 + I] = T\cdot(1 + I)$, which obviously implies $T[1 + I] \neq K$. To this end we demonstrate that $T(1 + I)$ is a preordering. Only the proof that $T(1 + I)$ is additively closed is not trivial. Let v be the valuation associated to A, let $t,t' \in T$, $\varepsilon,\eta \in 1+I$; we have to show

$x := t\varepsilon + t'\eta \in T\cdot(1 + I)$. If $v(t\varepsilon) \neq v(t'\eta)$, say $v(t\varepsilon) > v(t'\eta)$, then one gets: $x = t\varepsilon\omega$, where $\omega \in 1+I$, hence $x \in T\cdot(1 + I)$. If $v(t\varepsilon) = v(t'\eta)$, then $t' = t\omega$, $\omega \in A^{\times}\cap T$, and $x = t(\varepsilon + \eta\omega)$. We see $\varepsilon + \eta\omega = 1 + \omega + p$, $p \in I$. Assume $1 + \omega \in I$, then $\omega = -[1 - (1 + \quad)] \in T \cap -(1+I)$ follows which is a contradiction. Therefore $\varepsilon + \eta\omega = (1 + \omega)[1 + (1 + \omega)^{-1}p] \in T(1 + I)$ and $x \in T(1 + I)$ holds. ii) $\Rightarrow$ iii) Since $T[1 + I]$ is a proper preordering, there exists an ordering P with $T \subset T[1 + I] \subset P$, in particular $A \sim P$. iii) $\Rightarrow$ i) From $A \sim P$ it follows that $\bar{P} \neq k$. But we have $\bar{T} \subset \bar{P}$ implying $\bar{T} \neq k$.

If $A \sim T$, then there exist by iii) orderings $P \supset T$ which are compatible with P. Such orderings are characterized by $P \supset 1+I$, $P \supset T$. Therefore the orderings over $T[1 + I]$ are precisely those orderings $P \supset T$ compatible with R. In general, there may exist orderings $P \supset T$ which are not compatible with A; this is the case iff $T[1 + I] \neq T$ holds. A and T are called <u>fully compatible</u>, if $1+I \subset T$ holds. Because of

$$\pi^{-1}(\bar{T}^{\times}) = (A^{\times} \cap T)(1 + I),$$

the full compatibility can be characterized as follows:

$$\pi^{-1}(\bar{T}^{\times}) \subset T.$$

Fully compatible preorderings are obtained by a lifting procedure for preorderings of the residue field:

LEMMA 9. <u>Let $\hat{T}$ be a proper preordering of level n of k, V a subgroup of $K^{\times}$ of level n satisfying $\pi(V \cap A^{\times}) \subset \hat{T}$. Then</u>

$$T := V \cdot \pi^{-1}(\hat{T}^{\times}) \cup \{0\}$$

<u>is a proper preordering of level n in K with $\bar{T} = \hat{T}$ which is fully compatible with A.</u>

<u>Proof</u>. From $\pi(V \cap A^{\times}) \subset \hat{T}$ follows $\bar{T} = \hat{T}$. Obviously $K^{2^n} \subset T$, $TT \subset T$ hold. Take $a,b \in V$, $\varepsilon,\eta \in \pi^{-1}(\hat{T}^{\times})$; let v be the valuation associated to A. If $v(a) \neq v(b)$, then $a\varepsilon + b\eta \in T$ follows as in the proof of lemma 8. But if $a = b\omega$, $\omega \in V \cap A^{\times}$ holds, the result $a\varepsilon + b\eta = b(\omega\varepsilon + \eta) \in T$ is implied by $\overline{\omega\varepsilon + \eta} = \bar{\omega}\bar{\varepsilon}\ \ \bar{\eta} \in \hat{T}^{\times}$. Since we have $1+I \subset T$, T is fully compatible with A.

LEMMA 10. <u>If the preordering T is fully compatible with A, then the following statements hold</u>:

i) <u>for every ordering $P \supset T$ $\bar{P}$ is an ordering over $\bar{T}$</u>,

ii) <u>every ordering $\hat{P} \supset \bar{T}$ is induced by an ordering $P \supset T$</u>: <u>$\bar{P} = \hat{P}$</u>,

iii) <u>$\pi^{-1}(A(\bar{P})) = A(P)$ for every ordering $P \supset T$</u>.

<u>Proof</u>. i) Of course we have $A \sim P$. ii) By lemma 9 $T_1 := T \cdot \pi^{-1}(\hat{P}^{\times})$ is a proper preordering with $\bar{T}_1 = \hat{P}$. Let P be an ordering, $P \supset T_1$, then $\hat{P} \subset \bar{P}$ holds. Since

$\bar{P} \neq k$, we see $\hat{P} = \bar{P}$. iii) This follows by direct calculations, taking into account that $A(P) \subset A$, $\pi^{-1}(\bar{P}^{\times}) \subset P$ hold.

Among the valuation rings fully compatible with a preordering T there exists a smallest one. Let

$$A_T = \langle \bigcup_{P \supset T} A(P) \rangle$$

be the valuation ring generated by all valuation rings A(P), P ordering over T.

THEOREM 11. <u>A_T is the smallest valuation ring which is fully compatible with T. The preordering $\bar{T}$ of the residue field k_T induced by T satisfies</u>

$$\underline{A_{\bar{T}} = k_T.}$$

<u>Proof</u>. Let I be the maximal ideal of A_T. We have $I \subset I(P)$ for every ordering $P \supset T$, hence $1+I \subset \bigcap_{P \supset T} 1+I(P) \subset \bigcap_{P \supset T} P = T$. This means that A_T is fully compatible with T. By definition and theorem 8, any valuation ring which is fully compatible with T has to enclose A_T. Let $\pi: A_T \to k_T$ be the canonical epimorphism. Lemma 10 yields $\pi^{-1}(A_{\bar{T}}) = A_T$, therefore $A_{\bar{T}} = k_T$.

Besides A_T, there exists a further ring which has great importance for T. We write

$$A(T) = \{a \in K \mid \bigvee_{r \in \mathbb{Q}^+} r \pm a \in T\}.$$

The following theorem was first proved by Pejas [44; Satz 4] for the case $T = Q_1$.

THEOREM 12. A(T) is a ring with K as its fields of fractions. Moreover it holds:

$$A(T) = \bigcap_{P \supset T,\ P \text{ preordering}} A(P) .$$

Proof. We **have** $A(T) \subset A(P)$ for $T \subset P$, hence $A(T) \subset \cap A(P)$. Obviously $\mathbb{Q} \subset A(T)$ holds. Take $a \in \cap A(P)$. If $a \in \mathbb{Q}$, then $a \in A(T)$ holds. Assume $a \notin \mathbb{Q}$; for every $P \supset T$ we then find $r_P \in \mathbb{Q}^+$ with $r_P - a \in P$. We assert: $T[\{a-r_P | P \supset T\}] = K$. For, otherwise, some ordering P_o would lie over this preordering, and it would hold simultaneously: $a - r_{P_o}, r_{P_o} - a \in P_o$. In view of $a \notin \mathbb{Q}$, this yields a contradiction. In particular we see $-1 \in T[\{a-r_P | P \supset T\}]$. But -1 is already contained in some subpreordering finitely generated over T, say $-1 \in T[a-r_1,\ldots,a-r_n]$. Choose $r \in \mathbb{Q}^+$ with $r > \max\{r_1,\ldots,r_n\}$. We claim that $r-a \in T$ holds. Let $P \supset T$ be any ordering. Since $-1 \in T[a-r_1,\ldots,a-r_n]$ there must exist i with $a-r_i \notin P$. Now note that $a \in A(P)$ holds, hence $a-r_i \in A(P)$. Since P induces an order (first level) in the residue field (theorem 8), it follows $A(P)^\times \subset P \cup -P$. If $a-r_i \in A(P)^\times$, then $a-r_i \in -P$ follows, equivalently $r_i-a \in P$. But this implies $r - a = (r - r_i) + (r_i - a) \in P$. If $a - r_i \in I(P)$, then $r_i - a$ also holds.

In this case, $r - a = (r - r_i) + (r_i - a) \in P$ follows from the definition of $I(P)$ and $r - r_i \in \mathbb{Q}^+$. These arguments are valid for any $P \supset T$, therefore $r - a \in T$. Correspondingly, we find $s \in \mathbb{Q}^+$ with $s + a \in T$. Thus we obtain $a \in A(T)$, and finally $A(T) = \cap A(P)$. In particular, $A(T)$ proves to be a subring of K. For every $t \in T$ we conclude $\frac{1}{1+t}, \frac{t}{1+t} \in A(T)$ from the identity $1 - \frac{1}{1+t} = \frac{t}{1+t}$. A further consequence states that T lies in the field of fractions of $A(T)$. Because of $T - T = K$ this field must coincide with K.

In general, $A(T)$ is not a valuation ring, however, there exists an important class of fans of level 1 for which $A(T)$ and A_T coincide, as we will see later on.

As announced at the beginning of this section, we shall now attend to the relation between semiorderings of level 1 and valuation rings, discovered by A. Prestel.

Let S be a normed semiordering of level 1. We set

$$A(S) := \{a \in K \mid \bigvee_{r \in \mathbb{Q}^+} r \pm a \in S\},$$

$$I(S) := \{a \in K \mid \bigwedge_{r \in \mathbb{Q}^+} r \pm a \in S\}.$$

THEOREM 13 (Prestel, [46; (1.8) and (1.5)], [47; p. 112ff]). A(S) is a valuation ring with maximal ideal I(S). The semiordering $\bar{S} := \overline{S \cap A(S)}$, induced by S, is even an order of the residue field $A(S)/I(S)$. Moreover, it holds that

$\underline{S \cap A(S)^{\times} = \{\varepsilon \mid \varepsilon \in A(S)^{\times},\ \bar{\varepsilon} \in \bar{S}^{\times}}\}$.

Only the last statement is not covered by the quoted references. Assume $\bar{\varepsilon} \in \bar{S}^{\times}$; if $\varepsilon \notin S$ then $-\varepsilon \in S$ and $-\bar{\varepsilon} \in \bar{S}^{\times}$ would follow. This would imply the contradiction $\bar{S} = A(S)/I(S)$. It seems to be a reasonable conjecture that an analogous statement remains valid for semiorderings of higher level.

LEMMA 11. *Let T be a preordering of level 1 of the field K. If T admits a normed T-semiordering which is not an order, then there exists a valuation $v\colon K^{\times} \to \Gamma$ with a real valuation ring satisfying $v(T^{\times}) \neq \Gamma$.*

Proof. Let v be the valuation associated to A(S). Suppose $v(T^{\times}) = \Gamma$ holds. For any $a,b \in S^{\times}$ there must consequently exist $t,t' \in T$, $\varepsilon,\eta \in A(S)^{\times}$ with $a = t\varepsilon$, $b = t'\eta$. We see $\varepsilon,\eta \in A(S)^{\times} \cap S$. By theorem 13, the set $A(S)^{\times} \cap S$ is a subgroup of $K^{\times}$, hence $ab = tt'\varepsilon\eta \in S$. But S is not an order by assumption.

Those preorderings of level 1, above which are at the most two orders, are easily identified as fans. They are called *trivial fans* [8]. Let A be a real valuation ring, $\hat{T}$ a fan of the residue field. The condition of theorem 7 immediately shows that the lifted preordering $K^{2^n}\pi^{-1}(\hat{T}^{\times})$ is a fan again, see [8; Lemma 7]. In particular, this procedure enables us to construct non-trivial fans from trivial ones. The following theorem by L. Bröcker states that all fans can be obtained in this manner.

THEOREM 14 (L. Bröcker, [13 ; (2.7)]) Let T be a non-trivial fan of K. Then,

i) $A_T \neq K$,

ii) $\bar{T}$ is a trivial fan of k_T.

Proof. (E. Köpping). Choose an order $P \supset T$ and set $S := T \cup \{-a \mid a \in P \setminus T\}$. S turns out to be a normed T-semiordering which is not an order, see [8 ;(11)]. By lemma 11 there is a valuation v with real valuation ring A satisfying $v(T^{\times}) \neq \Gamma$. Let Σ be the greatest convex subgroup of Γ contained in $v(T^{\times})$. The corresponding valuation $v_{\Sigma}: K^{\times} \to \Gamma/\Sigma$, $a \mapsto v(a)\Sigma$ belongs to the valuation ring A_{Σ}, which, being a coarsening of A, is itself a real valuation ring. By [13 ; (2.9)], A_{Σ} is fully compatible with T, hence $A_T \subset A_{\Sigma}$. Because of $\Sigma \subset v(T^{\times}) \subsetneq T$, we have $A_{\Sigma} \neq K$ and, a forteriori, $A_T \neq K$. That T induces a fan in the residue field k_T of A_T is a special case of the following general result: fans induce fans again in the residue fields of all valuation rings which are compatible. By theorem 11, we see for the fan $\bar{T} \subset k_T$, that $A_{\bar{T}} = k_T$ holds. But by the arguments just given, $\bar{T}$ has to be trivial.

COROLLARY (See [15; Theor. 1] in the case of $T=Q_1$). <u>A preordering T of level 1 is a fan iff $\bar{T}$ is a trivial fan of k_T.</u>

<u>Proof</u>. T lies above the fan $K^{2^n}\pi^{-1}(\bar{T}^{\times})$, since T is fully compatible with A_T.

This theorem has striking consequences for the valuation rings A(P), $P \supset T$. Since $\bar{T}$ is a trivial fan, one learns by lemma 10:

<u>if T is a fan of level 1, then there are at the most two different rings among the valuation rings A(P), $P \supset T$. There are two different rings iff $\bar{T}$ admits two orders $\hat{P}_1, \hat{P}_2$ with $\hat{P}_1, \hat{P}_2 \supset \bar{T}$ and $A(\hat{P}_1) \neq A(\hat{P}_2)$.</u>

For convenient speaking we agree that a preordering T of higher level is called <u>homogeneous</u> iff all valuation rings A(P), $P \supset T$, coincide or, equivalently, iff $A(T) = A_T$ holds. If T is homogenous, then all orderings $\hat{P} \supset \bar{T}$ of k_T are <u>archimedean orders</u> by theorem 7 (note $A(\hat{P}) = k_T$). We call T <u>strongly-homogeneous</u> iff there is only one order above $\bar{T}$, i.e. iff $\bar{T}$ is itself an order.

According to theorem 14 there are three possibilities, which in fact all occur:

i) T is homogeneous,

ii) A(T) is a valuation ring, $A(T) \neq A_T$, for $P \supset T$ it holds that $A(P) = A(T)$ or $A(P) = A_T$,

iii) there are two incomparable valuation rings $A(P_1)$,

$A(P_2)$, $P_1, P_2 \supset T$; moreover, $A(T) = A(P_1) \cap A(P_2)$ is not a valuation ring.

In [15] R. Brown has given a further characterization for the preordering $T = Q_1$ being a fan. This result is deducible from theorem 14, as E. Köpping has observed. At the same time it can be extended to the case of arbitrary preorderings T of level 1. To this end one has to make use of the fact that any place $\lambda: K \to \mathbb{R} \cup \{\infty\}$ with $\lambda(T) \subset \mathbb{R}^2 \cup \{\infty\}$ belongs to a valuation ring A(P) where $P \supset T$ holds. We have the following result (see [15];corollary 6): a proper preordering T of level 1 is a fan iff there are at the most two places $\lambda: K \to \mathbb{R} \cup \{\infty\}$ with $\lambda(T) \subset \mathbb{R}^2 \cup \{\infty\}$, and if additionally for two such places $T \cdot \lambda_1^{-1}(\mathbb{R}^\times) = T \cdot \lambda_2^{-1}(\mathbb{R}^\times)$ holds.

§3. The existence of orderings of higher level

THEOREM 15. Let K be a real field, either every ordering of higher level of K is an order, or there exist orderings of exact level n for any $n \in \mathbb{N}$.

Proof. Let P be an ordering of exact level $m \geq 2$. By theorem 8, P induces an order $\bar{P}$ in the residue field k of A(P). The formula in the corollary to lemma 4 shows

$[\Gamma:v(P^{\times})] = 2^{m-1} \geq 2$, therefore $\Gamma \neq \Gamma^2$ (v the valuation associated to A(P), Γ its value-group). Our construction of an ordering P' of exact level n shall be based on the order $\bar{P}$ of k. Therefore $r = n-1$ holds. A subgroup and a character χ satisfying the required conditions may be found, since Γ/Γ^{2^n} is a non-trivial free $\mathbb{Z}/2^n\mathbb{Z}$-module.

We shall now characterize those fields which have only orders as orderings of higher level.

THEOREM 16. <u>For a real field K the following statements are equivalent</u>:

i) <u>every ordering of higher level is an order,</u>

ii) <u>every normed semiordering of higher level is an order,</u>

iii) <u>every real valuation ring has a 2-divisible value-group,</u>

iv) <u>$Q_1 = Q_n$ holds for every n,</u>

v) <u>$Q_n = Q_{n+1}$ holds for some $n \in \mathbb{N}$.</u>

<u>Proof</u>. i) $\Rightarrow$ iv) We have $Q_n = \bigcap_{\substack{P \text{ ordering} \\ \text{of level } n}} P = \bigcap_{P \text{ order}} = Q_1$.

v) $\Rightarrow$ iii) For a real valuation ring A with value group Γ, $v(Q_n) = \Gamma^{2^n}$ always holds. By assumption, in this case $\Gamma^{2^n} = \Gamma^{2^{n+1}}$ follows for some n, hence $\Gamma = \Gamma^2$.

iv) $\Rightarrow$ v) Obviously.

iii) ⇒ i) Let P be an ordering of exact level $n \geq 2$, let A be a valuation ring compatible with P, such that $\bar{P}$ is an order. As already observed in the proof of theorem 15, we must have $\Gamma \neq \Gamma^2$.

i) ⇒ ii) Now we may apply iii) and iv). Since $Q_1 = Q_n$ holds for any $n \in \mathbb{N}$, a normed semiordering of higher level has already to be normed quadratic one. It has even to be an order by [46;(2.2)].

ii) ⇒ i) By theorem 4 the ordering P is enclosed by a normed semiordering. Since S is an order, P = S follows.

<u>REMARKS</u>. 1) The equivalence of v) and i) can also be seen from theorem 15. For by assuming v), there are no orderings of exact level n+1.

2) The statement v) is to be stressed once again because of its peculiarity: if for some $n \in \mathbb{N}$ every sum of 2^n-th powers is already a sum of 2^{n+1}-th powers, then it follows that for arbitrary $r,s \in \mathbb{N}$ the sums of 2^r-th powers coincide with the sums of 2^s-th powers.

If v is a valuation of K with 2-divisible value group, and $\tilde{v}$ an extension of v to an algebraic extension L|K, then, as valuation theory shows [26], the value group of $\tilde{v}$ is also 2-divisible. If $Q_1 = Q_2 = \ldots$ holds in K, then this must hold in any algebraic extension L|K, too. If L is real this follows from theorem 16, observing the aforesaid property of the value group; if L is not real, we have $L = Q_n$ in any case by lemma 2, corollary and theorem 9.

Real fields with a single order satisfy the condition iii), hence we conclude:

COROLLARY 1. Let L be an algebraic, not necessarily real extension of a field with a single order. Then holds in L:

$$Q_1 = Q_2 = \ldots = Q_n = Q_{n+1} \ldots$$

The corollary applies particularly to algebraic extensions of $\mathbb{Q}$.

COROLLARY 2. If every order of K is archimedean, then

$$Q_1 = Q_2 = Q_3 = \ldots \qquad \text{holds.}$$

Proof. Without loss of generality assume that L is real. The trivial one is the only real valuation ring of L, as a non-trivial real valuation ring would yield a non-archimedean order by the procedure quoted above ($\Gamma = \Gamma_o$, $n = s = 1$).

Theorem 16 shows the way how the class of Pasch-fields can be further subdivided. Recall that a real field is called a Pasch-field (= SAP-field = WAP-field, see [46], [25]) if every normed semiordering of level 1 (= quadratic semiordering) is an order. By [46;(2.2)], a real field is a Pasch-field if for every valuation v with real valuation ring and non 2-divisible value group ($\Gamma \neq \Gamma^2$) it holds that

$[\Gamma:\Gamma^2] = 2$ and the residue field has a unique order.

For further investigation of Pasch-fields, we require the following reflection on real valuation rings. Zorn's lemma shows that every real valuation ring contains a minimum real one. Let A be a minimal real valuation ring, P an ordering that is compatible with A. Because of $A(P) \subset A$, we see $A = A(P)$. In general, the rings A(P) are not minimal real valuation rings. For example, let k be a field with an archimedean order $\bar{P}_1$, and a non-archimedean order $\bar{P}_2$. Now consider the rational function field $K = k(X)$. The valuation ring $A = k[X]_{(X)}$ yields an order P with $A(P) = A$, $\bar{P} = \bar{P}_1$. But A is not minimal, because A can be properly refined by the valuation ring $A(\bar{P}_2)$ of k.

THEOREM 17. Let K be a Pasch-field and $n \in \mathbb{N}$, $n \geq 2$. Then the following statements hold:

i) for every real valuation ring A with a non-2-divisible value group, there exists a unique ordering P of exact level n which satisfies $A \sim P$,

ii) the mapping $P \mapsto A(P)$ induces a bijection between the set of all orderings of exact level n and the set of all minimal real valuation rings with non-2-divisible value group.

Proof. i) The residue field k of A has a unique order by the result [46;(2.2)] already mentioned. This order may be denoted by P_k. Let $A \sim P$, then $\bar{P} = P_k$ follows by theorem 16 and its corollary. From $[\Gamma:\Gamma^2] = 2$ one gets $[\Gamma:\Gamma^{2^k}] = 2^k$; moreover, $[\Gamma:\Gamma^2] = 2$ implies the existence of an element $\alpha \in \Gamma$ with the property $\Gamma^{2^{k-1}} = \Gamma^{2^k} \cup \alpha^{2^{k-1}}\Gamma^{2^k}$. Because of $[\Gamma:v(P^{\times})] = 2^{n-1}$ (lemma 4, corollary), the equation $v(P^{\times}) = \Gamma^{2^{n-1}}$ follows. The character $\chi: v(P^{\times}) \to k^{\times}/P_k^{\times}$, which belongs to P, is fixed by $\chi(\alpha^{2^{n-1}}) = -P_k^{\times}$, since $r = n-1 > 0$, $\chi(\Gamma^{2^{n-1}}) \neq 1$, $\chi(\Gamma^{2^n}) = 1$ hold. Therefore the data of P are independent of P. Consequently, P is uniquely determined by A and n.

ii) Since $\bar{P}$ is an order, we get $[\Gamma:\Gamma^2]$ from the index-formula applied to A(P). Assume $A \subset A(P)$ for a real valuation ring A. The value group of A is likewise non-2-divisible. Hence one can construct an ordering P' of exact level n compatible with A. Obviously $P' \sim A(P)$, because of $\dot{A} \subset A(P)$. But by i), we see $P' = P$, implying $A(P) = A(P') \subset A$. The remaining statements of ii) follow from i) and the previous reflections.

COROLLARY 1. <u>If K admits at the most 3 orders, then there exists for every $n \geq 2$ at the most one ordering of exact level n.</u>

<u>Proof</u>. A real valuation ring with non-2-divisible value group yields at least two orders of K for every order of

the residue field. This shows that K is a Pasch-field. Moreover, there exists at the most one minimal real valuation ring A with $\Gamma \neq \Gamma^2$.

A field K is called pythagorean if it is real and satisfies $K^2 = Q_1$.

COROLLARY 2. If K admits 2 orders precisely, and if $Q_1 = Q_2 = \dots$ does not hold, then there exists $\alpha \in K^\times$ satisfying:

i) $P^+ := Q_1 \cup \alpha Q_1$, $\bar{P} = Q_1 \cup -\alpha Q_1$ are the orders of K,

ii) $P_n := Q_n \cup -\alpha^{2^{n-1}} Q_n$ is for $n \geq 2$ the unique ordering of exact level n,

iii) $Q_{n-1} = Q_n \cup \alpha^{2^{n-1}} Q_n$ for $n \geq 2$,

iv) Q_n is a fan for $n \geq 1$.

If, in addition, K is pythagorean, then $Q_n = K^{2^n}$ even holds.

Proof. Since $Q_1 = Q_2 = \dots$ does not hold, K admits a real valuation ring A with non-2-divisible value group Γ. Let P_k denote the unique order of the residue field of A, $M_1 = \{\varepsilon \in A^\times \mid \bar{\varepsilon} \in P_k\}$. Choose an element $\alpha \in K^\times$ where $\Gamma = \Gamma^2 \cup v(\alpha)\Gamma^2$ holds. The previous arguments show that $P^+ = M_1K^2 \cup \alpha M_1K^2$, $P^- = M_1K^2 \cup -\alpha M_1K^2$ are the two orders of K, and that $P_n = M_1K^{2^n} \cup -\alpha^{2^{n-1}} K^{2^n}$ is the unique ordering of exact level n, $n \geq 2$. The set $M_1K^{2^n}$ is contained in all orderings of level n, hence $M_1K^{2^n} \subset Q_n$. The converse inclusion $Q_n \subset M_1K^{2^n}$ follows from $v(Q_n) = \Gamma^{2^n}$; therefore $Q_n = M_1K^{2^n}$. Since $[K^\times:P_n^\times] = 2^n$ holds, we see $[K^\times:Q_n^\times] = 2^{n+1}$ and $Q_{n-1} = Q_n \cup \alpha^{2^{n-1}} Q_n$. $P_n^\times$ is the sole maximal subgroup of exact level n over $Q_n^\times$, hence Q_n turns out to be a fan. If K is additionally pythagorean, we get from $[K^\times:K^{\times 2}] = 4$ via $[K^\times:K^{\times 2^n}] = 2^{n+1}$ the desired conclusion $K^{2^n} = Q_n$.

Examples for corollary 2 are easy to find. For example, consider the power-series field $K = \mathbb{Q}((X))$. K has two orders and the canonical valuation ring is a real one with value-group $\Gamma = \mathbb{Z}$. This shows $Q_1 \neq Q_2 \neq Q_3 \neq \dots$. $K = \mathbb{R}((X))$ is a pythagorean field and satisfies $K^{2^n} = Q_n$. An example of a field with 3 orders and orderings of exact level $n \geq 2$ will be given after theorem 24.

§4. Extension theory

Assume that L|K is a field extension, and L and K are equipped with orderings of higher level $\mathfrak{P}$ and P respectively. $\mathfrak{P}$ is called an <u>extension</u> of P, if $\mathfrak{P} \cap K = P$ holds. We shall denote this fact by $\mathfrak{P}|P$. The phenomenons, which occur at the extension of orderings, can already be demonstrated by a simple example.

Consider the fields $K = \mathbb{R}((X))$, $L = K(\sqrt{X}) = \mathbb{R}((X^{1/2}))$. The order P_1 with $P_1 \ni X$ admits two extensions to orders of L. The second order P_2 with $P_2 \ni -X$ is not extendable to an order of L, but P_2 is in fact extendable to the unique ordering of exact level 2 of L. More generally speaking, the ordering P_n of K, $n \geq 2$, has a unique extension to L, namely the unique ordering of exact level $n+1$ of L. This example shows that in the wider frame of all orderings of higher level orders may become extendable without being extendable to others. Secondly it shows that the exact level may change under extension (in fact it can only increase). For our purpose, we shall only be concerned with faithful extensions $(L,\mathfrak{P})$ of (K,P), i.e. such extensions which preserve the exact level: $[L^{\times}:\mathfrak{P}^{\times}] = [K^{\times}:P^{\times}]$. But the following method seems to work for other extension problems, too. The basic idea of this method consists in using the extension theory for valuations. The transfer from the latter theory will be carried out with help of the theorems 8 and 11.

We associate the valuation ring $A(P)$ to every ordering P. Relative to a system of representatives $\mathfrak{A}$, which is kept fixed, P may be constructed from $\bar{P}$, a subgroup Γ_o and a character χ on Γ_o. If $\tilde{P}$ is an extension of P on L, then we have the corresponding valuation ring $A(\tilde{P})$ extending A(P). Besides $A(\tilde{P})$, one has to investigate the new data $\tilde{\mathfrak{a}}$, $\tilde{P}$, $\tilde{\Gamma}_o$, $\tilde{\chi}$. Conversely, if an extension $\tilde{A}$ of A on L is given, then an extension $\tilde{P}$ may possibly be constructed by suitable data $\tilde{\mathfrak{a}}$, $\overline{\tilde{P}}$, $\tilde{\Gamma}_o$, $\tilde{\chi}$.

Adopting the usual notations of the valuation theory, we denote ramification index, residue degree and the number of extensions by e, f and g respectively. Since the valuations under consideration admit real residue fields, which means fields of characteristic zero, they are always defectless [26;§§18,20,(20.23)]. In particular, we have the equations $\sum_1^g e_i f_i = [L:K]$ and - in the case of a Galois extension - $efg = [L:K]$ at our disposal. Moreover, we shall use the fact that the decomposition of a valuation v in a finite extension $L = K(a)$ is determined by the decomposition of the irreducible polynomial of a over the henselian closure of (K,v) [26;(17.17)].

LEMMA 12. <u>Let P be an ordering of higher level of K, compatible with the valuation v; let $\bar{P}$ be the induced ordering in the residue field. Further, let $(L,\tilde{v})$ be an extension of (K,v) with residue field l. If</u>

i) <u>$e(\tilde{v}|v)$ is odd, and</u>

ii) <u>$\bar{P}'$ is a faithful extension of $\bar{P}$ to l,</u>

<u>then P admits a faithful extension $\tilde{P}$ to L with $\bar{\tilde{P}} = \bar{P}'$.</u>

<u>Proof</u>. From $[\tilde{\Gamma}:\Gamma] = e \equiv 1 \bmod 2$ we get isomorphisms $\Gamma/\Gamma^{2^n} \simeq \tilde{\Gamma}/\tilde{\Gamma}^{2^n}$, $\Gamma/\Gamma_o \simeq \tilde{\Gamma}/\Gamma_o\tilde{\Gamma}^{2^n}$, which are induced by the natural embedding $\Gamma \to \tilde{\Gamma}$. The first isomorphism enables us to use the system of representatives $\mathfrak{A}$ for the field L, too. The second shows $[\tilde{\Gamma}:\Gamma_o\tilde{\Gamma}^{2^n}] = [\Gamma:\Gamma_o] = [K^\times:P^\times]/[k^\times:\bar{P}^\times]$. Let $\tilde{P}$ be a faithful extension of P to L, satisfying $\tilde{P} \sim \tilde{v}$, $\bar{\tilde{P}} = \bar{P}'$. From $\tilde{v}(\tilde{P}^\times) \supset \Gamma_o\tilde{\Gamma}^{2^n}$, where n is the exact level of P, and the index-formula (lemma 4, corollary), we conclude $\tilde{v}(\tilde{P}) = \Gamma_o\tilde{\Gamma}^{2^n}$. Let $\iota: k^\times/\bar{P}^\times \xrightarrow{\sim} l^\times/\bar{P}'^\times$ be the isomorphism which is induced by the inclusion-map $k^\times \to l^\times$. Let $\chi: v(P^\times) = \Gamma_o \to k^\times/P^\times$ be the character belonging to P (relative to $\mathfrak{A}$). Assume $\alpha \in \tilde{v}(\tilde{P}^\times)$, say $\alpha = \alpha_o\omega^{2^n}$ where $\alpha_o \in \Gamma_o$, $\omega \in \tilde{\Gamma}$. We have $\alpha_o = v(u)$ for some $u \in P$ and $u = a\varepsilon x^{2^n}$ where $a \in \mathfrak{A}$, ε unit of v, $x \in K^\times$. By definition of χ, $\chi(\alpha_o) = \bar{\varepsilon} \in k^\times/\bar{P}^\times$ follows, therefore $\alpha = \tilde{v}(a\varepsilon y^{2^n})$, $y \in L$, and finally, $\tilde{\chi}(\alpha) = \varepsilon\bar{P}'^\times$, i.e. $\tilde{\chi}(\alpha) = (\iota\chi)(\alpha_o)$. With that we have shown that all data of $\tilde{P}$ are uniquely determined by Γ_o, $\bar{P}'$ and χ. Hence the extending ordering $\tilde{P}$ is unique. Conversely, we choose for the construction of the desired extension:

$$\tilde{\Gamma}_o := \Gamma_o\tilde{\Gamma}^{2^n},\ \tilde{\chi}(\alpha) = \iota\chi(\alpha_o) \text{ where } \alpha = \alpha_o\omega^{2^n},\ \alpha_o \in \Gamma_o,\ \omega \in \tilde{\Gamma}.$$

Then we construct an ordering $\tilde{P}$ on L of the same exact level as P, according to theorem 11, using $\mathfrak{A}$, $\bar{P}'$, $\tilde{\Gamma}_o$, $\tilde{\chi}$. $\tilde{P}$ turns out to be an extension of P, and $\tilde{P} \sim \tilde{v}$, $\bar{\tilde{P}} = \bar{P}'$ hold.

An extension $(L,\tilde{v})|(K,v)$ of valued fields is called <u>immediate</u>, if the residue fields and the value groups coincide:

$$l = k \quad \text{and} \quad \tilde{\Gamma} = \Gamma, \text{ i.e. } \quad e = f = 1.$$

COROLLARY. <u>Let $(L,\tilde{v})|(K,v)$ be an immediate extension, P an ordering of K, compatible with v. Then there exists a unique ordering $\tilde{P}$ of L, which extends P and is compatible with $\tilde{v}$. $\tilde{P}|P$ is a faithful extension.</u>

<u>Proof</u>. The existence and uniqueness of a faithful extension follows from lemma 12. Let $\tilde{P}$ be an ordering with $\tilde{P}|P$, $\tilde{P} \sim \tilde{v}$. Using the index-formula, we get $[K^\times:P^\times] \leq [L^\times:\tilde{P}^\times]$ from $\bar{\tilde{P}} = \bar{P}$, $\Gamma \supset \tilde{v}(\tilde{P}^\times) \supset v(P^\times)$. Because of the embedding $K^\times/P^\times \to L^\times/\tilde{P}^\times$, the other inequality holds trivially, hence $\tilde{P}|P$ is faithful.

THEOREM 18. <u>Let v be a valuation, P an ordering of K, $(\tilde{K},\tilde{v})$ the henselian closure of (K,v). Then the following statements hold:</u>

i) <u>$P \sim v \Leftrightarrow P$ is extendable to $(\tilde{K},\tilde{v})$,</u>

ii) <u>if $P \sim v$, then P admits a unique extension to $(\tilde{K},\tilde{v})$, and this one is faithful.</u>

Proof. By theorem 9, corollary 1, every ordering of $\tilde{K}$ is compatible with $\tilde{v}$. Since $(\tilde{K},\tilde{v})|(K,v)$ is an immediate extension [26;(17.19)], all statements follow from the preceding lemma and its corollary now.

Prior to the proof of the next statements, we want to give a remark about faithful extensions. Let P be an ordering of exact level n, L|K an arbitrary extension. We claim that P is faithfully extendable to L, iff the preordering of level n of K, which is generated by P, is proper; this preordering T consists of the special sums:

$$T = \{ \sum_{\text{finite}} a_i x_i^{2^n} \mid a_i \in P,\ x_i \in L\}.$$

The necessity is obvious. Conversely. let T be proper, then every ordering P, where $T \subset P$ holds, is a faithful extension because of the embedding $K^x/P^x \to L^x/\tilde{P}^x$. It follows from this criterion, with the help of the corollary of lemma 1, that there exists a faithful extension to an arbitrary algebraic extension L|K iff faithful extensions to all finite subextensions exist.

In the following, the degree [L:K] of an arbitrary algebraic field extension will be understood as a Steinitz-number or "supernatural" number. The concept of the pythagorean closure may be found in [19].

THEOREM 19. <u>Let P be an ordering of K, and L|K an algebraic extension. Then there exists a faithful extension to L in the following cases:</u>

i) <u>[L:K] is odd,</u>

ii) <u>L is contained in the pythagorean closure.</u>

<u>Proof</u>. Due to the preliminary remark we may assume that L|K is finite. Let v be the valuation associated to A(P). We know that $\bar{P}$ is an order. The extensions $\tilde{v}_i$ of v to L satisfy $\Sigma e_i f_i = [L:K] \equiv 1 \mod 2$. Hence we can find an extension $\tilde{v}$ with odd numbers e,f. Now $(L,\tilde{v})$ satisfies the conditions of lemma 12, since $\bar{P}$ is extendable to an order of the odd extension l [9 ;§2, no.4]. ii) By the construction of the pythagorean closure [6 ; p.46], it is sufficient to consider the case $L = K(\sqrt{1+a^2})$. The valuation v may be chosen as before, let k be its residue field, and $(\tilde{K},\tilde{v})$ its henselian closure. If $1+a^2 \in \tilde{K}^2$, then v is fully decomposed in L [26 ;(17.17)], i.e. $e = 1$, $f = 1$, $g=2$. Otherwise, then a has to be a unit of $\tilde{K}$, and $1+\bar{a}^2 \notin k^2$ must hold. In this case, L is an unramified extension where $l = k(\sqrt{1+\bar{a}^2})$ holds. It is easy to see now, that the conditions of lemma 12 are satisfied.

We shall now determine the number of faithful extensions of a given ordering.

THEOREM 20. Let $L|K$ be a finite extension, P an ordering of K. Then the number of faithful extensions of P to L is less than or equal to the degree $[L:K]$.

Proof. Let $\tilde{P}$ be an extension of P to L. Then $A(\tilde{P})$ is a real valuation ring, and, in fact, an extension of $A(P)$ because of $A(\tilde{P}) \cap K = A(\tilde{P} \cap K) = A(P)$. Because of $\sum_{1}^{g} e_i f_i = [L:K]$, it is sufficient to show: if $\tilde{A}$ is a real extension of A with ramification index e, residue degree f, then $\#\{\tilde{P} | \tilde{P}$ faithful extension of P, $\tilde{A} \sim \tilde{P}\} \leq ef$. Let $(\tilde{K},\widetilde{A(P)})$ be the henselian closure of $(K,A(P))$, P' the unique (faithful) extension of P to $\tilde{K}$ (theorem 18). Since $\widetilde{A(P)}$ is henselian, we see that $P' \sim \widetilde{A(P)}$ and $\widetilde{A(P)} \supset A(P')$. But from $\widetilde{A(P)} \cap K = A(P) = A(P') \cap K$ we get $\widetilde{A(P)} = A(P')$ in view of [26;(13.4)]. Let $\tilde{A}$ be a real extension of $A(P)$ to L. Let $\tilde{L}$ be a henselian closure of $(L,\tilde{A})$ with valuation ring $\tilde{A}'$; $\tilde{L}$ is assumed to extend $\tilde{K}$ [26;(17.17)]. Then $\tilde{A}'$ is an extension of $A(P')$, and we have $[\tilde{L}:\tilde{K}] = ef$ [26;(20.23)]. By theorem 18, the orderings of $\tilde{L}$ correspond bijectively with those orderings of L which are compatible with $\tilde{A}$; the correspondence is given by $\hat{P} \mapsto \hat{P} \cap L$. One sees from theorem 18 that $\hat{P}$ is a faithful extension of P' iff $\hat{P} \cap L$ is a faithful extension of P. Therefore, the further discussion may be restricted to the following case:

<u>P an ordering of K, A(P) a henselian valuation ring.</u>

Let $\tilde{A}$ be the unique extension of A(P) to L. $\tilde{A}$ is henselian again. Let k,l be their residue fields, Γ, $\tilde{\Gamma}$ their value-groups, respectively. We have a decomposition

$\tilde{\Gamma}/\Gamma = \bigoplus_{i=1}^{k} Z_i$ into cyclic subgroups Z_i of order, say t_i. Choose for each i a generator $\alpha_i\Gamma$ of Z_i. Due to char k = 0, L|K is tamely ramified. Therefore there are elements $a_1,\dots,a_k \in K$ with $L = T(\sqrt[t_1]{a_1},\dots,\sqrt[t_i]{a_k})$, $\tilde{v}(\sqrt[t_i]{a_i}) = \alpha_i$, T being the inertia field of L|K. This shows the existence of the following tower of field extensions:

$$K \subset F_o \subset F_1 \subset \dots \subset F_t = L$$

where $T \subset F_o$, $e(F_o|K)$ odd, $[F_{i+1}:F_i] = 2$ holds.

All fields F_i have the same residue field, namely l. The extension $F_{i+1}|F_i$ is purely ramified. Now let $\tilde{P}$ be an extension of P to an intermediate F of L|K. Obviously $\tilde{A} \cap F \supset A(\tilde{P})$, since $\tilde{A} \cap F$ is henselian. But from $(\tilde{A} \cap F) \cap K = A(P') = A(\tilde{P}) \cap K$ we again obtain $A(\tilde{P}) = \tilde{A} \cap F$. Hence, $\tilde{P}$ induces an archimedean order in the residue field of F. Therefore, lemma 12 yields: the number of faithful extensions of P to F_o equals the number of extensions of $\bar{P}$ to orders of l. But this latter number is that of embeddings of l in $\mathbb{R}$, extending the embedding $k \to \mathbb{R}$, which is induced by $\bar{P}$, hence $r \leq f$. It remains to show that an ordering of F_o admits at the most 2^t faithful extensions to L. The considerations above allow us to confine ourselves to the case $t = 1$. To be more precise, we shall study the following case:

<u>$[L:K] = 2$, $L|K$ purely ramified, $A(P)$ henselian.</u>

Let be $L = K(\sqrt{a})$, $\tilde{P}$ a faithful extension of P to L and $\omega\tilde{P}^\times$, $\omega \in K^\times$, a generator of $K^\times/P^\times$. Then $\omega\tilde{P}^\times$ is a generator of $L^\times/\tilde{P}^\times$. Because of $a = (\sqrt{a})^2$, a cannot have the maximal order in $L^\times/\tilde{P}^\times$. Hence there exists $i \in \mathbb{N}$, $u \in \tilde{P}$ with $a = \omega^{2i}u$. It necessarily follows that $u \in P$. Since $K(\sqrt{a}) = K(\sqrt{u})$ we may assume $a \in P$. $A(\tilde{P})$ is the unique extension of $A(P)$, moreover $\bar{\tilde{P}} = \bar{P}$ holds. We want to show that there are only two possibilities for the character $\tilde{\chi}$ associated to $\tilde{P}$, with which we would have established the proof. From $a = (\sqrt{a})^2 \in P$ $\sqrt{a} \in P \cup -P$ and $\tilde{v}(\sqrt{a}) \in \tilde{\Gamma}_o = \tilde{v}(\tilde{P})$ follow. From $\tilde{\Gamma} = \Gamma \cup \Gamma\tilde{v}(\sqrt{a})$ ($\tilde{\Gamma}$ value group of $\tilde{v}$) one concludes $\tilde{\Gamma}_o = \Gamma_o \cup \Gamma_o\tilde{v}(\sqrt{a})$ where $\Gamma_o = v(P^\times)$. We find a section $\mu: \Gamma/\Gamma^{2^n} \to K^\times/K^{\times 2^n}$ satisfying $\mu(v(a)\Gamma^{2^n}) = aK^{\times 2^n}$, since $v(a)^{2^{n-1}} \notin \Gamma^{2^n}$ holds. Moreover we may assume $a \in \mathfrak{A}$. Computations show that $\tilde{v}$ induces an isomorphism $(\mathfrak{A}L^{\times 2^n} \cup \mathfrak{A}L^{\times 2^n}\sqrt{a})/L^{\times 2^n} \cong \tilde{\Gamma}/\tilde{\Gamma}^{2^n}$. We choose a system of representatives $\tilde{\mathfrak{A}} \subset L^\times$ for $\mathfrak{A}L^{\times 2^n} \cup \mathfrak{A}L^{\times 2^n}\sqrt{a}$, and define $\tilde{\chi}$ relative to $\tilde{\mathfrak{A}}$. Then $\tilde{\chi}|\Gamma_o = \chi$ holds. Consequently there are only the possibilities $\tilde{\chi}(\tilde{v}(\sqrt{a})) = \pm 1$.

We can gain better estimates in the case of faithful extensions of orders. Let P be an order of K, $L|K$ a finite extension, A a valuation ring, compatible with P, and Γ its value group. Let $A_1,\dots,A_t$ be all <u>real</u> valuation rings extending A to L, $\Gamma_1,\dots,\Gamma_t$ their value groups respectively. By r_i, we denote the number of the faithful extensions of $\bar{P}$ to the residue field of A_i. Then the following statement holds:

LEMMA 14. <u>The number of faithful extensions is less than or equal to</u>

$$\sum_{i=1}^{t} r_i[\Gamma_i:\Gamma_i^2\Gamma].$$

<u>Proof</u>. Let $\tilde{P}$ be an order extending P. By the corollary of theorem 10, we find a subfield F of K with $A = A(P,F)$. Clearly $\tilde{P} \sim A(\tilde{P},F)$ and $A(\tilde{P},F) \cap K = A(P,F) = A$ hold. This means $\tilde{P} \sim A_i$ for some $i = 1,\dots,t$. Pick one extension $\tilde{A} \in \{\tilde{A}_1,\dots,\tilde{A}_t\}$. Let $\hat{P}$ be an order on the residue field of $\tilde{A}$ which extends $\bar{P}$. In order to prove this lemma, it is sufficient to show the following result (compare with the proof of theorem 20): the number of orders $\tilde{P}$ extending P and satisfying $\tilde{P} \sim \tilde{A}$, $\bar{\tilde{P}} = \hat{P}$ equals $[\tilde{\Gamma}:\tilde{\Gamma}\Gamma]$. If $\tilde{P} \cap K = P$, $\tilde{P} \sim \tilde{A}$, $\bar{\tilde{P}} = \hat{P}$ hold, then $\tilde{P}$ encloses the preordering $T := L^2P\{\varepsilon \in \tilde{A}^\times \mid \bar{\varepsilon} \in \hat{P}^\times\}$. Conversely, if $\tilde{P}$ is an order containing T, then we get $P \subset \tilde{P}$, $\tilde{P} \sim \tilde{A}$,

$\bar{\tilde{P}} \supset \hat{P}$ first, which finally implies $\tilde{P} \cap K = P$, $\tilde{P} \sim \tilde{A}$, $\bar{\tilde{P}} = \hat{P}$. The preordering T turns out to be a fan of level 1. From $v(T^{\times}) = \tilde{\Gamma}^2\Gamma$, $\tilde{A}^{\times} \subset T^{\times} \cup -T^{\times}$ one obtains $[L^{\times}:T^{\times}] = 2[\tilde{\Gamma}:\tilde{\Gamma}^2\Gamma]$ (see [8 ;lemma 7]). But over a fan of index $[L^{\times}:T^{\times}] = 2^{n+1}$ there lie 2^n orders, see [8 ;Satz 20] e.g..

COROLLARY. <u>Assumptions as in lemma 13. If P admits [L:K] extensions to orders of L, then every valuation ring lying over A is real, and, moreover, the value groups Γ, $\tilde{\Gamma}$ satisfy</u>

$$\tilde{\Gamma}^2 \subset \Gamma.$$

<u>In particular, the ramification index is a power of 2.</u>

<u>Proof</u>. As usual, g denotes the number of valuation rings lying over A. From $t \leq g$, $r_i \leq f_i$, $[\Gamma_i:\Gamma_i^2\Gamma] \leq e_i$, $[L:K] = \sum_1^g e_i f_i$, and lemma 13 follows the conclusion.

The next result is stated as an independent theorem, although it is a further consequence of lemma 13. We do not assume $L|K$ to be finite.

THEOREM 21. <u>Let $L|K$ be a Galois extension. For every real valuation ring of L, the inertia group relative to $L|K$ is an abelian group of exponent 2.</u>

<u>Proof</u>. We may confine ourselves to the case of finite Galois extensions. Let $\tilde{A}$ be a real valuation ring of L, $\tilde{P}$

be an order compatible with $\tilde{A}$, set $P := \tilde{P} \cap K$. By theorem 20, P admits at the most $[L:K]$ extensions to orders of L. Given $\sigma \in G(L|K)$, then $\sigma(\tilde{P})$ is an order again, and an extension of P. Assume $L = K(a)$, $f(x) = \mathrm{Irr}(a,K)$ and $\sigma(\tilde{P}) = \tilde{P}$ for $\sigma \in G(L|K)$. σ permutes the roots of $f(x)$, but does not change their order relative to $\tilde{P}$ because of $\sigma(\tilde{P}) = \tilde{P}$. This shows $\sigma(a) = a$, i.e. $\sigma = id$. Hence, P has exactly $[L:K]$ extensions to orders. By the corollary, $\tilde{\Gamma}/\Gamma$ is a group of exponent 2, and the inertia group is isomorphic to the character group of $\tilde{\Gamma}/\Gamma$ (there is no wild ramification in our case)[26;§20].

The exact number of faithful extensions of orders to Galois extensions has just been determined in the foregoing proof. This partial result can be extended to all orderings of higher type.

THEOREM 22. <u>Let L|K be a Galois extension, P, $\tilde{P}$ orderings of K, L respectively. Assume $\tilde{P}$ is a faithful extension of P to L. Then, by</u>

$$\sigma \mapsto \sigma(\tilde{P}),$$

<u>a bijection is given of the Galois group $G(L|K)$ onto the set of all faithful extensions of P to L.</u>

<u>Proof</u>. In view of theorem 20, it is sufficient to show the following statement for finite Galois extensions L|K: if $\sigma(\tilde{P}) = \tilde{P}$, $\sigma \in G(L|K)$, then $\sigma = id$ follows. For its proof,

we may even assume that $L|K$ is a cyclic extension, with σ as a generator of $G(L|K)$. In the case of $\tilde{P}$ being an order, we refer to the proof of theorem 21. If $\tilde{P}$ is not an order, then $A(\tilde{P})$ is a proper real valuation ring of L. Denote the decomposition field and the inertia field of $L|K$ relative to $A(\tilde{P})$ by Z and T respectively [26;§20]. Since $L|K$ is abelian, the extension $Z|K$ is Galois. Therefore, for $\tau := \sigma|_Z$ the following holds: $\tau(\tilde{P} \cap Z) = \tilde{P} \cap Z$. $A(\tilde{P} \cap Z)$ is a valuation ring lying over $A(\tilde{P} \cap K)$, the other extensions of $A(\tilde{P} \cap K)$ to Z are conjugate to $A(\tilde{P} \cap Z)$. From $\tau(A(\tilde{P} \cap Z)) = A(\tau(\tilde{P} \cap Z)) = A(\tilde{P} \cap Z)$, we obtain $Z = K$. σ induces, on the residue field of $A(\tilde{P})$, an automorphism $\bar{\sigma}$, satisfying $\bar{\sigma}(\bar{\tilde{P}}) = \bar{\tilde{P}}$. Since $\bar{\tilde{P}}$ is an order, we get $\bar{\sigma} = id$. This means $\sigma = id$ on T, and σ is contained in the inertia group. As just proved, $\sigma^2 = id$ and $[L:K] = 2$ follow. At the end of the proof of theorem 20, it was shown that one may assume $L = K(\sqrt{a})$, $a \in \tilde{P} \cap K$ and $\sqrt{a} \in \tilde{P}$ in the case of $\sigma \neq id$. But then $-\sqrt{a} = \sigma(\sqrt{a}) \in \sigma(\tilde{P})$, and $\sigma(\tilde{P}) \neq \tilde{P}$ follows.

So far the extension theorems yield consequences concerning the behaviour of sums of 2^n-th powers. One obtains directly from theorems 3,19 the following result.

THEOREM 23. Let $L|K$ be an odd extension, or L be contained in the pythagorean closure of K. Then

$$\underline{Q}_n(L) \cap K = \underline{Q}_n(K) \qquad \text{holds.}$$

Of course, the set of all sums of 2^n-th powers in a field F is denoted by $Q_n(F)$.

For the next application, we need the concept of the real closure. Let P be an ordering of higher level of K. On applying Zorn's lemma it is easily shown that there exists a maximal real algebraic extension of K admitting a faithful extension of P. Let R be such extension, $\tilde{P}$ a faithful extension of P to R: we call $(R,\tilde{P})$ a real closure of (K,P). If P is an order, then R is real-closed, and $\tilde{P} = R^2$ holds, as is known [4 ;Satz 1]. In this case R is called a real closure of K.

THEOREM 24. Let $(R,\tilde{P})$ be a real closure of (K,P). Assume P to be of exact level $n \geq 2$. Then the following statements hold:

i) R admits exactly 2 orders, and, for every $m \geq 2$, a unique ordering of exact level m,

ii) R is the intersection of two real closures of K and has no odd algebraic extensions,

iii) R carries a henselian valuation with real-closed residue field.

Proof. $(R,\tilde{P})$ has no more faithful algebraic extensions. Let v be the valuation associated to $A(\tilde{P})$. By theorem 18, v is henselian. Let r be its residue field. r carries the order $\bar{\tilde{P}}$. Let $l|r$ be a finite real extension contained in the real closure of $(r,\bar{\tilde{P}})$. According to [26;(27.1)], there is a (real) finite unramified extension $L|R$ with residue field l. P is faithfully extendable to L (lemma 12). Hence $l = r$ follows; and r turns out to be real-closed already.

Let $L|R$ be a real algebraic extension. The unique extension $\tilde{v}$ of v to L has a real residue field by [46;(2.10)] or theorem 9, corollaries 1,2, consequently the field r. This shows that the set L^{2^m} is a fan for every $m \in \mathbb{N}$, for pick $a \in L$ and assume that $a^i \notin -L^{2^m}$ holds for all $i \in \mathbb{N}$. If $\tilde{v}(a) \neq 1$, then $1+a \in L^{2^m} \cup L^{2^m}a$ follows, since the group $1 + I(\tilde{P})$ is divisible. If $\tilde{v}(a) = 1$, we first conclude $\bar{a} \in r^{2^m}$ using $r = r^2 \cup -r^2$, $r^2 = r^{2^m}$. Finally one gets $1+a \in L^{2^m}$. L^{2^m} turns out to be a preordering and, by theorem 7, even a fan.

We are now going to prove $[R^\times:R^{\times 2}] \leq 4$. For that purpose we show $\alpha^{2^{m-1}} \in -\tilde{P}$ where $\alpha \in R^\times$, $\alpha \notin R^2 \cup -R^2$. From this result one deduces the assertion. Assume $L = R(\sqrt{\alpha})$ where $\alpha \notin R^2 \cup -R^2$ holds. L is a real extension. Suppose $-1 \notin L^{2^n}\tilde{P}$. Since L^{2^n} is a fan, the set $L^{2^n}\tilde{P}$ would turn out to be a preordering. We would find faithful extensions of $\tilde{P}$ taking the orderings over $L^{2^n}\tilde{P}$. Therefore $-1 \in L^{2^n}\tilde{P}$, i.e. $-1 = x^{2^n}u$, $x \in L$, $u \in \tilde{P}$. From $L^{2^n} \cap R = R^{2^n} \cup \alpha^{2^{n-1}} R^{2^n}$ one gets $\alpha^{2^{n-1}} \in -\tilde{P}$. It is impossible that $[R^\times : R^{\times 2}] = 2$ holds, since otherwise R could not carry an ordering of level $s \geq 2$ because of $R^2 = R^{2^k}$.

Since R is pythagorean and $[R^\times : R^{\times 2}] = 4$ holds, R admits exactly 2 orders. Now the corollary 2 of theorem 14 yields statement i).

In view of the definition and theorem 19 R can only have extensions of degrees 2^t, $t \in \mathbb{N}$. The absolute Galois group $G(\bar{R}|R)$ is therefore a pro-2-group. For $F := R(\sqrt{-1})$ one deduces $[F^\times : F^{\times 2}] = 2$, for instance from [6 ;lemma 1]. Hence, F has exactly one quadratic extension. Carrying over this result to the Galois group $G(\bar{R}|F)$, we see that $G(\bar{R}|F)$ is pro-cyclic by [30 ;Theorem 12.5.3]. Choose $\omega \in G(\bar{R}|F)$, let σ be an involution in $G(\bar{R}|R)$. We want to show that $\sigma\omega$ is an involution again. Since $G(\bar{R}|F)$ is abelian, we see that $\sigma\omega\sigma\omega = \omega\sigma\omega\sigma$ and $(\sigma\omega)^2\sigma = \sigma(\sigma\omega)^2$. We now apply [4 ;Satz 8] to the fixed field of σ, and obtain $(\sigma\omega)^2 = 1$ or $(\sigma\omega)^2 = \sigma$, which finally implies $(\sigma\omega)^2 = 1$, $\sigma\omega \neq 1$. This argument is valid for an arbitrary element $\omega \in G(\bar{R}|F)$. Now take a generator ω of $G(\bar{R}|F)$.

Then we see that $G(\bar{R}|R)$ is generated by two involutions, hence, R is the intersection of two real-closed fields.

Two real closures related to the same order are known to be isomorphic. The analogous problem of isomorphy for the orderings of higher level will be solved in chapter IV.

We would now like to present an example of a field with three orders having orderings of any exact level. The rational function field $\mathbb{Q}(X)$ admits orderings of any level, since its real valuation rings have value groups isomorphic to $\mathbb{Z}$. Let P_1 be an ordering of exact level $n \geq 2$ of $\mathbb{Q}(X)$, and $(R_1, \tilde{P}_1)$ be a real closure of $(\mathbb{Q}(X), P_1)$. Let P_2 be an archimedean order of $\mathbb{Q}(X)$ and R_2 a real closure of $(\mathbb{Q}(X), P_2)$. The pythagorean field $K := R_1 \cap R_2$ is the intersection of 3 real-closed fields by theorem 24. In particular, we have $[K^\times : K^{\times 2}] \leq 8$. K is equipped with at least three orders, namely one archimedean extension of P_2 and at least 2 others which may be constructed by means of $A(\tilde{P}_1 \cap K)$ and $\overline{\tilde{P}_1 \cap K}$. Because of $[K^\times : K^{\times 2}] \leq 8$, K can carry at the most 4 orders. But in this case, K^2 has to be fan, and consequently all orders have to be non-archimedean by [8 ; 3rd section]. This is a contradiction, and everything is proved.

As remarked in the proof, the relations $R^{2^s} + R^{2^s} = R^{2^s}$ are valid for every $s \in \mathbb{N}$ in the real closures $(R,\tilde{P})$. This fact yields astonishing consequences for the 2^m-th powers of sums of 2^n-th powers. In the following theorem K need not be assumed to be real. Generally, the statement fails to be true for finite fields, e.g. $K = \mathbb{F}(9)$, $n = m = 1$.

THEOREM 25. <u>Let K be an infinite field, let $n,m \in \mathbb{N}$. For arbitrary $x_1,\ldots,x_r \in K$ there exist $y_1,\ldots,y_s \in K$ satisfying</u>

$$\underline{(x_1^{2^n} + \ldots + x_1^{2^n})^{2^m} = y_1^{2^{n+m}} + \ldots + y_s^{2^{n+m}}.}$$

<u>Proof</u>. We may assume char $K \neq 2$. If K is not real, then $K = Q_t$ holds for every $t \in \mathbb{N}$ by lemma 1 and theorem 9. If K is real, then $Q_{n+m} = \cap P$ where P ranges over all orderings of level n+m. Therefore we only need show $(\Sigma x_i^{2^n})^{2^m} \in P$ for every such P. Let $(R,\tilde{P})$ be a real closure of (K,P). We have $\Sigma x_i^{2^n} \in R^{2^n}$. Hence $(\Sigma x_i^{2^n})^{2^m} \in R^{2^{n+m}}$ holds. Because of $R^{2^{n+m}} \subset \tilde{P}$ we obtain $(\Sigma x_i^{2^n})^{2^m} \in \tilde{P} \cap K = P$.

We like to specialize the result of theorem 25 to the case of the rational function field $K = \mathbb{Q}(X_1,\ldots,X_r)$. Theorem 25 states the existence of a "generic" identity:

$$(X_1^{2^n} + \ldots + X_r^{2^n})^{2^m} = f_1(X)^{2^{n+m}} + \ldots + f_s(X)^{2^{n+m}}$$

where $f_1(X),\ldots,f_s(X) \in Q(X_1,\ldots,X_r)$ are rational functions. Such identities are explicitly known only in special cases. D. Hilbert proved in [34] that the f_i, $i = 1,\ldots,s$, may be chosen as linearforms if $n = 1$. Moreover, he considered arbitrary exponents instead of the 2-powers 2^n only.

§5 n-pythagorean fields

As already stated, a field is called pythagorean, if it is real and satisfies $K^2 + K^2 = K^2$. We call K <u>n-pythagorean</u>, $n \in \mathbb{N}$, if K is real and satisfies $K^{2^n} + K^{2^n} = K^{2^n}$. Pythagorean fields coincide with 1-pythagorean fields. K is called <u>∞-pythagorean</u>, if it is n-pythagorean for every $n \in \mathbb{N}$.

THEOREM 26. <u>Every n-pythagorean field is m-pythagorean for all $m \leq n$.</u>

<u>Proof</u>. We have the equality $(a^{2^m} + b^{2^m})^{2^{n-m}} = \Sigma c_i^{2^n} = d^{2^n}$ for some $d \in K$ by assumption and theorem 25. Since K is real, we obtain $a^{2^m} + b^{2^m} = d^{2^m}$.

A real field K is called strictly-n-pythagorean, if the set K^{2^n} is a fan or, equivalently, if every maximal subgroup of level n is additively closed. A strictly-n-pythagorean field is obviously n-pythagorean, the converse does not hold. If K is strictly n-pythagorean for every n, then K is called strictly-∞-pythagorean. Strictly-∞-pythagorean fields are equivalently characterized by the property that altogether every maximal subgroup of a higher level is additively closed. A strictly-n-pythagorean field is easily seen to be strictly-m-pythagorean for $m \leq n$, too. Strictly-1-pythagorean fields are called strictly-pythagorean in this work, see [11], [13], in [24] they are called superpythagorean.

That the set K^{2^n} is a fan can be checked by the following conditions which simplify the test of theorem 7:

$$(*) \qquad \bigwedge_{a \notin -K^{2^n}} \quad K^{2^n} + K^{2^n} a \subset \bigcup_{i=0}^{2^n-1} K^{2^n} a^i .$$

The proof is a simple application of theorem 7.

We shall now study n-pythagorean and strictly-n-pythagorean fields. Our interest applies mainly to strictly-n-pythagorean fields because these fields naturally occur in the study of hereditarily-pythagorean fields.

LEMMA 14. Given a pythagorean field, the following statements hold:

i) A_{K^2} is the smallest 2-henselian valuation ring of K,

ii) $A_{K^2} = A_{Q_n}$ for every $n \in \mathbb{N}$,

iii) if K^2 is homogeneous (strongly-homogeneous), then the same holds for Q_n, $n \in \mathbb{N}$.

Proof. i) Let I be the maximal ideal of A_{K^2}. From $1 + I \subset K^{\times 2}$ we obtain that $1 + I$ is 2-divisible and, finally, that A_{K^2} is a 2-henselian valuation ring. Every 2-henselian valuation ring is fully compatible with K^2, hence it has to enclose A_{K^2}.

ii) Obviously $A_{K^2} \subset A_{Q_n}$ holds. But A_{K^2} is 2-henselian, which implies $A_{Q_n} \subset A_{K^2}$.

iii) In the case of K^2 being homogeneous, the residue field k of A_{K^2} carries only archimedean orders. Given an ordering $P \supset Q_n$, the induced ordering $\bar{P} \subset k$ has to be an archimedean order by theorem 16, corollary 2. Therefore $A(\bar{P}) = k$ holds, from which we deduce $A(P) = A_{K^2} = A_{Q_n}$. In the case of K^2 being strongly-homogeneous, then $\bar{Q}_n$ turns out to be the unique ordering of k.

COROLLARY. <u>A real field is n-pythagorean (strictly-n-pythagorean), iff it admits a 2-henselian valuation ring with an n-pythagorean (strictly-n-pythagorean) residue field.</u>

<u>Proof</u>. The existence of such a valuation ring follows from lemma 14 and direct calculation. Conversely, let A be a 2-henselian valuation ring with an n-pythagorean residue field k. For $a_1,\dots,a_r \in k$ we obtain $t := a_1^{2^n} + \dots + a_r^{2^n} = b^{2^n}(\sum_1^1 \varepsilon_i^{2^n} + p)$ where $b \in K$, $\varepsilon_i \in A^{\times}$, $p \in I$. We have $\sum_1^1 \bar{\varepsilon}_i^{2^n} = \bar{\eta}^{2^n}$ for some $\eta \in A^{\times}$, hence, $t = b^{2^n}(\eta^{2^n} + p')$ where $p' \in I$, too. Since $1 + I$ is 2-divisible, we get $t = b^{2^n}\omega^{2^n} \in K^{2^n}$, as required. In order to prove that K is strictly-n-pythagorean, one may apply the condition (*) above.

This criterion applies to the generalized power-series-fields

$$k((\Gamma)) = \{f = \sum_{\gamma\in\Gamma} \alpha_\gamma X^\gamma \mid \text{supp}(f) \text{ well-ordered}\},$$

where k is a field, Γ a totally ordered abelian group[49]. $k((\Gamma))$ is naturally equipped with an henselian valuation which has the residue field k and the value group Γ. If $\Gamma = \mathbb{Z}$, we write $k((X))$ instead of $k((\mathbb{Z}))$, this is a common usage.

L. Bröcker [13] and, independently, R. Brown [15] recognized that strictly-pythagorean fields can be characterized by means of their valuations.

THEOREM 27. A pythagorean field is strictly-pythagorean iff the residue field of A_{K^2} admits at the most two orders.

Proof. If K is strictly-pythagorean, then the set K^2 is a fan. The assertion now follows by theorem 14. The residue field k of A_{K^2} is pythagorean again. If it carries at the most two orders, then k^2 turns out to be a trivial fan. Lemma 14, corollary , yields the required result.

COROLLARY 1. A strictly-pythagorean field is either strictly-∞-pythagorean, or $K^2 = Q_n$ holds for every $n \in \mathbb{N}$.

Proof. A_{K^2} is 2-henselian. Therefore it is sufficient to consider this alternative only for the residue field k of A_{K^2}. k admits at the most 2 orders, hence theorem 17, corollary, applies.

A field K is called euclidean, if K is real and K^2 is an order. Euclidean fields are precisely the pythagorean fields with a unique order. Euclidean fields turn out to be strictly-∞-pythagorean, we have the relations

$K^2 = K^{2^n}$, $n \in \mathbb{N}$.

COROLLARY 2. If K is a real field, then the following statements are equivalent:

i) K is strictly-∞-pythagorean,

ii) K is strictly-pythagorean and 2-pythagorean,

iii) K is pythagorean, and the residue field of A_{K^2} has a unique order,

iv) K^2 is a strongly-homogeneous fan.

Proof. i) $\Rightarrow$ ii) Clearly. ii) $\Rightarrow$ iii) Let k be the residue field of A_{K^2}. k is pythagorean. Suppose k has two orders, P_1, P_2. Then $k^2 \neq k^4$ must hold. Because of $k^4 + k^4 = k^4$, there exists an ordering P of k of exact level 2. The valuation ring $A(P)$ of k has a non-2-divisible value group. Therefore, one may obtain from the induced $\bar{P}$ at least 2 orders, hence P_1 and P_2. This shows $A(P) \sim P_1, P_2$ and $1 + I(P) \subset P_1 \cap P_2 = k^2$. $A(P)$ turns out to be a non-trivial 2-henselian valuation ring. Using $A(P)$, one might properly refine the ring A_{K^2} getting a 2-henselian valuation ring again. This result contradicts lemma 14, i). iii) $\Rightarrow$ iv) Since A_{K^2} is 2-henselian, K^2 is a fan, even strongly-homogeneous as follows directly from the definition.
iv) $\Rightarrow$ i) In particular, K^2 has to be a preordering. Hence, K must be pythagorean. The residue field of A_{K^2} is a pythagorean field with a unique order, i.e. an euclidean field. Now apply the corollary of lemma 14.

It is an astonishing consequence that a strictly-2-pythagorean field is in fact strictly-∞-pythagorean. Whether this holds for n-pythagorean fields is not known. But we would like to mention the following partial result. Let K be a real field with the property, that every ordering of higher level is already an order. For example, see §3. If K is n-pythagorean for some $n \geq 2$, then K has to be even euclidean, for K is pythagorean and $K^2 = Q_n = K^{2^n}$ holds. But this implies $K = K^2 \cup -K^2$, as required.

Chapter II The Relative Theory

§1 Ω-henselian valuation rings

Let $R, R', \dots$ be valuation rings of the field K. As hitherto we denote their residue fields by $k, k', \dots$ or $\bar{R}, \bar{R}', \dots$. If $R \subset R'$, then R induces a valuation ring $R/\!\!/R' := \pi(R)$ of $\bar{R}'$, where $\pi: R' \to \bar{R}'$ is the canonical epimorphism. In this way, one obtains a bijection between the valuation rings contained in R' - these are the refinements of R' - and the valuation rings of $\bar{R}'$.

LEMMA 1. Let $L|K$ be an algebraic extension, let $R \subset R'$ be valuation rings of K. Then the following statements hold:

i) every valuation ring $\tilde{R}'$ of L extending R' encloses an extension $\tilde{R}$ of R to L,

ii) over every extension $\tilde{R}$ of R to L there lies a unique extension $\tilde{R}'$ of R' to L.

Proof. i) Choose an extension of $R/\!\!/R'$ to $\bar{\tilde{R}}'$. It has a presentation $\tilde{R}/\!\!/\tilde{R}'$. $\tilde{R}$ turns out to be an extension of R.

ii) Let Γ be the value group of R, $\tilde{\Gamma}$ the value group of $\tilde{R}$. For a convex subgroup Σ of Γ we write $|\Sigma|$ for its convex closure in $\tilde{\Gamma}$. Thus, $|\Sigma| \cap \Gamma = \Sigma$. Conversely, let $\tilde{\Sigma}$ be a convex subgroup of $\tilde{\Gamma}$. Since $\tilde{\Gamma}/\Gamma$ is a torsion-group, we have $\tilde{\Sigma} = |\tilde{\Sigma} \cap \Gamma|$. Assume now $R' = R_\Sigma$ (compare with chapt. I, §2). Given any convex subgroup $\tilde{\Sigma}$ of $\tilde{\Gamma}$, we conclude $(\tilde{R}_{\tilde{\Sigma}}) \cap K = R_{\tilde{\Sigma}\cap\Gamma}$. This proves that $\tilde{R}_{|\Sigma|}$ is the unique overring of $\tilde{R}$ which extends R'.

As already explained in the introduction, the theory of hereditarily-pythagorean fields is based on a certain class of Galois extensions of a real field k. Accordingly, we also need a relative version of the henselian property of valuation rings. To this end, we first only make the hypothesis that $\Omega|K$ is a normal (possibly infinite) algebraic extension of the field K. A valuation ring R (or the valuation associated to R) of K is called <u>Ω-henselian</u>, if R admits a unique extension to Ω, [13]. Thus, the Ω-henselian valuation rings are precisely those which are indecomposed in Ω.

In the case of $\Omega = \bar{K}$, the algebraic closure of K, we prefer the term "henselian" instead of "$\bar{K}$-henselian". The familiar results on henselian valuations are transferred to the relative case by Bröcker [13] . In particular, the following holds:

R is Ω-henselian iff Hensel's lemma applies to every monic polynomial $f \in R[X]$ which splits into factors of degree 1 over Ω.

There always exist minimal Ω-henselian extensions $(\tilde{K},\tilde{R})$ of (K,R) in Ω. These are pairwise conjugate under $\mathrm{Aut}(\Omega|K)$, and are called the <u>Ω-henselian closures</u> of (K,R). They are immediate extensions of (K,R). In the special case of $\mathrm{char}\,\bar{R} = 0$, the Ω-henselian closures are characterized as the maximal immediate extensions of (K,R) in Ω [26;§14ff], [13].

LEMMA 2. i) <u>Every valuation ring R of K has a smallest Ω-henselian valuation overring,</u>
ii) <u>every overring of an Ω-henselian valuation ring is again Ω-henselian.</u>

<u>Proof</u>. ii) follows directly from lemma 1. i) Let $\tilde{R}$ be an extension of R to Ω. By [26;§14], the set $\{\sigma\tilde{R} \mid \sigma \in \mathrm{Aut}(\Omega|K)\}$ consists of all extensions of R to Ω. Let $\hat{\tilde{R}}$ be the valuation ring generated by all rings $\sigma\tilde{R}$, $\sigma \in \mathrm{Aut}(\Omega|K)$. Because of $\sigma\hat{\tilde{R}} = \hat{\tilde{R}}$ for any $\sigma \in \mathrm{Aut}(\Omega|K)$, we see that $\hat{R} := \hat{\tilde{R}} \cap K$ is an Ω-henselian valuation ring of K. Obviously $R \subset \hat{R}$. Let R' be an Ω-henselian valuation overring of R, and $\tilde{R}'$ its unique extension to Ω. By lemma 1 we may assume $\tilde{R} \subset \tilde{R}'$, which implies $\hat{\tilde{R}} \subset \tilde{R}'$ and $\hat{R} \subset R'$.

We are mainly interested in the following situation: <u>K real, $\Omega \supset K_2$</u>, where K_2 denotes the maximal (Galois)

2-extension of K.

THEOREM 1. Let K be real and $\Omega|K$ a Galois extension satisfying $\Omega \supset K_2$. Then K has a smallest Ω-henselian valuation ring.

Proof. In particular, any Ω-henselian valuation ring is 2-henselian. Thus, it is overring of every valuation ring $R(P)$, where P is an order of K. This shows that the family $\{R_\alpha\}$ of all Ω-henselian valuation rings is totally ordered by inclusion. Therefore, $R := \cap R_\alpha$ is a valuation ring. Let $\hat{R}$ be the smallest Ω-henselian valuation overring of R. Then $\hat{R} \subset R_\alpha$ holds for any α. Thus, $\hat{R} \subset \cap R_\alpha = R$, i.e. $R = \hat{R}$.

The smallest Ω-henselian valuation ring is called the Ω-henselian valuation ring of K.

§2. Prime-closed extensions and Artin-Schreier theory

The Artin-Schreier theory of the real closure of a field K refers to its algebraic closure. As already explained in the introduction, the results remain valid for certain other extension fields. A first example is given in [6].

We recall that for arbitrary algebraic extension $L|K$ the degree $[L:K]$ will be understood as a Steinitz-number or a "supernatural" number. Given a prime number p, the maximal (Galois) p-extension of a field K is denoted by $K_p|K$. If $K_p = K$, then K is called <u>p-closed</u>. Moreover, we set

$$\mathbb{P}(L|K) = \{p \mid p \text{ prime number}, p \mid [L:K]\}.$$

$\mathbb{P}(L|K)$ is called the set of prime numbers of $L|K$.

We shall study the following pairs (Ω, k) of fields:

<u>k a real field, $\Omega|k$ a Galois extension,</u>

<u>$2 \in \mathbb{P}(\Omega|k)$, $\Omega_p = \Omega$ for every $p \in \mathbb{P}(\Omega|k)$.</u>

An extension $\Omega|k$ of this type will be called <u>prime-closed</u>, compare with [13]. For every real intermediate field K of a prime-closed extension of $\Omega|k$ the extension $\Omega|K$ is also prime-closed.

Let $\Omega|k$ be prime-closed, then Ω contains the maximal 2-extension $k_2|k$. On the other hand, Ω is contained in the algebraic closure $\bar{k}|k$. Therefore, $k_2|k$ and $\bar{k}|k$ present the two extreme cases. The latter one is on the basis of the Artin-Schreier theory, whereas the extension $k_2|k$ has been studied in [6].

A prime-closed extension $\Omega|k$ does not always contain the p-th roots of unity for a $p|[\Omega:k]$. An example will be given later. An extension $\Omega|k$ is called <u>saturated</u> if it is prime-closed, and if for every $p|[\Omega:k]$, p a prime number, the p-th roots of unity lie in Ω. In fact, a saturated extension contains all p^n-th roots of unity, where $p|[\Omega:k]$

and $n \in \mathbb{N}$. $k_2|k$, $\bar{k}|k$ and $M|k$ are examples of saturated extensions, where M denotes the maximal solvable extension of k.

In order to construct further examples, take a class C of finite groups, which is closed as to the formation of subgroups, factorgroups, finite products, and group-extensions with kernel and factorgroup from C; moreover, C is assumed to contain all finite 2-groups and all finite p-groups for those prime numbers p, which divide the order of some group in C. Now take the maximal C-extension Ω of k, i.e. the maximal Galois extension $\Omega|k$ having a pro-C-Galois group, compare [50]. $\Omega|k$ turns out to be a prime-closed extension, since the Galois group $G(\Omega_p|k)$ is a pro-C-group for every $p \in \mathbb{P}(\Omega|k)$.

For example, in the case of $k_2|k$,we take the class of all finite 2-groups, in the case of $M|k$ we consider all solvable finite groups.

Now let $\mathbb{P}$ denote some set of prime numbers, assume $2 \in \mathbb{P}$. The class C of all $\mathbb{P}$-groups, i.e. of all finite groups,the orders of which have only prime factors of $\mathbb{P}$, satisfies the aforesaid conditions. Let Ω be the maximal $\mathbb{P}$-extension (=maximal C-extension) of the real field k. Obviously $\mathbb{P}(\Omega|k) \subset \mathbb{P}$. Equality holds, if k admits proper p-extensions for every $p \in \mathbb{P}$. Since $k = \mathbb{Q}$ has this property, we have proved:

THEOREM 2. <u>Given any set $\mathbb{P}$ of prime numbers, where $2 \in \mathbb{P}$, there exists a prime-closed extension $\Omega|k$ with $\mathbb{P}(\Omega|k) = \mathbb{P}$.</u>

For example, consider the maximal $\{2,7\}$-extension $\Omega|\mathbb{Q}$. Ω does not contain the 7-th roots of unity, and therefore presents an example of a prime-closed, but not saturated extension of $\mathbb{Q}$.

Now assume $\Omega|k$ to be prime-closed. Due to Zorn's lemma there are maximal real extensions of k in Ω. These extensions are called <u>the real closures of k in Ω</u>, for short, <u>the real Ω-closures of k</u>. According to the characterization of the real closure in the absolute case, the following theorem holds:

THEOREM 3. <u>Let R be an intermediate field of $\Omega|k$. Then the following statements are equivalent:</u>

i) <u>R is a real closure of k in Ω,</u>

ii) <u>$R(\sqrt{-1}) = \Omega$, $\Omega \neq R$,</u>

iii) <u>$1 < [\Omega:R] < \infty$.</u>

<u>Proof</u>. i) $\Rightarrow$ ii) Let F be a 2-Sylow-field of $\Omega|R$. $F|R$ is an odd extension, hence F is real again [9 ;§2, no.4]. But this implies $F = R$, and $\Omega|R$ proves to be a 2-extension. By assumption on $\Omega|k$, every quadratic extension of R is

contained in Ω. Thus, R admits no real quadratic extensions, which implies that R is euclidean and $\Omega = R(\sqrt{-1})$ [6;Sätze 1,3]. ii) ⇒ iii) Clearly. iii) ⇒ i) Let p be a prime divisor of $[\Omega:R]$, and F a p-Sylow-field of $\Omega|R$. We shall show that $\Omega = F_p$. Obviously $\Omega \subset F_p$ holds. But, on the other hand, $F_p \subset \Omega$, since Ω is p-closed. The maximal p-extension $F_p|F$ therefore turns out to be a proper, but finite extension. A theorem of Whaples, as stated in [6;Satz 3] or [54; Theorem 2], now says $p = 2$, F is euclidean. Because of $[F:R] < \infty$, R is also euclidean [6;lemma 2]. Ω is a non-real 2-extension of R, hence $\Omega = R(\sqrt{-1})$ by [6;Satz 3]. This finishes the proof.

COROLLARY. The non-trivial elements of finite order of $G(\Omega|k)$ are precisely the involutions of $G(\Omega|k)$.

By the proof of the last theorem, the real Ω-closures of k are euclidean fields. The real closures of k in $\Omega = k_2$ coincide with the minimal euclidean extensions, i.e. the euclidean closures of k [6;Satz 6]. The real closures of k in $\Omega = \bar{k}$ are plainly the real closures of k [6].

Let R be a real closure of k in Ω. Since R is euclidean, the set $P := R^2 \cap k$ turns out to be an order of k. If R_1 and R_2 are real Ω-closures of k, which are isomorphic over k, then they induce the same order in k. The converse is valid, too. First choose real closures $\bar{R}_i$ of R_i, with respect to the algebraic closure $\bar{k}$ of k. Since R_i carries a single order, we obtain $R_i^2 = \bar{R}_i^2 \cap R_i$, thus $\bar{R}_1^2 \cap k = \bar{R}_2^2 \cap k$. But it is well known ([4] or [7], [29], [39] for different proofs) that there exists a k-isomorphism $\sigma: \bar{R}_1 \cap \bar{R}_2$. As $\Omega | k$ is normal and $R_i = \Omega \cap \bar{R}_i$ holds, σ induces a k-isomorphism between R_1 and R_2.

A real Ω-closure of k has been proved to be euclidean. In view of [6 ;Satz 2], this implies $\mathrm{Aut}(R|k) = 1$.

Every order P of k is induced by a real Ω-closure R, i.e. $P = R^2 \cap k$, since the real field $k(\sqrt{P})$ is contained in Ω.

We summarize:

THEOREM 4. <u>Let $\Omega | k$ be prime-closed, and let R, R_1, R_2 be real Ω-closures of k. Then the following holds:</u>

i) $R_1 \underset{k}{\cong} R_2 \Leftrightarrow R_1^2 \cap k = R_2^2 \cap k$,

ii) <u>$\mathrm{Aut}(R|k) = 1$,</u>

iii) <u>every order of k is induced by some real Ω-closure of k.</u>

COROLLARY. <u>Every involution in $G(\Omega | k)$ is self-normalizing.</u>

This last statement follows from the theorem 3 and 4. See [27;(1.11)].

We shall now consider orderings of higher level in our relative situation. According to the absolute case - $\Omega = \bar{k}$, dealt with in chapt. I, §4 - we define: let P be an ordering of higher level of k, then a maximal extension $(R,\tilde{P})$ of (k,P) <u>in Ω</u>, where $\tilde{P}$ is a faithful extension, is called a <u>real Ω-closure of (k,P)</u>. The case of level 1, i.e. of orders, has just been settled by theorem 4. Theorem 24, from chapter I, which refers to the case of exact level ≥ 2 and $\Omega = \bar{k}$, can also be transferred to our relative situation.

THEOREM 5. <u>Let $\Omega|k$ be prime-closed, and $(R,\tilde{P})$ a real Ω-closure of (k,P). Assume that P has exact level $n > 2$. Then the following holds:</u>

i) <u>R admits precisely two orders and a unique ordering of exact level m for every $m \geq 2$,</u>

ii) <u>R is the intersection of two real Ω-closures of k and has no odd algebraic extensions,</u>

iii) <u>if A is the Ω-henselian valuation ring of R, and $\tilde{A}$ its extension to Ω, then the following holds:</u>

$$\bar{\tilde{A}} = \bar{A}(\sqrt{-1}),\ \bar{A} \text{ euclidean},\ \bar{\tilde{A}} \text{ 2-closed.}$$

<u>Proof</u>. Let $(\hat{R},\hat{P})$ be a real $\bar{k}$-closure of $(R,\tilde{P})$. From $\hat{R} \cap \Omega = R$ we obtain that $G(\Omega|R)$ is a subgroup of $G(\bar{k}|\hat{R})$. According to the proof of theorem 24, the following holds: $G(\bar{k}|\hat{R}) = \langle\sigma\rangle \cdot U$ where $\sigma^2 = 1$, $\sigma u \sigma = u^{-1}$ for $u \in U$, $U \simeq \mathbb{Z}_2$ (= additive group of the dyadic integers). This yields ii). Since $R = \Omega^\sigma \cap \Omega^\tau$, $\sigma^2 = \tau^2 = 1$ holds, R has to be pythagorean with $[R^\times : R^{\times 2}] \leq 4$. R carries the ordering $\tilde{P}$, the exact level of which is $n \geq 2$. Thus $[R^\times : R^{\times 2}] = 4$, and from chapt. I, theorem 17, corollary 2, we derive i). Moreover, R is even strictly-∞-pythagorean. By chapt. I, theorem 27, corollary 2, the 2-henselian valuation ring A_{R^2} of R has a euclidean residue field. But A_{R^2} is Ω-henselian, too, as $\Omega|R$ is a 2-extension. We even have $\Omega = R_2$. Since $\bar{R}(i)$ is 2-closed, we conclude that $\tilde{\bar{R}} = \bar{R}(i)$.

<u>§3 The relative pythagorean closure</u>

Given a prime-closed extension $\Omega|k$, it is quite natural to consider the intersection of all real Ω-closures of k. This intersection is, of course, a field which is called the <u>pythagorean closure of k in Ω</u>. We denote this field by $(\Omega|k)^*$. By theorem 2, corollary, $(\Omega|k)^*$ is the fixed field of that subgroup of $G(\Omega|k)$ which is generated by the torsion-elements. Hence $(\Omega|k)^*|k$ is a Galois extension. Moreover, $(\Omega|k)^*$ is pythagorean, being the intersection of pythagorean (even euclidean) fields. If $k \subset l \subset (\Omega|k)^*$, we have $(\Omega|l)^* = (\Omega|k)^*$.

In the special case $\Omega = k_2$, $(k_2|k)^*$ is by [6;Satz 10] the smallest pythagorean extension field k_{pyth} of k at all. Furthermore, $(k_2|k)^*$ can be constructed by successive adjoining square roots of sums of squares. The extension $(\bar{k}|k)^*$ was also investigated in [28], but from a different point of view. In [28], it is called "Galois order closure".

In the sequel, $\Omega|k$ is always assumed to be prime-closed.

THEOREM 6. (See [6; Satz 10, Korollar 3], [28;§1]). <u>$(\Omega|k)^*$ is the largest Galois extension of k in Ω, to which every order of k can be (faithfully) extended.</u>

<u>Proof</u>. Evidently every order of k is extendable to $(\Omega|k)^*$. Conversely, let L|K be any such Galois extension of k in Ω. Assume further that R is a real Ω-closure of k, inducing the order P on k. P admits an extension $\tilde{P}$ to L, and there is a real Ω-closure $\tilde{R}$, where $\tilde{R} \supset L$, $\tilde{R}^2 \cap L = \tilde{P}$ holds. Thus, by theorem 4: $\tilde{R} \underset{k}{\cong} R$. Since L|K is a Galois extension, we conclude $L \subset R$. This shows $L \subset \cap R = (\Omega|k)^*$.

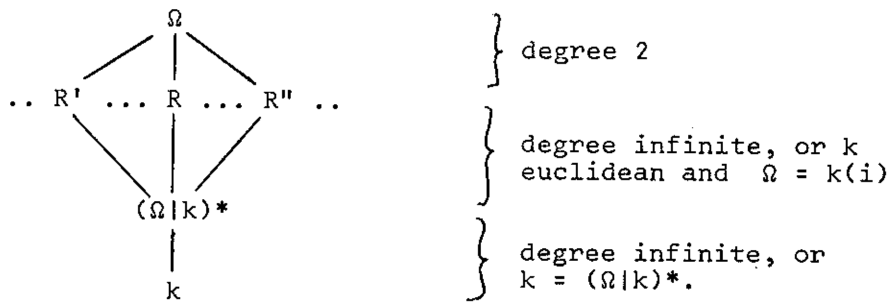
THEOREM 7. (comp. with [6 ;Satz 10,Korollar 4],[28;Corollary 16]). <u>$(\Omega|k)^*$ is the largest Galois extension of k in Ω with a torsion-free Galois group.</u>

Proof. If $k \subset L \subset \Omega$, and $L|K$ is a torsion-free Galois extension, then L has to be contained in the fixed field of any involution of $G(\Omega|k)$. This means: $L \subset (\Omega|k)^*$. For the converse, we have to show that $G((\Omega|k)^*|k)$ is torsion-free. If otherwise, there is an intermediate field L with $1 < [(\Omega|k)^*:L] < \infty$. Suppose the odd prime number p divides this degree. By assumption, the maximal p-extension of $(\Omega|k)^*$ is contained in Ω. But, in view of $[\Omega:R] = 2$ for every real Ω-closure R, it is even contained in every real Ω-closure. Thus, $(\Omega|k)^*_p = (\Omega|k)^*$. However, this result contradicts the theorem of Whaples [54;Satz 3]. Therefore $(\Omega|k)^*$ is a 2-extension of L. Since $[(\Omega|k)^*:L] < \infty$ and $(\Omega|k)^*$ is pythagorean, L proves also to be pythagorean [19;p.149]. Moreover, every order of L is (faithfully) extendable to $(\Omega|k)^*$, because of $(\Omega|k)^* = (\Omega|L)^*$. We have $(L_2|L)^* = L$, since L is pythagorean. Now theorem 6, applied to the extension $L_2|L$, yields the desired contradiction.

COROLLARY. Either $k = (\Omega|k)^*$, or $[(\Omega|k)^*:k] = \infty$ holds.

If a real Ω-closure R has finite degree over $(\Omega|k)^*$, then $(\Omega|k)^*$ has to be euclidean as well. Furthermore, $(\Omega|k)^*$ must have a trivial group of automorphism over k, being an euclidean algebraic extension of k. This implies $k = (\Omega|k)^*$ and $[\Omega:k] < \infty$. But considering the theorem of

Whaples, the degree $[\Omega:k]$ can be divided only by the prime number $p = 2$, thus, $\Omega = k(i)$. Consequently, as in [6], we obtain the following diagram concerning the structure of the extension $\Omega|k$:



It is well known that the quadratic extension $K(i)$, $i = \sqrt{-1}$, of a pythagorean field K contains all roots of unity of order a power of two [10 ;lemma 4]. This fact remains valid in a more general way. In order to derive the proper result, we need the following statement: let K be a real field, ζ a root of unity in $K(i)$, then $\zeta + \zeta^{-1} \in K$, for the norm $N_{K(i)|K}(\zeta)$ is a root of unity and a sum of squares in K at the same time. Thus, $N(\zeta) = 1$, and ζ^{-1} is conjugate to ζ over k.

THEOREM 8. <u>$(\Omega|k)^*(i)$ contains all roots of unity which lie in Ω.</u>

<u>Proof</u>. According to the foregoing remark, for every root of unity $\zeta \in \Omega$, and for every real Ω-closure R of k the element $\zeta + \zeta^{-1}$ lies in R. Hence, $\zeta + \zeta^{-1} \in (\Omega|k)^*$. Therefore, ζ satisfies a quadratic equation over $(\Omega|k)^*$, namely $\zeta^2 - (\zeta + \zeta^{-1})\zeta + 1 = 0$. But $(\Omega|k)^*$, being pythagorean, has only one non-real quadratic extension, that is $(\Omega|k)^*(i)$.

We obtain the special consequence that $(M|k)^*(i)$ contains all roots of unity.

§4 Generalizations

A detailed analysis of the proofs in the last two sections shows that some results hold under weaker conditions on the Galois extension $\Omega|k$. In favour of a homogeneous presentation, we have renounced giving the differentiated statements. However, many results on hereditarily-pythagorean fields can be proved on weaker assumptions. Therefore, we would now like to quote the more general versions of the required statements.

THEOREM 3'. Let Ω be a 2-closed Galois extension of the real field K, R an intermediate field. Then the following statements are equivalent:

i) R is a real Ω-closure of k,

ii) $R(\sqrt{-1}) = \Omega$, $\Omega \neq R$,

iii) $[\Omega:R] = 2^t$ for some $t \in \mathbb{N}$.

In the proof, one may use the part i) ⇒ ii) of the proof of theorem 3 and the result [6;Satz 3] on a characterization of euclidean fields.

If $\Omega|k$ is a 2-closed Galois extension, then the real Ω-closures are likewise euclidean fields. Thus, they induce via $R \mapsto R^2 \cap k$ all orders of k. Hence, the theorems 4,5,6,8 remain valid on the assumption that Ω is a 2-closed Galois extension of k (k real). With theorem 7, it is to be modified as follows:

THEOREM 7'. Let Ω be a 2-closed Galois extension of the real field k. Then $(\Omega|k)^*$ is the largest Galois extension of k in Ω with a 2-torsion-free Galois group.

Chapter III Hereditarily-Pythagorean Fields

§1. Theorems of characterization

In this section we start off with a 2-closed Galois extension $\Omega|k$ of the real field k. We shall study those real intermediate fields K, which are hereditarily-pythagorean (hereditarily-euclidean) - abbreviated by h.p. and h.e. - with respect to Ω, i.e. for which every real extension in Ω is pythagorean (euclidean). We shall characterize these fields in several ways.

THEOREM 1. Given a real intermediate field K of $\Omega|k$, then the following statements are equivalent:

i) K is hereditarily-pythagorean field with respect to Ω,

ii) $G(\Omega|K(\sqrt{-1}))$ is abelian,

iii) every non-real extension of K in Ω contains $\sqrt{-1}$,

iv) every real extension L of K in Ω is the intersection of its real Ω-closures, i.e. $L = (\Omega|L)^*$.

In chapt. IV, §1, we shall sharpen this result and prove that a real intermediate field K of $\Omega|k$ is h.p. iff the Galois group $G(\Omega|K)$ is meta-abelian.

Fields which are hereditarily-pythagorean, regarding their algebraic closure, are called absolutely hereditarily-pythagorean. If no confusion is to be expected, we drop the reference to the 2-closed extension $\Omega|k$, and simply use the term "hereditarily-pythagorean fields".

The proof will result from a series of lemmas. We always denote $i=\sqrt{-1}$. Given a 2-closed extension $\Omega|k$ and a real intermediate field K, then the extension $\Omega|K$ is again 2-closed. Hence, the results of chapter II, § 4 can be applied.

LEMMA 1. Let V be an abelian subgroup of $G(\Omega|K)$ with fixed field $F = \Omega^V$. Then either $\# V = 2$, or F is not real.

Proof. If F is real, then choose a real Ω-closure of F. $R|F$ is then an abelian extension. Because of $\mathrm{Aut}(R|F) = 1$, chapt. II, theor. 4, we obtain $R = F$ and $\# V = 2$.

LEMMA 2. Let $U = G(\Omega|K(i))$ be abelian and σ an involution in $G(\Omega|K)$. Then the following holds:

$$\bigwedge_{u \in U} \sigma u \sigma = u^{-1}$$

Proof. We set $W = \{\sigma u \sigma u \mid u \in U\}$. W is a subgroup of U, as U is abelian. Denote $F' := \Omega^W$. We have $\sigma(F') = F'$ and $G(\Omega|F) = \langle\sigma\rangle \cdot W$, where $F = (F')^\sigma$. $G(\Omega|F)$ is abelian because of $\sigma w = w\sigma$, for $w \in W$. But F is real, and we may apply lemma 1.

Before we come to the next lemma we would like to remark that a real field K is pythagorean iff K(i) is the only non-real quadratic extension.

LEMMA 3. The following statements are equivalent:

i) K is h.p. relative to K_2,

ii) every non-real extension in K_2 contains $\sqrt{-1}$,

iii) $G(K_2|K(\sqrt{-1}))$ is abelian.

Proof. i) ⇒ ii) We may assume that $L|K$ is a finite extension, $L \subset K_2$. Then there exists a chain of field extensions $K = L_o \subset L_1 \subset \ldots \subset L_r = L$, where $[L_j:L_{j-1}] = 2$ holds. Moreover, we find k such that L_k is real, hence pythagorean, but L_{k+1} is not real. By the foregoing remark, we see $i \in L_{k+1} \subset L$. ii) ⇒ III) Set $U = G(K_2|K(i))$. Thus, $G(K_2|K) = \langle\sigma\rangle\cdot U$ with some involution σ. Given $u \in U$, we set $F := K_2^{\sigma u}$. Because of $\sigma u(i) = -i$, F is a real field. Now lemma 1 shows $(\sigma u)^2 = 1$. This implies $\sigma u \sigma = u^{-1}$, and that U is abelian. iii) ⇒ i) By lemma 2 we have $G = \langle\sigma\rangle\cdot U$, where $\sigma u \sigma = u^{-1}$ holds. Hence, G is generated by the involutions σu, $u \in U$, which implies that K is pythagorean [6; Satz 10, Korollar 2]. These arguments are still valid for every real extension of K in K_2.

Now we interrupt the proof of theorem 1, and demonstrate how it can be determined in the base field K itself, whether K is h.p. relative to K_2. This statement can be found in [11] without proof.

THEOREM 2. <u>A real field is hereditarily-pythagorean relative to its maximal 2-extension iff it is strictly-pythagorean.</u>

<u>Proof</u>. If K is h.p. relative to K_2, then every real quadratic extension of K is also pythagorean. From [19; Sätze 2,4] we obtain that K^2 is a fan. Owing to the construction of the intermediate fields of $K_2|K$, we need only prove that any real quadratic extension $L = K(\sqrt{a})$ is likewise strictly-pythagorean. From the exact sequence

$$1 \to \{K^{\times 2}, aK^{\times 2}\} \to K^{\times}/K^{\times 2} \to L^{\times}/L^{\times 2} \to N(L^{\times})/K^{\times 2} \to 1 .$$

[6 ; page 43], we obtain $L^{\times} = K^{\times}L^{\times 2} \cup \sqrt{a}K^{\times}L^{\times 2}$, taking into account the relation $N(L^{\times}) = K^{\times 2} \cup -aK^{\times 2}$. Let U be a subgroup of $L^{\times}$, $-1 \in U$, $[L^{\times}:U] = 2$. For $P := K^{\times} \cap U$ we see $-1 \notin P$, $[K^{\times}:P] = 2$; Thus, P is additively closed, since K^2 is a fan. The order $P \cup \{0\}$ has two faithful extensions $\tilde{P}_1, \tilde{P}_2$ on L, because of $a = (\sqrt{a})^2 \in U \cap K^{\times} = P$. Observing $PL^2 \subset \tilde{P}_i$ and $[L^{\times}:PL^{\times 2}] = 4$, we conclude $PL^2 = \tilde{P}_1 \cap \tilde{P}_2$. Hence, PL^2 is a fan, and its overset $U \cup \{0\}$ has to be an order.

LEMMA 4. <u>Let $L|K$ be an arbitrary finite extension, where L is strictly-pythagorean. Then there exists $t \in \mathbb{N}$, satisfying the following conditions</u>:

i) <u>$[L^{\times}:K^{\times}L^{\times 2}] = 2^t$</u> ,

ii) an order of K, which is faithfully extendable to L, has precisely 2^t faithful extensions.

COROLLARY 1. If, in addition, [L:K] is odd, then an order has a unique extension to L, namely PL^2.

Proof. Generally, the number of faithful extensions is finite and congruent to [L:K] modulo2, [39; Prop. 5.2] or [37; page 289, Exc. 2].

COROLLARY 2. If, in addition, L|K is a Galois extension, then $[L:K] = 2^t$ follows.

Proof. Given a real Galois extension, the number of faithful extensions equals zero or [L:K], [39; Coroll. 5.1] or chapt. I, theorem 22.

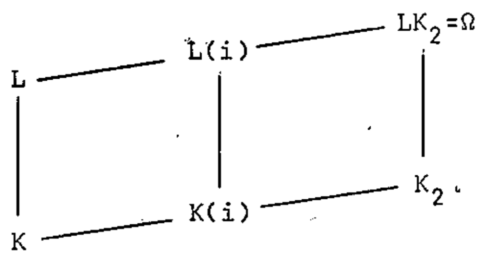
Proof of lemma 4. Let P be an order of K, faithfully extendable to L. Then $-1 \notin PL^2$ holds, and PL^2 has to be a preordering of L, as L^2 is a fan. The orders of L enclosing PL^2 are precisely the faithful extensions of P to L. They are of finite number, and correspond to the maximal subgroups of L, which contain $P^{\times}L^{\times 2}$. This correspondence is due to the fact that L^2 is a fan. Thus, $[L^{\times}:P^{\times}L^{\times 2}]=2^{t+1}$, $[L^{\times}:K^{\times}L^{\times 2}] = 2^t$, and there are 2^t faithful extensions.

LEMMA 5. If K is euclidean and h.p. relative to Ω, then K is even h.e. relative to Ω, and G(Ω/K(i)) is abelian of odd order.

<u>Proof</u>. Let L be a 2-Sylow-field of $\Omega|K$. L is real again, being an odd extension of K. Thus, L is h.p. relative to Ω. In particular, L turns out to be strictly-pythagorean because of $L_2 \subset \Omega$ and theorem 2. By lemma 4, corollary 1, L admits a single order. Hence, L is euclidean. But $\Omega|L$ is a 2-extension, which implies $\Omega = L(i)$ [6 ; Satz 3]. Consequently, $[\Omega:K(i)]$ is odd. Set $U = G(\Omega|K(i))$ and choose an involution $\sigma \in G(\Omega|K)$ and an element $u \in U$. Consider $F := \Omega^{\sigma u}$. Either $(\sigma u)^2 = 1$ holds, or F is not real by lemma 1. In the latter case, $[F:K]$ has to be even, which implies $i \in F$. For, if $i \notin F$, we would obtain $4|[F(i):K]$ contradicting the fact $[\Omega:K] = 2r$, r odd. But $i \in F$ is also a contradiction, as $\sigma u(i) = -i$ shows. Thus, $(\sigma u)^2=1$, or equivalently $\sigma u \sigma = u^{-1}$ must hold for every $u \in U$. This implies that U is abelian. Every real Ω-closure of K is an odd extension of K. Since every real extension L of K in Ω is contained in some real Ω-closure, L is likewise euclidean, by, say, lemma 4, corollary 1.

In order to prove a succeeding criterion, which will be formulated in theorem 3, i), we shall only assume in the sequel that K is h.p. relative to K_2, i.e. $G(K_2|K(i))$ is abelian, and that $G(\Omega|K_2)$ is abelian. As just proved, every h.p. field fulfils these assumptions, for we have $K_2 \subset \Omega$, and lemma 5 can be applied to every euclidean closure E (= real K_2-closure) of K. Note that $K_2 = E(i)$ holds.

First, we observe that $[\Omega:K_2]$ must be odd. Now choose a 2-Sylow-field L of $\Omega|K$. Then L(i) turns out to be a 2-Sylow-field of $\Omega|K(i)$. We have $\Omega = L_2$. Hence $[\Omega:K_2]$ and $[\Omega:LK_2]$ are relatively prime, implying $\Omega = LK_2$. Thus, we are presented with the following situation:



Being an odd extension of K, L has to be real. Moreover, $G(\Omega|L(i)) = G(K_2|K(i))$ is abelian, and, by lemma 3, L is shown to be h.p. relative to $\Omega = L_2$. Set $V = G(\Omega|L(i))$, $W = G(\Omega|K_2)$. On account of $L(i) \cap K_2 = K(i)$ (note $[L(i):K(i)]$ is odd), $G(\Omega|K(i))$ is generated by V and W. In order to prove that $G(\Omega|K(i))$ is abelian, we only need show that V and W are commutable. Let σ be an arbitrary involution of $G(\Omega|L)$ and set $E = K_2^\sigma$. E is an euclidean field where $K_2 = E(i)$ holds. By assumption, $G(\Omega|E(i))$ is abelian. From Lemma 2, we now derive $\sigma w \sigma = w^{-1}$ for an arbitrary $w \in W$. Now pick $v \in V$, $w \in W$ and an involution $\sigma \in G(\Omega|L)$. By lemma 2, σv is likewise an involution. Thus, as just remarked, we have $\sigma w^{-1}\sigma = w$, $(\sigma v)w(\sigma v)^{-1} = w^{-1}$. these two equations imply $vw = wv$.

So far, we have established the implication i) $\Rightarrow$ ii) of theorem 1. ii) $\Rightarrow$ iii). By lemma2, we have $G(\Omega|K) = \langle\sigma\rangle\cdot U$, $U = G(\Omega|K(i))$, $\sigma^2 = 1$, $\sigma u \sigma = u^{-1}$ where $u \in U$. If $L|K$ is a non-real extension in Ω, then $G(\Omega|L)$ has to be 2-torsion-free by chapt.II, theorem 3'. This proves $G(\Omega|L) \subset U$ and $L \supset K(i)$. iii) $\subset$ i) Let $L|K$ be a real extension in Ω, $F|L$ be a non-real extension. Being non-real, F has to contain the element $\sqrt{-1}$. By the remark before lemma 3, L turns to be pythagorean. ii) $\Rightarrow$ iv) See the proof of iii) $\Rightarrow$ i) in the proof of lemma 3. iv) $\Rightarrow$ i) follows from the fact that the real Ω-closures are euclidean.

Thus, the proof of theorem 1 has been concluded. As announced, statement i) of the following theorem has been proved, too.

THEOREM 3 *For a real intermediate field K of $\Omega|k$, the following statements hold:*

i) *K hereditarily-pythagorean relative to $\Omega \Leftrightarrow G(K_2|K(i))$, $G(\Omega|K_2)$ abelian,*

ii) *K hereditarily-euclidean relative to $\Omega \Leftrightarrow G(\Omega|K_2)$ abelian, $K_2 = K(i)$,*

iii) <u>K hereditarily-euclidean relative to $\Omega \Leftrightarrow [\Omega:K] = 2u$, u odd</u>.

<u>Proof</u>. Euclidean fields are characterized by $K_2 = K(i)$ among all real fields [6; Satz 3]. From this result, from lemma 5 and i) one proves ii). Due to lemma 5, we need only prove the implication "$\Leftarrow$" of iii). A real extension L of K in Ω has to be pythagorean, for, if otherwise, the pythagorean closure of L, which lies in Ω, would have the degree 2^∞, implying the contradiction $2^\infty | [\Omega:K]$. Hence, K is h.p. But K is likewise euclidean, since $[\Omega:K] = 2u$ enforces $[K_2:K] = 2$ and $K_2 = K(i)$. Applying lemma 5, one obtains the assertion.

The statements ii), iii) of theorem 3 can also be found in [48; (1.2) and (3.1)] for the absolute case $\Omega = \bar{k}$, compare with [27; 5.1] too.

REMARK. The proof of theorem 1 suggests a new formulation, stating in which cases the base field k, and not an intermediate field, is hereditarily-pythagorean. However, we prefer the formulation just given, since the extensions of k in Ω, which are hereditarily- pythagorean relative to Ω, may be regarded as generalizations of the real Ω-closures of k. this has already been explained in the introduction.

We shall now prove an entirely different characterization of h.p. fields. This one results from the investigation of sums of squares in the rational function field K(X). Since K(X) is not pythagorean, there are sums of squares in K(X), which are not squares.

THEOREM 4. <u>A real field K is absolutely hereditarily-pythagorean iff every sum of squares of K(X) is a sum of 2 squares</u>.

<u>Proof</u>. By [43; p. 314], every sum of squares of K(X) is a sum of 2 squares iff the level of every finite non-real extension equals one, i.e. iff all these fields contain $\sqrt{-1}$. Now theorem 1 yields the assertion.

This theorem enables us to show that every torsion-element of the Wittring W(K(X)) has an order at the most 2, if K is absolutely h.p. We would like to state, without proof, that over such constant fields the following statements, concerning the fundamental ideal I of W(K(X)) [43; p. 37], can be proved:

$$I^{n+1} \text{ is torsion-free } \Leftrightarrow [K^{\times}:K^{\times 2}] \leq 2^{n}.$$

For the proof, one may use Milnor's sequence for the Wittring of K(X) [43 ; p. 265 ff], furthermore some statements on the number of square classes in extensions of h.p. fields, which will be proved in §6, and, finally, the following result $W(L) \simeq \mathbb{Z}/2\mathbb{Z}[L^{\times}/L^{\times 2}]$ where $L = K(i)$, K strictly-pythagorean. This last statement can be deduced from the following theorem [53; Theor. 1], [8 ; Satz 21]: <u>A field K is strictly-pythagorean iff the Wittring W(K) is isomorphic to a group-ring $\mathbb{Z}[G]$. If K is strictly-pythagorean, then the canonical epimorphism $\mathbb{Z}[K^{\times}/K^{\times 2}] \to W(K)$, induces an isomorphism $\mathbb{Z}[P^{\times}/K^{\times 2}] \to W(K)$, where P is any order of K</u>.

§2. The Ω-henselian valuation ring and examples

Hereditarily-pythagorean fields show remarkable valuation-theoretical properties, as was first discovered by L. Bröker [13]. $\Omega|k$ is assumed to be a <u>2-closed Galois- extension</u> of a real field k in this section, too. According to chapt. II, theorem 1, k admits a smallest Ω-henselian valuation ring, its Ω-henselian valuation ring. This valuation ring is real. Now consider any real valuation ring A of k and an extension $\tilde{A}$ of A to Ω, then $\bar{\tilde{A}}|\bar{A}$ is a 2-closed Galois extension of the real field $\bar{A}$.

LEMMA 6. <u>Let K be a real intermediate field of $\Omega|k$, A a Ω-henselian valuation ring of K, and $\tilde{A}$ its extension to Ω. Then the following statements are equivalent:</u>

i) <u>K is h.p. relative to Ω,</u>

ii) <u>$\bar{A}$ is h.p. relative to $\bar{\bar{A}}$.</u>

<u>Proof</u>. Consider a real intermediate field L of $\Omega|K$. Set A_L for the extension of A to L. Since A_L is 2-henselian, because of $\Omega = \Omega_2$, we know by chapt.I, §5 that L is pythagorean iff $\bar{A}_L$ is pythagorean. From this, and the fact that every real intermediate field of $\bar{\bar{A}}|\bar{A}$ occurs as the residue field of a (even unramified) real intermediate field of $\Omega|k$, the assertion follows.

The following statement is a special case of a theorem of L. Bröcker [13; (1.5)].

LEMMA 7. <u>Let $\mathcal{V}$ be a set of pairwise incomparable, 2-henselian, non-dyadic valuation rings of the field F. If $\#\mathcal{V} \geq 2$ and F is generated by the valuation rings $A \in \mathcal{V}$, then F is 2-closed.</u>

<u>Proof</u>. We have to prove: $K = K^2$. First, assume that $\mathcal{V}$ is finite and, without loss of generality, even $\mathcal{V} = \{A_1, A_2\}$. Take $a \in K^x$. Since A_1 and A_2 are independent, there is an element b by the approximation theorem [26; § 11] satisfying: $a = b\varepsilon$, $1 = b\eta$, $\varepsilon \in 1 + I_1$, $\eta \in 1 + I_2$. The groups $1 + A_i$ are 2-divisible, hence $a \in K^2$.

Now consider the general case. Let $A \neq K$ be an arbitrary non dyadic, 2-henselian valuation ring of K. From the hypothesis on $\mathcal{V}$, the existence of a ring $A' \in \mathcal{V}$ follows such that A and A' are incomparable. Let $\tilde{A} = A \cdot A'$ be the valuation ring generated by A and A'. Then $A//\tilde{A}$ and $A'//\tilde{A}$ are two independent, 2-henselian, non-dyadic valuation rings of the residue field $\bar{\tilde{A}}$. Thus, $\bar{\tilde{A}}$ turns out to be 2-closed, hence $\bar{A} = \overline{A//\tilde{A}}$ is also 2-closed. Since A is 2-henselian, one obtains $A^{\times} = (A^{\times})^2$, i.e. every unit is a square. The rings of $\mathcal{V}$ generate F. Due to the first part of the proof, we may assume that this is not true for any finitely many rings of $\mathcal{V}$. Now choose $a \in K^{\times}$, $A_1 \in \mathcal{V}$. If $a \in A_1^{\times}$ then $a \in K^2$ follows. If $a \notin A_1^{\times}$, we may assume $a \notin A_1$. There are $A_2, \ldots, A_n \in \mathcal{V}$, such that $a \in A_1 \cdot \ldots \cdot A_n =: \hat{A}$ holds. $\hat{A}$ is a non-dyadic, 2 henselian valuation ring $\neq$ F. Because of $a \in \hat{A} \setminus A_1$, we obtain $a \in \hat{A}^{\times} \subset K^2$.

THEOREM 5. (L. Bröcker, [13 ; (3.5)]) <u>Let K be an intermediate field of $\Omega|k$, which is hereditarily-pythagorean relative to Ω. Then the residue field of the Ω-henselian valuation ring of K admits at the most two orders.</u>

<u>Proof</u>. Let A be the Ω-henselian ring of K, $\tilde{A}$ its extension to Ω. As already seen (lemma 6), $\bar{A}$ is h.p. relative to the 2-closed Galois extension $\bar{\tilde{A}}/\bar{A}$. From chapt. II, lemma 1, one concludes that the $\bar{\tilde{A}}$-henselian valuation ring of $\bar{A}$ is trivial. From the outset, we may therefore assume, that K has a trivial Ω-henselian valuation ring. Denote by Z a

2-Sylow-field of $\Omega|K$. Thus, Z is strictly-pythagorean. By chapt.I, lemma 14, A_{Z^2} is the Ω-henselian valuation ring ($\Omega = Z_2$) of Z. Its residue field carries at the most 2 orders (chapt. I., theorem 27). Let $\tilde{A}$ be the extension of A_{Z^2} to Z(i), and set $\mathfrak{I} = \{\sigma\tilde{A} \mid \sigma \in G(Z(i)|K)\}$. $Z(i)|K$ is a Galois extension as can be derived from lemma 1. Denote by $\hat{A}$ the valuation ring of Z(i), which is generated by the rings of $\mathfrak{I}$. Then $\hat{A} \cap K$ is a Z(i)-henselian valuation ring. But, furthermore, $\hat{A}$, being an overring of $\tilde{A}$, is Ω-henselian. Putting both statements together, we see that $\hat{A} \cap K$ is even Ω-henselian. By assumption on K, we must have $\hat{A} \cap K = K$ implying $\hat{A} = Z(i)$. If $\# \mathfrak{I} = 1$, then $\tilde{A} = Z(i)$ follows. In this case we get $A_{Z^2} = Z$, and Z has at the most 2 orders. Since every order of K is extendable to the odd extension $Z|K$, K itself has at the most 2 orders. If $\# \mathfrak{I} \geq 2$, then Z(i) is 2-closed by lemma 7. Thus, Z is euclidean, and we see that K has only one order.

In view of lemma 6, this theorem states that the valuation theory renders the reduction possible onto the class of h.p. fields with at the most 2 orders. Such fields can be constructed as follows. Assume that a 2-closed extension $\Omega|k$ is given. Let R_1, R_2 be two real Ω-closures of k. Then the field $K := R_1 \cap R_2$ is h.p. relative to Ω, since $G(\Omega|K(i))$ is a procyclic group. Because of $[K^\times:K^{\times 2}] \leq 4$, K carries at the most 2 orders. So far, it is unknown whether, conversely, every h.p. field having at most two orders is the intersection of two real Ω-closures.

In general, the intersection of more than two real Ω-closures is no longer h.p. relative to Ω. If, for instance, k is not pythagorean, then the relative pythagorean closure $(\Omega|k)^*$ is not even strictly-pythagorean, as will be proved in chapt. IV, §1.

In the case $k = \mathbb{Q}$, we have the following result.

THEOREM 6. <u>Assume $k = \mathbb{Q}$ and $\Omega = k_2$, or $\Omega = M$, or $\Omega = \bar{k}$. Then every intermediate field, which is hereditarily-pythagorean relative to Ω, is the intersection of two real Ω-closures.</u>

<u>Proof</u>. Let K be h.p. relative to Ω. Since K admits archimedean orders only, and K^2 is a fan, K is seen to have at the most two orders by [11] or [; Satz 21] . In the case $\Omega = k_2$, the results of §6 now yield that $G(\Omega|K(i))$ is cyclic. In order to show that $G(M|K(i))$ is cyclic, we make use of a theorem of Iwasawa [36 ;Theorem 6], which states that $G(M|\mathbb{Q}^{ab})$ is free-solvable ($\mathbb{Q}^{ab}$ denotes the maximal abelian of $\mathbb{Q}$). Because of $K = (M|K^*)$, K(i) contains all roots of unity by chap. II, theorem 5. Thus $K(i) \supset \mathbb{Q}^{ab}$, since the latter extension is generated by the roots of

unity due to the classical result of Kronecker-Weber. Hence, $G(M|K(i))$ is a subgroup of a free-solvable profinite group. Being abelian, $G(M|K(i))$ has to be cyclic. The remaining group $G(\tilde{\mathbb{Q}}|K(i))$ is cyclic due to a theorem of Geyer [27;2.3], in which all abelian subgroups of $G(\tilde{\mathbb{Q}}|\mathbb{Q})$ are proved to be cyclic. In all the three cases, $G(\Omega|K)$ is generated by two involutions, which implies the assertion.

It is a well-known fact that a relatively algebraically closed subfield of a real-closed field is real-closed again. Accordingly, the following result holds.

LEMMA 8. Let K be an absolutely hereditarily-pythagorean field, and assume that k is algebraically closed in K. Then k is itself an absolutely hereditarily-pythagorean field.

Proof. By the Galois theory, $G(\bar{k}|k(i))$ is a subgroup of $G(\bar{K}|K(i))$, thus abelian.

The lemmas 6 and 8 yield the construction of many examples of absolutely h.p. fields. One starts off with an h.p. field K which is real-closed, or is the intersection of two real closures of some field. Secondly, one takes the generalized power-series fields $K((\Gamma))$ - see chapt. I, §4, for example $K = \mathbb{R}((X_1))\ldots((X_n)) \simeq \mathbb{R}(\mathbb{Z}\times\ldots\times\mathbb{Z})$.

Finally, one considers relatively algebraically closed subfields. Due to theorem 5, one may regard the fields obtained in this manner as prototypes of absolutely hereditarily-pythagorean fields.

§3 Extension of maximal subgroups

As before, we assume $\Omega | k$ to be a 2-closed Galois extension. Let us recall some concepts and facts of the first chapter. By definition, subgroups of level n are those subgroups V of K , such that $-1 \notin V$, $K^{\times 2^n} \subset V$ holds. The maximal subgroups of level n are characterized by the properties: $-1 \notin U$, $K^{\times}/U$ cyclic of order 2^m where $m \leq n$. In this case, U is called of exact level m. Every subgroup of the level n is the intersection of the maximal subgroups of the level n in which it is contained.

Let K be h.p. relative to Ω and $F|K$ a field-extension (in Ω, tacitly assumed). If U and $\tilde{U}$ are maximal subgroups of a higher level of K and F resepectively, then $\tilde{U}$ is called an extension of U, if $\tilde{U} \cap K = U$ holds. Because of the embedding $K^{\times}/U \to F^{\times}/\tilde{U}$, the exact level of $\tilde{U}$ is greater than or equal to the exact level of U. If F is not real, then F contains K(i) and is therefore a Galois extension of K. This statement can easily be deduced from the structure of $G(\Omega|K)$, see lemma 2. It is well known that a non-real Galois extension M of a real field N is a quadratic extension of a real intermediate field. Hence, in the present case, $F = F_o(i)$ for some real field F_o. By chapt. II, theorem 8, all roots of unity of order a 2-power are contained in F. Thus, there are no subgroups of a higher level in F. Maximal subgroups are extendable to real extensions of K in Ω only.

For the following basic lemma we need only assume K to be a strictly-pythagorean field. Note that every maximal subgroup U of a level n, and every element $a \in K^{\times}$ satisfy the following alternative: $a^{2^{n-1}} \in U$ or $a^{2^{n-1}} \in -U$.

LEMMA 9. Let $L = K(\sqrt{a})$ be a real quadratic extension of the strictly-pythagorean field K, let U be a maximal subgroup of K of the exact level n. Then the following holds:

i) If $a^{2^{n-1}} \in U$, then U has precisely two extensions to L, and these extensions are also of the exact level n. Furthermore, there exists $\gamma \in K$, such that $\gamma^2 a \in U$ holds, and the extensions are given by:

$$U_1 = \langle\gamma\sqrt{a}\rangle U L^{\times 2^n}, \quad U_2 = \langle-\gamma\sqrt{a}\rangle U L^{\times 2^n}.$$

ii) If $a^{2^{n-1}} \in -U$, then U has a unique extension, namely $\mathfrak{U} = UL^{\times 2^{n+1}}$, and this one has the exact level n+1.

<u>Proof</u>. In the proof of theorem 2, it has been shown that $L^{\times} = \langle\sqrt{a}\rangle K^{\times}L^{\times 2}$. This implies (*) $L^{\times 2^{t-1}} = \langle a^{2^{t-2}}\rangle K^{\times 2^{t-1}}L^{\times 2^{t}}$ for $t \geq 2$. Suppose $\mho$ is an extension U with $[L^{\times}:U] = 2^{t}$. Obviously $t \geq n$. Assume $t \geq n+2$, then from (*) we derive the contradiction $L^{\times 2^{t-1}} \subset UL^{\times 2^{t}} \subset \mho$. Choose a generator ωU, $\omega \in K^{\times}$, for $K^{\times}/U$. i) The coset aU has not the maximal order in $K^{\times}/U$. Thus, $a = (\omega^{2})^{r}u$ for some $u \in U$. Because of $L = K(\sqrt{a\omega^{-2r}})$, we may assume $a \in U$. We have $-1 \notin UL^{\times 2^{n}}$, since, if otherwise, we would obtain $-1 \in U(K^{\times 2^{n}} \cup a^{2^{n-1}}K^{\times 2^{n}}) = U$. Therefore U admits extensions $\mho$, having the exact level n. Since $a = (\sqrt{a})^{2} \in U$ holds, we see $\sqrt{a} \in \mho$ or $-\sqrt{a} \in \mho$ for $\mho|U$. Assume $\sqrt{a} \in \mho$. We have $\mho \supset \langle\sqrt{a}\rangle UL^{\times 2^{n}}$. From $L^{\times} = \langle\sqrt{a}\rangle K^{\times}L^{\times 2} = \langle\sqrt{a}\rangle K^{\times}L^{\times 2^{n}}$ we derive $[L^{\times}:\langle\sqrt{a}\rangle UL^{\times 2^{n}}] | 2^{n}$. Thus, we obtain $\mho = \langle\sqrt{a}\rangle UL^{\times 2^{n}}$. Hence, U has precisely two extensions to subgroups of a level n. Taking into account the fact $L^{\times 2^{n}} \subset UL^{\times 2^{n+1}}$, we see that U is not extendable to a maximal subgroup of the exact level n+1. ii) Since $-a^{2^{n-1}} \in U$, we obtain $L^{\times} = \langle\sqrt{a}\rangle UL^{\times 2^{n+1}}$. Because of $-1 \notin UL^{\times 2^{n+1}}$, U has an extension to a maximal subgroup $\mho$ of the level n+1. The level of $\mho$ cannot be n as $(\sqrt{a})^{2^{n}} \notin U$ holds. Obviously $\mho \supset UL^{\times 2^{n+1}}$. Computing the

index, we get $\mathfrak{U} = UL^{\times 2^{n+1}}$.

Before we turn to the next theorem, we want to premise some general remarks on extensions of a h.p. field K in Ω.

1) Let $F|K$ be a real finite extension, say $[F:K] = 2^t \cdot u$, u odd. Choose an involution $\sigma \in G(\Omega|F)$. Denoting the Galois group $G(F(i)|K(i))$ by V, the Galois group $G(F(i)|K)$ has the following structure: $G(F(i)|K) = \langle\sigma\rangle \cdot V$, where $\sigma v \sigma = v^{-1}$ for $v \in V$ holds. This follows easily from the known structure of $G(\Omega|K)$. Set V_o for the odd part of V in the primary decomposition of V. Then the fixed field F_o of $\langle\sigma\rangle \cdot V_o$ is contained in F and of degree 2^t.

2) Assume, in addition to 1), that $F|K$ is a Galois extension. Then $\langle\sigma\rangle$ has to be a normal subgroup of $G(F(i)|K)$. This implies $V^2 = 1$ in virtue of $\sigma v \sigma = v^{-1}$ for $v \in V$. Hence, $G(F|K)$ is abelian of exponent 2.

3) Now start off from any odd extension $F|F_o$, both fields being strictly-pythagorean. One derives, from the corollary of lemma 4, that the embedding $F_o^\times \to F^\times$ yields an isomorphism $F_o^\times / F_o^{\times 2} \xrightarrow{\sim} F^\times / F^{\times 2}$. Consequently, we get isomorphisms $F_o^\times / F_o^{\times 2^n} \xrightarrow{\sim} F^\times / F^{\times 2^n}$ for every $n \in \mathbb{N}$.

THEOREM 7. Let K be hereditarily-pythagorean relative to Ω, and $F|K$ a real extension in Ω of degree $[F:K] = 2^t \cdot u$, u odd. Then the following statements hold:

i) Every maximal subgroup of a higher level of K is extendable to F. Thereby, the exact level increases by t at the most.

ii) The number of extensions is at the most 2^t.

iii) If $F|K$ is a Galois extension (then necessarily $[F:K] = 2^t$), then a maximal subgroup has either no extension or precisely 2^t faithful extensions. In the latter case, the extensions are conjugate under the Galois group.

Proof. i), ii). Let F_o be the above-mentioned intermediate field of degree 2^t. Since $F_o(i)|K$ is a Galois 2-extension, F_o can be reached from K after some succesive quadratic extensions. Therefore, lemma 9 applies, and we obtain the statements i), ii) for the extension $F_o|K$. As remarked above, there is an isomorphism $F_o^\times/F_o^{\times 2^n} \xrightarrow{\sim} F^\times/F^{\times 2^n}$ for $n \in \mathbb{N}$. Hence, all maximal subgroups of F_o are extendable to F in a unique way, and the exact level remains unchanged. iii) Let $\tilde{U}$ be a faithful extension of U. Given $\sigma \in G(F|K)$, the set $\sigma\tilde{U}$ is obviously a faithful extension of U again. Assume $\sigma\tilde{U} = \tilde{U}$, $\sigma \neq \mathrm{id}$. Since $G(F|K)$ is abelian of exponent 2, the fixed field F_1 of σ satisfies $F = F_1(\sqrt{a})$

for some $a \in F$. On F_1, we have $\tilde{U} \cap F_1 = \sigma\tilde{U} \cap F_1$. Hence, $\tilde{U}$ and $\sigma\tilde{U}$ are both faithful extensions of $U \cap F_1$. However, lemma 9 then yields $\tilde{U} \neq \sigma\tilde{U}$.

This last result shows that the totality of maximal subgroups of a higher level obeys an extension theory over h.p. base fields, as it is known for extendable orders. However, on the one hand, one gains extensions without restriction, but, on the other hand, the exact level and the "arithmetical" character of the maximal subgroups are not preserved under extension. For example, given an order P, the maximal subgroup $P^{\times}$ is always extendable, but the extending subgroup is not necessarily the multiplicative group of an order. This fact was one of the reasons to introduce and to investigate orderings of a higher level. In the case of hereditarily-∞-pythagorean fields, which are to be studied in the next section, the extensions do not leave the scope of orderings.

§4. Hereditarily-∞-pythagorean fields

A real field K, for which $K^{2^n} + K^{2^n} = K^{2^n}$ holds, has been called n-pythagorean, chapt. I, §5. If all real extensions of K in Ω are n-pythagorean, then K is called <u>hereditarily-n-pythagorean</u> relative to Ω. Analogically, one should understand the terms *hereditarily-∞-pythagorean*, *hereditarily-strictly-n-pythagorean*, *hereditarily-strictly-∞-pythagorean*.

From § 5 of chapter I one obtains the result that every henselian field with hereditarily-strictly-∞-pythagorean residue field is itself of this type. In particular, $\mathbb{R}((X_1))\dots((X_n))$ or the real closures of orderings of a higher type prove to be hereditarily-strictly-∞-pythagorean relative to their algebraic closure.

We continue to assume that $\Omega|k$ is a 2-closed Galois extension. From theorem 2 in §1, we know that h.p. fields are even hereditarily-strictly-pythagorean fields. In this connection we can even prove

THEOREM 8. *Given a real intermediate field K of $\Omega|k$ the following statements are equivalent:*

i) *K is hereditarily-pythagorean relative to Ω,*

ii) *K is hereditarily-strictly-pythagorean relative to Ω,*

iii) *$Q_1(L)$ is a fan for every real extension of K in Ω.*

Proof. It remains to prove iii) ⇒ i). We shall show in chapt. IV, §1, theorem that the pythagorean closure of a non-pythagorean field is not even strictly-pythagorean. Thus, every real extension of K in Ω has to be pythagorean

It has been noted at the end of chapt. I, §5, that a 2-pythagorean number-field is even euclidean. Let k be a real number-field, E_1 and E_2 two different euclidean closures of k. Then the field $E := E_1 \cap E_2$ is no longer euclidean because of [6 ;Satz 3]. E must carry two orders P_1, P_2. Denote by R_i a real closure of P_i, i = 1,2, and set $K := R_1 \cap R_2$. K has precisely two orders, namely $R_1^2 \cap K$, $R_2^2 \cap K$. It is true that K is h.p., but not hereditarily-2-pythagorean according to the foregoing remark. However, the following is valid.

THEOREM 9. For an intermediate field K of $\Omega|k$ the following statements are equivalent:

i) K is hereditarily-n-pythagorean relative to Ω for some $n > 2$,

ii) K is hereditarily-∞-pythagorean relative to Ω,

iii) K is hereditarily-strictly-∞-pythagorean relative to Ω,

iv) K is hereditarily-pythagorean in Ω and the residue field of its Ω-henselian valuation ring has a unique order.

Proof. iii) ⇒ ii) ⇒ i) Obvious. i) ⇒ iv) Since lemma 6 holds in accordance for the characterization of hereditarily-n-pythagorean fields, we may assume, as in the proof of theorem 5, that K has a trivial Ω-henselian valuation ring. Let Z be a 2-Sylowfield of $\Omega|K$. Z is strictly-pythagorean and 2-pythagorean. If $A_{Z^2} = Z$, then Z is euclidean (chapt. I, theorem 27, coroll. 2). If, on the other hand, $A_{Z^2} \neq Z$ holds, then the same statements on Z follow from the proof of theorem 5. Since $Z|K$ is an odd extension, K is euclidean, too. iv) $\Rightarrow$ iii) The residue field has to be euclidean. By lemma 5, it is even hereditarily-euclidean, in particular hereditarily-strictly-∞-pythagorean. Now the corollary of chapt. I, lemma 14, yields the conclusion.

In the case of 2-extension we have the analogue of theorem 2.

THEOREM 10. <u>A real field is hereditarily-∞-pythagorean relative to its maximal 2-extension iff it is strictly-∞-pythagorean.</u>

<u>Proof</u>. Let K be strictly-∞-pythagorean. By chapt. I, theorem 27, corollary 2, K admits a 2-henselian valuation with euclidean residue field e. e is also the residue field of all real extensions of K in K_2. Thus, these extensions are again strictly-∞-pythagorean. The remaining statement which has not been proved yet, follows from theorem 8.

A simple extension theory exists for orderings of higher level of hereditarily-∞-pythagorean fields. Thereby, it is essential, not only to consider faithful extensions. In such fields, the sets $U \cup \{0\}$ are orderings of higher level, where U is any maximal subgroup of higher level. This follows from the fact that they are even strictly-∞-pythagorean. In §3 we have proved an extension theorem for maximal subgroups. Using this theorem we obtain

THEOREM 11. Let K be hereditarily-∞-pythagorean relative to Ω, and $F|K$ a real extension, contained in Ω, of degree $[F:K] = 2^t \cdot u$, u odd. Then the following holds:

i) Every ordering of higher level is extendable to F. Thereby, the exact level increases by t at the most.

ii) The number of extensions is at the most 2^t.

iii) If $F|K$ is a Galois extension (then necessarily $[F:K] = 2^t$), then an ordering has either none, or precisely 2^t extensions. In the latter case, the extensions are conjugate under the Galois-group.

The statement iii) also results from chapt. I, theorem 22.

The intermediate fields of $\Omega|k$, which are hereditarily-∞-pythagorean relative to Ω, seem to fully replace the real Ω-closures in a certain sense, for they have not only the particular structure of the Galois group (theorem 1), but the isomorphy-problem is solvable for them by structures in the base field k, as will be proved in chapt. IV.

§5. Algebraic extensions

So far, we only needed the assumption that $\Omega|k$ is a 2-closed extension. But in this section we make the stronger hypothesis that $\Omega|k$ is a saturated extension of the real field k, see chapt. II, §2. By assumption, given any $m|[\Omega:K]$, the extension field Ω contains all m-th roots of unity. Indeed, they even lie in the quadratic extension K(i) of every h.p. intermediate field K of $\Omega|k$. This last statement, to be used in the sequel, follows from chapt.II, theorem 8, in view of $K = (\Omega|K)^*$ (theorem 1).

THEOREM 12. Let K be a hereditarily-pythagorean intermediate field of $\Omega|k$. Set $L = K(i)$. Then, given any $n|[\Omega:K]$, the embedding induces an isomorphism $K^\times/(K^{\times n} \cup -K^{\times n}) \xrightarrow{\sim} L^\times/L^{\times n}$.

Proof. We first show: $K^\times \cap L^{\times n} = K^{\times n} \cup -K^{\times n}$. Obviously $K^{\times n} \cup -K^{\times n} \subset L^{\times n}$, since L contains a primitive 2n-th root of unity. Assume $x^n = \alpha$, where $x \in L^\times$, $\alpha \in K^\times$. Then $\alpha^2 = N(x)^n = \beta^{2n}$, $\beta \in K^\times$ holds because of $N(L^\times) = K^{\times 2}$. We see that $\alpha \in K^{\times n} \cup -K^{\times n}$. In order to prove $K^\times L^{\times n} = L^\times$, it is sufficient to prove $K^\times L^{\times p} = L^\times$ for all prime divisors p of n. If $p = 2$, the result follows from the following exact sequence already used in the proof of theorem 2:

$$K^\times/K^{\times 2} \to L^\times/L^{\times 2} \overset{\tilde{N}}{\to} N(L^\times)/K^{\times 2} \to 1,$$

and the fact $N(L^\times) = K^{\times 2}$. Assume now that $p \neq 2$. Take any $a \in L^\times$. Then $N(a) = \alpha^2$, $\alpha \in K^\times$ holds. Thus, we assume $N(a) = 1$. Set $F := L(\sqrt[p]{a})$. We are going to show that $F|K$ is a cyclic extension of degree $2r$ where $r|p$. To this end, consider a monomorphism $\sigma: F \to \bar{K}$, where $\bar{K}$ is the algebraic closure of K, which is non-trivial on L. From $\sigma(a)a = 1$ we derive $\sigma(\sqrt[p]{a}) = \zeta\cdot(\sqrt[p]{a})^{-1}$, where $\zeta^p = 1$. Since $\zeta \in L$, the extension $F|K$ turns out to be a Galois extension. Let τ be a generating automorphism of $F|L$. We have $\tau(\sqrt[p]{a}) = \eta\sqrt[p]{a}$, $\eta^p = 1$. Thus, $\tau\sigma(\sqrt[p]{a}) = \tau(\zeta(\sqrt[p]{a})^{-1}) = \eta^{-1}\zeta(\sqrt[p]{a})^{-1}$, and, on the other hand, $\sigma\tau(\sqrt[p]{a}) = \sigma(\eta\sqrt[p]{a}) = \eta^{-1}\zeta(\sqrt[p]{a})^{-1}$ because of $\sigma(\eta) = \eta^{-1}$ (see chapt. II, proof of theorem 8). Hence, $G(F|K)$ proves to be abelian. Noting that p is odd, we even conclude that $F|K$ is cyclic of degree $2r$, $r|p$. The hypothesis on $\Omega|k$ now yields $F \subset \Omega$. This implies that K admits an odd cyclic extension of degree r in F, hence in Ω. But every odd extension is real, and, if $r > 1$, we get a contradiction to the result proved before theorem 7, that a real Galois extension of K in Ω has exponent 2.

In order to formulate the next statement smoothly we make the following definition: a field-extension $M|N$ is called a <u>radical extension</u>, if every element of M is contained in the composition $M_1 \cdots M_r$ of some pure sub-extension M_i, $i = 1,\ldots,r$, i.e. $M_i = N(\alpha_i)$, where $\alpha_i \in M$, $\alpha_i^{n_i} \in N$ for some $n_i \in \mathbb{N}$. We do not assume that N contains any root of unity.

THEOREM 13. A real intermediate field K of $\Omega|k$ is hereditarily-pythagorean relative to Ω iff every extension of K in Ω is a radical extension.

Proof. First assume that K is h.p. relative to Ω. The proof will be based on theorem 12: given $m|[\Omega:K]$, we have $L^{\times} = K^{\times}L^{\times m}$, where $L = K(i)$. Now take any finite extension $F|K$ in Ω of degree, say, $[F:K] = n$. By the assumption on $\Omega|k$ and the remark at the beginning of this section, $F(i)|L$ is a Kummer extension. Thus, there are $a_1,\ldots,a_r \in L^{\times}$, because of $L^{\times} = K^{\times}L^{\times t}$ even $a_1,\ldots,a_r \in K^{\times}$, such that $F(i) = L(\sqrt[t]{a_1},\ldots,\sqrt[t]{a_r})$, $t = [F(i):L]$, holds. If F is not real, then $2t = n$ and i^n, $(\sqrt[t]{a_j})^n \in K$. Hence, in this case, $F = F(i) = K(\sqrt[n]{a'_1},\ldots,\sqrt[n]{a'_{r+1}})$ follows. If F is real, then $t = n$. Choose an order P of F and a corresponding real Ω-closure R of P. Thus, F = F(i) $\cap$ R. Since suitable roots of unity exist in F(i), we may assume $a_i \in P$. By assumption on $\Omega|k$, we have $\Omega^m = \Omega$ for $m|[\Omega:k]$. This shows $\tilde{P}^m = \tilde{P}$ for the extension $\tilde{P}$ of P to R, taking theorem 12 into account. So, for some choice of the root we obtain $\sqrt[n]{a_i} \in R$ and, finally, $\sqrt[n]{a_j} \in F(i) \cap R = F$. Thus, we have proved $F = K(\sqrt[n]{a_1},\ldots,\sqrt[n]{a_r})$. It remains to show the converse. K is now assumed to be a real intermediate field, having only radical extensions in Ω. Adjoin all roots of unity, which lie in Ω, to K. Denote the resulting field by M. Being an extension of K in Ω, the field M is easily seen to have only radical extensions in Ω, too. Take any $\alpha \in \Omega$, such that $\alpha^n \in M$ for some $n \in \mathbb{N}$. We want to show that $M(\alpha)|M$ is seen to be an abelian extension. Once this has been proved, $\Omega|M$ is seen to be an abelian extension. Choose n minimal, such that $\alpha^n \in M$. From Capelli's theorem on the pure equation we deduce that $\alpha^n \in M^p$ for some prime number $p|n$, or $\alpha^n \in -4M^4$ and $4|n$, if not $[M(\alpha):M] = n$. If $\alpha^n = \beta^p$, $\beta \in M$, $n = mp$, we conclude $(\alpha^m\beta^{-1})^p = 1$, hence $\alpha^m\beta^{-1} \in M$ and $\alpha^m \in M$. If $n = 4m$, we get $[\alpha^{2m}(2i\beta^2)^{-1}]^2 = 1$, hence $\alpha^{2m} \in M$. In either case, we arrive at a contradiction. Now $[M(\alpha):M] = n$ implies that Ω, hence M, contains the n-th roots of unity. Thus $M(\alpha)|M$ is abelian. M itself is an abelian extension of K. Hence, $\Omega|K$ has a meta-abelian Galois group. The theorem 6 of chapt. IV, §1 applies, and yields that K has to be h.p. relative to Ω.

REMARK. The statement that a real field with only radical extensions must be hereditarily-pythagorean is essentially due to F. Halter-Koch. Using his results of [31], he was the first who proved a rather similar statement under some stronger assumptions on the radical extensions.

If $F|K$ is a finite extension in Ω, where K is a h.p. intermediate field of $\Omega|k$, then $F = K(C)$ for some subgroup C of $F^{\times}$ with $K^{\times} \subset C$ and $C^{n} \subset K$. Moreover, the proof of the foregoing theorem has shown that we may choose $n = [F:K]$. In the sequel we shall study this in a more detailed manner assuming only that Ω contains all n-th roots of unity. It is rather surprising that it is possible to establish such relations between the degree $[F:K]$ and the orders of the groups $C/K^{\times}$ and $C^{n}/K^{\times n}$ as they are known from Kummer theory. We shall base the proofs on our previous results. However, it should be mentioned that they can be derived from general theorems concerning the degree of radical extensions [31], [52].

THEOREM 14. <u>Let K be a hereditarily-pythagorean intermediate field of $\Omega|k$. Assume $F|K$ to be a finite extension contained in Ω, such that $F = K(C)$, where C is a subgroup of $F^{\times}$, $C^{n} \subset K$ for some $n \in \mathbb{N}$, such that Ω contains all n-th roots of unity. Set $\hat{C} = \{a \in F^{\times} \mid a^{n} \in K^{\times}\}$, $W_{2n} = \{\zeta \in F^{\times} \mid \zeta^{2n} = 1\}$. Then the following statements</u>

<u>hold:</u>

i) <u>If F is real, then $\hat{C} = C$, $[F:K] = [C^n:K^{\times n}] = [C:K^\times]$,</u>

ii) <u>If F is non-real, then $\hat{C} = CW_{2n}$,</u>
<u>$[F:K] = [\hat{C}^n:K^{\times n}] = [\hat{C}:K^\times]\cdot\frac{2}{n}$.</u>

<u>Proof</u>. By assumption, Ω contains the n-th roots of unity, which lie in fact in $K(i) =: L$ and, hence, in every non-real extension of K in Ω. The extension $F(i)|L$ is a Kummer extension generated by the subgroup C. By the Kummer theory, we first obtain $F \cap CL^\times = \{a \in F \mid a^n \in L^\times\}$. From $C \subset F$ we see $F \cap CL^\times = C(F \cap L^\times)$. Thus, if F is real, then $F \cap CL^\times = C$, otherwise $F \cap CL^\times = CL^\times$. Take any $a \in F$, such that $a^n \in K$. If F is real, we get $a \in C$, i.e. $C = \hat{C}$. If F is non-real, then $a = cy$, where $c \in C$, $y \in L^\times$. Using $C^n \subset K$ we see $y^n \in K \cap L^n$. But $K \cap L^n = K^n \cup -K^n$ by theorem 12. This implies $\hat{C} = CW_{2n}$. The Kummer theory applied to $\hat{C}$, instead of C, further yields the relations $[F(i):L] = [\hat{C}L^\times:L^\times] = [\hat{C}^nL^{\times n}:L^{\times n}]$. We have $[\hat{C}L^\times:L^\times] = [\hat{C}:\hat{C} \cap L^\times]$, $[\hat{C}^nL^{\times n}:L^{\times n}] = [\hat{C}^n:\hat{C}^n \cap L^{\times n}]$. If K is real, then $[F:K] = [F(i):L]$, $\hat{C} = C$, $C \cap L^\times = K^\times$, $C^n \cap L^{\times n} = K^{\times n}$ (note $K \cap L^n = K^n \cup -K^n$). If K is non-real, we see $\hat{C} \cap L = (C \cap L)W_{2n} = K^\times W_{2n}$, $\hat{C}^n \cap L^{\times n} = K^{\times n} \cup -K^{\times n}$. Because of $F = F(i)$, $[F:K] = 2[F:L]$ and $[K^\times W_{2n}:K^\times] = n$ the assertion follows.

§6. The Galois group $G(\Omega|K)$ and invariants

Assume K to be a hereditarily-pythagorean intermediate field of the 2-closed Galois-extension $\Omega|k$. By theorem 1 and lemma 2, the structure of the "absolute" Galois group $G(\Omega|K)$ is completely determined by the Galois group $G(\Omega|K(i))$. By $\mathbb{Z}_p$, we denote the compact, additive group of the p-adic integers.

THEOREM 15. Let $\Omega|k$ be a prime-closed Galois extension, K a hereditarily-pythagorean intermediate field. Then there exists a uniquely determined sequence of cardinal numbers $\{\alpha_p\}$, where p ranges over the set of prime numbers such that

$$G(\Omega|K(i)) \cong \prod_p \mathbb{Z}_p^{\alpha_p}$$

holds. Moreover,

$$G(K_2|K(i)) = \mathbb{Z}_2^{\alpha_2}, \quad G(\Omega|K_2) = \prod_{p\neq 2} \mathbb{Z}_p^{\alpha_p}.$$

Proof. $G(\Omega|K(i))$ is a torsion-free (chapt. II, theorem 3) and abelian pro-finite group (theorem 1). The topological character group $\mathrm{char}(G(\Omega|K(i)))$ is thus a discrete, divisible, abelian torsion-group. The structure of these latter groups are known, e.g. [33;(A.14)]; they are direct sums of the Prüfer-groups $\mathbb{Q}_p/\mathbb{Z}_p$. From the duality-theorem of Pontrjagin, we obtain $G(\Omega|K(i)) = \prod_p \mathbb{Z}_p^{\alpha_p}$. Set

$U := G(\Omega|K(i))$, then $U/U^p \simeq (\mathbb{Z}/p\mathbb{Z})^{\alpha_p}$.
Thus, $\alpha_p = \dim_{\mathbb{F}_p} \mathrm{char}(U/U^p)$. The remaining statements result from the fact that $G(\Omega|K_2)$ has an odd order, which has been proved in §1.

The cardinal numbers α_p are called the <u>invariants</u> of the hereditarily-pythagorean field K. We are going to prove that they can be arbitrarily prescribed.

Given any totally ordered abelian group Γ, the henselian power-series field $k = \mathbb{R}((\Gamma))$ is absolutely h.p. by lemma 6. The field $l := k(i) = \mathbb{C}((\Gamma))$ admits only tamely ramified extensions, and is its own inertia field [26;p.171,table]. Using [26;(20.12)], we obtain $G(\bar{k}|l) \cong \mathrm{char}(\Gamma_d|\Gamma)$, where Γ_d denotes the divisible closure of Γ.
Now assume a sequence of cardinal numbers $\{\alpha_p\}$ is given. Set $\alpha = \sup\{\alpha_p\}$. Choose a set I of cardinality α, and set $\Gamma := \mathbb{Z}^{(I)}$ (direct sum). Γ can have the structure of a totally ordered group given, by first well-ordering I and then imposing the lexicographical order on Γ [49].
We have $\Gamma_d = \mathbb{Q}^{(I)}$, thus

$$\mathrm{char}(\Gamma_d/\Gamma) = \mathrm{char}(\mathbb{Q}/\mathbb{Z})^{(I)} = \hat{\mathbb{Z}}^I = \prod_p \mathbb{Z}_p^I .$$

The set I contains subsets I_p of cardinality α_p. Hence, we may regard $U := \prod_p \mathbb{Z}_p^{\alpha_p}$ as a subgroup of $G(\bar{k}|\ell)$. The fixed field K of $\langle\sigma\rangle\cdot U$, σ an involution, is the required h.p. field, having the invariants α_p.

We are now going to interpret the invariants by terms of the base field K. To this end, we shall make use of theorem 12 in the following way. If $p = 2$, then $P^\times/K^{\times 2} \xrightarrow{\sim} L^\times/L^{\times 2}$; if p is an odd prime number, then $K^\times/K^{\times p} \xrightarrow{\sim} L^\times/L^{\times p}$, where $L = K(i)$ and P is an order of K.

THEOREM 16. Assume $\Omega|k$ is saturated, and K is a hereditarily-pythagorean intermediate field with invariants α_p. Then the following statements hold.

i) If $p \nmid [\Omega:K]$, then $\alpha_p = 0$,

ii) if $p \neq 2$, $p \mid [\Omega:K]$, then $\alpha_p = \dim_{\mathbb{F}_p} K^\times/K^{\times p}$,

iii) $\alpha_2 = \dim_{\mathbb{F}_2} P^\times/K^{\times 2}$, where P is an order of K.

Proof. If $\alpha_p \neq 0$, then obviously $p \mid [\Omega:K]$. The statements ii), iii) result from the relation

$\alpha_p = \dim_{\mathbb{F}_p} \operatorname{char}(U/U^p)$ proved in theorem 15, where $U = G(\Omega|K(i))$. Since K(i) contains the suitable roots of unity, the Kummer theory yields $\operatorname{char}(U/U^p) \simeq L^\times/L^{\times p}$ and finally, in view of the foregoing remark, the desired conclusion.

The theorems 15 and 16 present a remarkable example of how a field determines its absolute Galois group.

From $G(\Omega|K(i)) = \prod_p \mathbb{Z}_p^{\alpha_p}$ one obtains $G(L_p|L) = \mathbb{Z}_p^{\alpha_p}$, where $L = K(i)$. Thus, α_p is the rank of the Galois group of the maximal p-extension L_p of L [50; Chapt. IV, §6]. Compared to it, K is p-closed, for $p \neq 2$. By the invariant α_2, the algebraic theory of quadratic forms over K is determined. Since K is strictly-pythagorean, we obtain an isomorphism $W(K) \simeq \mathbb{Z}[P^\times/K^{\times 2}]$ as already observed. Moreover, there is a homeomorphism $X(K) \simeq \{0,1\}^{\alpha_2}$, for the topological embedding $X(K) \hookrightarrow \mathrm{char}\,(P^\times/K^{\times 2})$, given by $P \mapsto \chi_P$, $(\chi_P(aK^{\times 2}) = \mathrm{sgn}_P(a))$ is a homeomorphism, because of the fact that K^2 is a fan.

THEOREM 17. Suppose $\Omega|k$ is saturated and K is a hereditarily-pythagorean intermediate field of $\Omega|k$. Moreover, assume $[K^\times:K^{\times p}] < \infty$ for the prime divisor $p \mid [\Omega:K]$. Then, for every extension F of K in Ω the following inequality holds:

$$[F^\times:F^{\times p}] \leq [K^\times:K^{\times p}].$$

If $F|K$ is finite, then even $[F^\times:F^{\times p}] = [K^\times:K^{\times p}]$ holds for $p \neq 2$.

Proof. Due to theorem 12, it suffices to investigate the fields K(i) and F(i). In view of the theorems 15 and 16, one has to consider the Galois groups $G(\Omega|K(i)) = \prod_p \mathbb{Z}_p^{\alpha_p}$ and $G(\Omega|F(i)) = \prod_p \mathbb{Z}_p^{\alpha_p}$. The exact sequence of abelian groups

$$1 \to G(\Omega|F(i)) \to G(\Omega|K(i)) \to G(F(i)|K(i)) \to 1$$

induces an exact sequence of the corresponding p-Sylow-groups: $1 \to \mathbb{Z}_p^{\beta_p} \to \mathbb{Z}_p^{\alpha_p} \to G(F(i)|K(i))_p \to 1$. The morphisms occuring herein are continuous. Hence, in virtue of the density of $\mathbb{Z}$ in $\mathbb{Z}_p$, the sequence under consideration is an exact sequence of $\mathbb{Z}_p$-modules. Since $\mathbb{Z}_p$ is a principal ideal domain, we conclude $\beta_p \leq \alpha_p$. If, in addition, $F|K$ is finite, then $G(F(i)|K(i))_p$ is a torsion-module, and the equality $\beta_p = \alpha_p$ results.

The behaviour of the number of square classes under field extensions are even characteristic for h.p. fields. We set $q_F = [F^{\times}:F^{\times 2}]$ for every field F. If F is strictly-pythagorean, then $q_{F(i)} = \frac{1}{2}q_F$ holds, as was proved in theorem 2. Concerning the proof (not the statement) of the next theorem, we may thus restrict ourselves to real extensions, for every non-real extension of a h.p. field is a quadratic extension of a suitable real intermediate field.

THEOREM 18. Let $\Omega|k$ be a real 2-closed Galois extension, and K a real intermediate field with a finite number of square classes. Then the following statements are equivalent:

i) K is hereditarily-pythagorean relative to Ω,

ii) for every finite real extension $F|K$, $F \subset \Omega$, we have $q_F = q_K$,

iii) for every finite extension $F|K$, $F \subset \Omega$, we have $q_F \leq q_K$,

iv) <u>for every extension $F|K$, $F \subset \Omega$, we have</u> $q_F < \infty$.

<u>Proof</u>. i) ⇒ ii) As remarked before theorem 7, and in its proof, there exists an intermediate field F_o of $F|K$, such that $F_o|K$ is an odd extension, and that one arrives at F starting from F_o, after some successive quadratic extensions. Lemma 4, corollary 1 states $F_o^{\times} = K^{\times}F_o^{\times 2}$. Because of $K^{\times} \cap F_o^{\times 2} = K^{\times 2}$, we see $q_{F_o} = q_K$. Analyzing the exact sequence used in the proof of theorem 2, we see that the number of square classes does not change from a strictly-pythagorean field to a real quadratic extension. Thus, altogether, $q_F = q_{F_o} = q_K$. ii) ⇒ iii) Obvious by the foregoing remark. iii) ⇒ iv) We shall even show $q_F \leq q_K$. Suppose, on the contrary, $q_F > q_K$ for some extension F of K in Ω. This implies the existence of elements $a_1,\dots,a_{n+1} \in F^{\times}$, where $q_K = 2^n$ such that they are independent modulo $F^{\times 2}$. However, in the finite subextension $K(a_1,\dots,a_{n+1})$, they have to be quadratically dependent. That is a contradiction. iv) ⇒ i) Let F' be a real extension of K in Ω, and F be the pythagorean closure of F'. F is contained in Ω. Suppose $F' \neq F$ holds. Then $F|F'$ is an infinite Galois extension, and F is seen to carry infinitely many orders, particularly implying $q_F = \infty$.

As a constrast to the last result, we would like to mention the fact proved in [43; p. 219], that the maximal

2-extension of $\mathbb{Q}$ has indeed only one square class, but that every proper finite extension has an infinite number of square classes.

Analogous to theorem 18, hereditarily-pythagorean fields can be characterized among the real intermediate fields having only finitely many orders, see [13; (3.9)]. In the statements of theorem 18, one has only to replace q_F by $\# X(F)$. In order to carry out the proof, one may note $q_F = 2^{2^{\alpha_2+1}}$, $\# X(F) = 2^{2^{\alpha_2}}$

At the end of this section we want to present a result of L. Bröcker with his kind permission. He proved that h.p. fields can be characterized by the Haar-measure of the set of involutions. Consider a real intermediate field K of a 2-closed extension $\Omega|k$. As we know from chapt. III, §4, the orders of K correspond bijectively to the conjugate classes of the involutions in $G(\Omega|K)$. We denote the set of involutions of $G(\Omega|K)$ by $I(K)$. It is easy to see that $I(K)$ is closed in the Krull-topology. Being a compact group, $G(\Omega|K)$ carries a unique Haar-measure μ_K, normalized by $\mu_K(G(\Omega|K)) = 1$. If $F|K$ is a finite real extension contained in Ω, then $\mu_F = \frac{1}{[F:K]} \cdot \mu_K | G(\Omega|F)$ holds.

$I(K)$ is obviously contained in the coset $G(\Omega|K(i))\cdot\sigma$, where σ is any involution. Thus, we obtain $0 \leq \mu_K(I(K)) \leq \frac{1}{2}$. If K is h.p. relative to Ω, then the coset $G(\Omega|K(i))\cdot\sigma$

consists entirely of involutions. Hence, in this case, $\mu_K(I(K)) = \frac{1}{2}$.

THEOREM 19. (L. Bröcker) A real intermediate field K of a 2-closed Galois extension $\Omega|k$ is hereditarily-pythagorean relative to Ω iff $\mu_K(I(K)) > 0$. If K is hereditarily-pythagorean, then $\mu_K(I(K)) = \frac{1}{2}$.

Proof. Assume $\mu_K(I(K)) > 0$. We are first going to show that K has to be pythagorean. The Galois group $G(\Omega|(\Omega|K)^*)$ $=: H$ is generated by the set I(K) of positive measure, hence it has also positive measure as a subgroup of $G(\Omega|K)$. Being the fixed field of H, the field $(\Omega|K)^*$ is a finite extension of K. $(\Omega|K)^*$ is pythagorean, hence K, too, in virtue of [19 ; Korollar 1]. Next assume that a family $\{F_\alpha\}_{\alpha\in S}$ of finite real extensions of K in Ω is given, such that every order of K extends to some of the fields F_α. We want to show that some of these fields have to be pythagorean. Using the generalization of chapt. III, theorem 4, to 2-closed extensions, we obtain that I(K) is covered by the set of all conjugates $\omega G(\Omega|F_\alpha)\omega^{-1}$ where $\alpha \in S$, $\omega \in G(\Omega|K)$. But I(K) is compact, so I(K) can already be covered by a finite number of them. This implies $0 < \mu_K(I(K) \cap \omega G(\Omega|F_\alpha)\omega^{-1}) =$ $= \mu_K(I(K) \cap G(\Omega|F_\alpha))$, since $\omega I \omega^{-1} = I$ and μ_K is an invariant measure. We get $\mu_{F_\alpha}(I(F_\alpha)) > 0$ and, finally, that F_α is pythagorean. For a first application, we choose an odd finite extension $F|K$, $F \subset \Omega$. We obtain that F has to be pythagorean. For a further application we need the following general result.

LEMMA 10. Let T be a preordering of level 1 of a real field M, and P any order, such that $T \subset P$. If $T+aT = T \cup aT$ holds for every $a \in P$, then T is a fan.

Proof. Consider a maximal subgroup U, such that $U \supset T^{\times}$ holds. We have to show that U is the multiplicative group of an order. Since $T+aT = T \cup aT$ for $a \in P$, we see that $P \cap U =: U_o$ is additively closed. Therefore U_o is the intersection of the multiplicative groups of some orders. If $[K^{\times}:U_o] = 2$, then $U = P^{\times}$. If otherwise, then $[K :U_o] = 4$ must hold. Over U_o there are only 3 subgroups of $K^{\times}$ of index 2 relative to $K^{\times}$. These are $P^{\times}$, U and a certain group V, which has to contain -1. Hence, U is seen to be the multiplicative group of an order.

We shall make use of lemma 10 to prove that K is strictly-pythagorean. Suppose K^2 is not a fan. Then we can choose an element $a(P)$ for every order P, such that $K^2 + a(P)K^2 \neq K^2 \cup a(P)K^2$. The real quadratic extension $F_P := K(\sqrt{a(P)})$ is therefore not pythagorean by [19; Satz 2]. But, applying our previous result to the family $\{F_P\}$, P ranging over all orders of K, we see (on the contrary) that some F_P has to be pythagorean.

So far, we have proved that every finite odd extension of K in Ω is strictly-pythagorean. Now take any real finite extension $F|K$, $F \subset \Omega$. Choose a Galois extension $\hat{F}|K$ such that $F \subset \hat{F} \subset \Omega$. $\hat{F}$ itself is real, or a quadratic extension of a real intermediate field of $\hat{F}|F$. By the Galois theory, F is in either case contained in a real finite extension F_o, which can be attained after an odd extension, followed, if necessary, by successive quadratic extensions. F_o must be pythagorean as strictly-pythagorean fields are h.p. relative to their maximal 2-extension. Since $F_o|F$ is finite, F has to be pythagorean, too.

§7 The Brauer group $Br(\Omega|K)$

Let $F|K$ be any field extension. We denote the group of all classes of central simple algebras over K, which split over F, by $Br(F|K)$. Moreover, $Br(F|K)_q$ denotes the subgroup of the elements of exponent q. Our knowledge on the "absolute" Galois group $G(\Omega|K)$ makes it possible to compute the Brauer group $Br(\Omega|K)$. One has only to exploit the relation $Br(\Omega|K) \simeq H^2(G(\Omega|K),\Omega^{\times})$.

THEOREM 20. Let $\Omega|k$ be a saturated Galois extension, and K a hereditarily-pythagorean intermediate field. Set $L = K(i)$, $G(\Omega|L) = \prod_p \mathbb{Z}_p^{\alpha_p}$. Then the following statements hold:

i) The scalar extension $Br(\Omega|K) \to Br(\Omega|L)$ induces a split-exact sequence

$$0 \to Br(L|K) \to Br(\Omega|K) \to Br(\Omega|L)_2 \to 0.$$

ii) $Br(\Omega|K) = Br(\Omega|K)_2$, $\dim_{\mathbb{F}_2} Br(\Omega|K) = \alpha_2 + \binom{\alpha_2}{2} + 1$.

iii) $Br(\Omega|K)$ and $Br(\Omega|L)_2$ are generated by the classes of quaternion algebras.

Proof. i) From the group extension $1 \to G(\Omega|L) \to G(\Omega|K) \to G(L|K) \to 1$, one obtains the Hochschil-Serre-sequence [35;Chapt.III,5.]:

$$0 \to Br(L|K) \to Br(\Omega|K) \to Br(\Omega|L)^{G(L|K)} \to H^3(G(L|K),L^\times).$$

$G(L|K)$ is cyclic, hence $H^3(\quad) = H^1(\quad) = 1$ by Hilbert 90. Thus, we have an exact sequence

$0 \to Br(\Omega|K) \to Br(\Omega|L)^{G(L|K)} \to 0$. Let A be a central-simple algebra over L which is split by Ω. Then A is similar to a crossed product $[F,G(F|L),f_{\sigma,\tau}]$, where $F|L$ is a finite Galois extension, and $F \subset \Omega$ holds. The order of A in the Brauer group is a divisor of $[F:K]$ by [48;V,§3]. Thus, the class of A belongs to a subgroup $Br(\Omega|L)_n$, where $n|[\Omega:K]$. For such n we shall show that

$Br(\Omega|L)_n \simeq H^2(G,W(n))$, where $G = G(\Omega|L)$, and $W(n)$ denotes the group of the n-th roots of unity. Due to our assumption on $\Omega|k$, we know $W(n) \subset \Omega$ and, by chapt. III, theorem 8, even that $W(n) \subset L$ holds. Because of $\Omega^n = \Omega$ we get an exact sequence $1 \to W(n) \to \Omega \overset{n}{\to} \Omega \to 1$ of G-modules. The corresponding cohomology-sequence yields $Br(\Omega|L)_n \to H^2(G,W(n))$. Being a torsion-group, $Br(\Omega|L)$ is the sum of the subgroups $Br(\Omega|L)_q$, where q is any prime-power. So far, we have shown: if $Br(\Omega|L)_q \neq 0$, then $q|[\Omega:K]$ and $Br(\Omega|L)_q \simeq H^2(G,W(q))$. Note that $G = \prod_p \mathbb{Z}_p^{\alpha_p}$ holds, and that G operates trivially on $W(q) \subset L$. Hence, Scharlau's considerations in [51;section 3] apply. Thus, observing $H^1(G,W(q)) \simeq L^\times/L^{\times q}$, we obtain the result that $Br(\Omega|L)$ is generated by the classes of algebras which have a cyclic splitting field. Let σ be an involution in $G(\Omega|K)$. Then $\langle\sigma_{|L}\rangle = G(L|K)$ holds. We shall show that σ operates on $Br(\Omega|L)$ by taking the inverse. To prove this, it is sufficient to consider cyclic algebras only. Suppose the cyclic algebra $(b,F|L,\omega)$ is given, where $L \subset F \subset \Omega$, $b \in L$, ω generator of $G(F|L)$. Because of $L = KL^n$ for every $n|[\Omega:K]$ (theorem 12), we may assume $b \in K$. Thus, computing in $Br(L)$, we obtain:

$\sigma(b,F|L,\omega) = (b,F|L,\sigma\omega\sigma) = (b,F|L,\omega^{-1}) = (b^{-1},F|L,\omega) =$
$= -(b,F|L,\omega)$, [18;V,§5]. Hence we have proved

$Br(\Omega|L)^{G(L|K)} = Br(\Omega|L)_2$. By [51;lemma 3.3], $Br(L)_2$ is generated by quaternion algebras. To be more precise: given any totally ordered basis $\{\alpha_i L^{\times 2}\}_{i\in I}$ of $L^\times/L^{\times 2}$, then $\{\alpha_i \cup \alpha_j = (\alpha_i,\alpha_j)\}_{i<j}$ is a basis of $Br(L)_2 = H^2(G,\mathbb{Z}/2\mathbb{Z})$. Let P be an order of K. By theorem 12, each $\alpha_i L^{\ 2}$ corresponds uniquely to a class $\beta_i K^{\times^2}$, $\beta_i \in P^\times$, such that $\alpha_i L^{\times^2} = \beta_i L^{\times^2}$ holds. Therefore, we can define a section $Br(\Omega|L)_2 \to Br(\Omega|K)$ by $(\alpha_i,\alpha_j) \mapsto (\beta_i,\beta_j)$. This proves i). Because of $[L:K] = 2$, $Br(L|K)$ consists only of quaternion algebras. Moreover, we have $Br(L|K) \simeq H^2(G(L|K),L^\times) \simeq H^0(G(L|K),L^\times) \simeq K^\times/K^{\times 2}$, for $N(L^\times) = K^{\times 2}$ holds. Now the whole assertion follows observing $\dim_{\mathbb{F}_2} K^\times/K^{\times^2} = \alpha_2 + 1$ and $\dim_{\mathbb{F}_2} L^\times/L^{\times 2} = \alpha_2$.

REMARK. The proof of the fact $Br(\Omega|L)^{G(L|K)} = Br(\Omega|L)_2$ shows that theorem 4.1 of [51] fails to be true. Take as an example for this an absolutely h.p. field, such that the residue field of its henselian valuation ring is real-closed. In this case, $L = K(i)$ turns out to be the inertia field of K. By theorem 20, only the map $Br(\bar{K}|K) \to Br(\bar{K}|L)_2$ is surjective, but not the map $Br(\bar{K}|K) \to Br(\bar{K}|L)$, since in general $Br(\bar{K}|L) \neq Br(\bar{K}|L)_2$ holds! To make this more evident, take $K = \mathbb{R}((\mathbb{Z}\times\mathbb{Z})) \simeq \mathbb{R}((X))((Y))$. Then a double application of Witt's sequence [51;p.243] yields the result $Br(\bar{K}|K) = (\mathbb{Z}/2\mathbb{Z})^4$. This corresponds to theorem 20, whereas

[51;Satz 4.1] implies for instance the existence of non-trivial elements of odd orders.

As already remarked, the field $K = \mathbb{R}((X_1))\ldots((X_n))$ is absolutely h.p.. We have $q_K = 2^{n+1}$, hence $\alpha_2 = n$ and $Br(\bar{K}|K) \simeq (\mathbb{Z}/2\mathbb{Z})^{\frac{1}{2}(n^2+n+2)}$

Chapter IV Hereditarily-Pythagorean Extensions of Fields

§1. Hereditarily-pythagorean extensions

We continue to assume that a 2-closed extension $\Omega|k$ is given. Let K be an intermediate field of $\Omega|k$, which is hereditarily-pythagorean relative to Ω. In this chapter, we shall study the extension $K|k$, whereas we have been concerned with the extension $\Omega|K$ in the last chapter. By chap.III, theorem 1, the field K is the intersection of real Ω-closures. However, given an arbitrary family $\{R_\alpha\}$ of real Ω-closures R_α, its intersection $K := \bigcap_\alpha R_\alpha$ need not be hereditarily-pythagorean relative to Ω. This will be shown, among other results, in this section.

THEOREM 1. i) Let Γ be a family of involutions of $G(\Omega|k)$. Set $K := \bigcap_{\sigma \in \Gamma} \Omega^\sigma$. Then K is hereditarily-pythagorean relative to Ω iff the product $\sigma\tau\omega$ is again an involution for any three involutions $\sigma, \tau, \omega \in \Gamma$.

ii) The intersection of a family of real Ω-closures is hereditarily-pythagorean relative to Ω iff this holds for the intersection of any three of them.

Proof. It is sufficient to prove i). If K is h.p., then the involutions $\sigma \in \Gamma$ operate on $G(\Omega|K(i))$ by taking the inverse. Hence, $(\sigma\tau\omega)^2 = \sigma\cdot(\tau\omega)\cdot\sigma\cdot\tau\omega = 1$. Conversely, assume that Γ satisfies the quoted condition. $G(\Omega|K(i))$ is generated by the products $\sigma\tau$ where $\sigma,\tau \in \Gamma$ holds. From this, it follows that $\sigma\tau\cdot\sigma'\tau' = (\sigma\tau\sigma')\cdot\tau' = (\sigma'\tau\sigma)\tau' = \sigma'(\tau\sigma\tau') =$ $= \sigma'\tau'\sigma\tau$. But this means that $G(\Omega|K(i))$ is abelian, hence, K is h.p. relative to Ω.

It is interesting to rephrase the last result in terms of <u>generators and relations</u>. An intermediate field K of $\Omega|k$ is h.p. relative to $\Omega|k$ iff $G(\Omega|K)$, as a topological group, is generated by a subset Γ subject to the relations $\sigma^2=1, \sigma\neq 1$, $(\sigma\tau\omega)^2 = 1$ for $\sigma,\tau,\omega \in \Gamma$.

LEMMA 1. <u>Let</u> $\{K_\alpha\}_{\alpha\in I}$ <u>be a family of intermediate fields of $\Omega|k$, each of them hereditarily-n-pythagorean relative to Ω. Assume that there exists, for any two fields</u> K_α, K_β, <u>a field</u> K_γ, <u>such that</u> $K_\alpha \cap K_\beta \supset K_\gamma$. <u>Then the field</u> $K := \bigcap_\alpha K_\alpha$ <u>is again hereditarily-n-pythagorean relative to Ω.</u>

<u>Proof</u>. In view of chapt.III, theorem 8, we only need consider the cases $n = 1$, $n = \infty$. But there is no advantage in doing so, and n may be an arbitrary natural number. Given an element $x \in K$, we find $y_\alpha \in K_\alpha$, such that $1+x^{2^n} = y_\alpha^{2^n}$ for every $\alpha \in I$. Fix $\alpha_o \in I$. For $\alpha \in I$, we find by assumption $\gamma \in I$ with $K_\gamma \subset K_\alpha \cap K_{\alpha_o}$. Hence, the equation

$y_\alpha^{2^n} = y_\gamma^{2^n}$ holds in K_α, and, accordingly, $y_{\alpha_o}^{2^n} = y_\gamma^{2^n}$ in K_{α_o}. Since K_α and K_{α_o} are real, it follows that $y_{\alpha_o} = \pm y_\gamma = \pm y_\alpha$, and, from this, $y_{\alpha_o} \in \bigcap_\alpha K_\alpha = K$. Therefore, K is n-pythagorean. Let L be a real extension of K in Ω. We have to show that L is n-pythagorean. It is sufficient to assume $L|K$ to be finite, say $L = K(a)$. We derive $L = \bigcap_\alpha K_\alpha(a)$, as the degrees of the irreducible polynomials $f_\alpha(X)$ of a over K_α are bounded from above by $[L:K]$. Hence, we find a field K_{α_o} and $m \in \mathbb{N}$, such that $[K_\alpha(a):K] = m$ holds for every field $K_\alpha \subset K_{\alpha_o}$. Considering solely such fields K_α, one easily proves $\bigcap_\alpha K_\alpha(a) = K(a) = L$. Supposing that all the extensions $K_\alpha(a)$ were not real, they would all have to contain the element $\sqrt{-1} \in L$. By the first part of this prof, L is seen to be pythagorean.

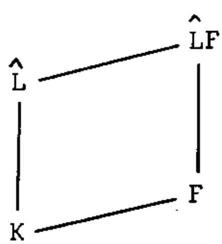
The following result is, using Zorn's lemma, an immediate consequence of lemma 1.

THEOREM 2. <u>Every hereditarily-n-pythagorean ($n=1,\infty$) intermediate field of $\Omega|k$ contains minimal hereditarily-n-pythagorean extensions of k.</u>

If $L|K$ is a finite extension, and L pythagorean, then K is also pythagorean [19; p. 149]. This has already been applied on several occasions. The corresponding statement is valid for h.p. fields, as we shall now prove.

THEOREM 3. <u>Assume that K, L are intermediate fields of $\Omega|k$, and that $L|K$ is a finite extension. If L is hereditarily-n-pythagorean ($n=1,\infty$) relative to Ω, then the same holds for K.</u>

<u>Proof</u>. Denote the Galois closure of $L|K$ by $\hat{L}|K$. First we assume that $\hat{L}$ is real. Being a strictly-pythagorean Galois extension of K, $\hat{L}|K$ has to be a 2-extension, by chapt.III, lemma 4, corollary 2. Consequently, L can be attained from K by successive quadratic extensions. We may assume $L=K(\sqrt{a})$ We have $K(\sqrt{-a}) \subset \Omega$. Since K is pythagorean, $K(\sqrt{-a})$ is real. $K(\sqrt{-a})$ is again h.p. relative to Ω, because $G(\Omega|L(i)) = G(\Omega|K(\sqrt{a},i)) = G(\Omega|K(\sqrt{-a},i))$ is abelian. Now consider a real extension $F|K$, $F \subset \Omega$. If $F(\sqrt{a})$ is real, then $F(\sqrt{a})$, being an extension of L, is pythagorean. Hence, in this case, F must be real too. If $F(\sqrt{a})$ is not real, then $i \in F(\sqrt{a})$ follows, and $a = -b^2$ for some $b \in F$. Hence, $K(\sqrt{-a}) \subset F$, and F is shown to be pythagorean. It remains to study the case of $\hat{L}$ being non-real. Then $L(i) \subset \hat{L}$, and $G(\Omega|\hat{L})$ has to be abelian. Let F be a real extension of K. Consider the diagramm



$\hat{L}F$ is a non-real Galois extension of F. Consequently there is a real intermediate field F' of $\hat{L}F|F$, such that $[\hat{L}F:F']=2$. Because of $i \in \hat{L}$, we get $\hat{L}F = F'(i)$. Being a subgroup of $G(\Omega|\hat{L})$, $G(\Omega|F'(i))$ has to be abelian. Hence, F' and, finally, F is seen to be pythagorean. With this, we have proved that K is h.p. We now attend to the case that L is even hereditarily-∞-pythagorean. Let A be the Ω-henselian valuation ring of L, $\tilde{A}$ **its extension** on L(i). By $\tilde{B}$, we denote that valuation ring of L(i) which is generated by the conjugates $\sigma\tilde{A}$, $\sigma \in G(L(i)|K)$. Then $B := \tilde{B} \cap K$ is the Ω-henselian valuation ring of K. If $\tilde{A} = \sigma\tilde{A}$ holds for all $\sigma \in G(L(i)|K)$, then $B = A \cap K$ follows. In this case, $\bar{A}|\bar{B}$ is a finite extension. $\bar{A}$ is euclidean by chapt.III, theorem 9, hence, $\bar{B}$ is also euclidean. A second application of this theorem shows that K is hereditarily-∞-pythagorean relative to Ω. If $\tilde{A} \neq \sigma\tilde{A}$ holds for some $\sigma \in G(L K(i))$, then $\bar{\bar{B}}$ is 2-closed by chapt.III, lemma 7. Since $\bar{B}|\bar{\bar{B}}$ is finite, $\bar{B}$ must also be euclidean in this case [6; Satz 6]. As before, we see that K is hereditarily-∞-pythagorean.

In the following corollary, we do not assume L to be contained in some 2-closed extension Ω|K.

COROLLARY. Let L|K be a finite field extension. If L is strictly-n-pythagorean (n=1,∞), then the same holds for K.

<u>Proof</u>. Set $F := L \cap K_2$. F is quadratically closed in L. From this, one derives that $F^{2^n} = F \cap L^{2^n}$ is a fan of level n. We may therefore assume that F is contained in $\Omega = K_2$. But now theorem 3 applies.

Statements similar to those of theorem 3 and its corollary have been proved in [13], too.

For further reflexions we require a result on the extensions of fans of the first level. Let T denote a preordering (1. level) of K. Given $a \in T$, we set $L = K(\sqrt{a})$. We denote a faithful extension to L of an order P of K by $\tilde{P}$. Set

$$\tilde{T} := \bigcap_{\substack{\tilde{P}|P \\ P \supset T}} \tilde{P}$$

$\tilde{T}$ is clearly a preordering. We assert

(*) $\tilde{T} = \{x \in L \mid N(x), Tr(x) \in T\}$.

Let $\sigma: L \to L$ be the non-trivial K-automorphism of L. Given an order $\tilde{P}$ of L, then $\sigma(\tilde{P})$ is again an order, lying over $P = \tilde{P} \cap K$. Hence, $\sigma(\tilde{T}) = \tilde{T}$. For $x \in \tilde{T}$, it follows that $x + \sigma(x), x \cdot \sigma(x) \in \tilde{T} \cap K$. We have $\tilde{T} \cap K = T$, as every order over T is extendable to L because of $a \in T$. Conversely, assume $x \in L$ is given, such that $x + \sigma(x), x \cdot \sigma(x) \in T$ holds. Consider an order $\tilde{P}$ over $\tilde{T}$. If $x \notin \tilde{P}$, then $\sigma(x) \notin \tilde{P}$ and, consequently, $x + \sigma(x) \notin \tilde{P}$ which contradicts the assumption $x + \sigma(x) \in T \subset \tilde{P}$.

LEMMA 2. <u>$\tilde{T}$ is a fan iff T is a fan and $N(L) \subset T \cup -T$ holds.</u>

<u>Proof</u>. Assume $\tilde{T}$ to be a fan. Consider $x = \alpha + \beta\sqrt{a} \in L^{\times}$. If $\alpha\beta\sqrt{a} \in -\tilde{T}$, then the contradiction $\alpha^2\beta^2 \in -T$ follows, since $\tilde{T}$ is invariant under $G(L|K)$. Hence, we obtain $\alpha + \beta\sqrt{a} = t\cdot(\alpha\beta\sqrt{a})^{\varepsilon}$, $t \in \tilde{T}$, $\varepsilon = 0,1$, which shows $N(x) \in T \cup -T$. T is a fan because of $T = \tilde{T} \cap K$. Now we prove the converse. From (*) one derives $L^{\times} = \langle\sqrt{a}\rangle K^{\times}\tilde{T}^{\times}$. Let $\tilde{U}$ be a subgroup of L, such that $-1 \notin \tilde{U}$, $[L^{\times}:\tilde{U}] = 2$, $\tilde{U} \supset \tilde{T}^{\times}$ and $\sqrt{a} \in \tilde{U}$ without loss of generality. Set $U = \tilde{U} \cap K$. It follows that $\tilde{U} = \langle\sqrt{a}\rangle U\tilde{T}^{\times}$. Since T is a fan and $T^{\times} \subset U$ holds, there exists an order $P \supset T$, such that $U = P^{\times}$. Let $\tilde{P}$ be the extension of P to L, with $\sqrt{a} \in \tilde{P}$. We have $\tilde{P} \supset \tilde{T}$ and $\tilde{P} = \langle\sqrt{a}\rangle K\tilde{T}$, hence $\tilde{U} = \tilde{P}^{\times}$. Therefore, $\tilde{T}$ is a fan.

THEOREM 4. <u>If $k \neq (\Omega|k)^*$, then $(\Omega|k)^*$ is not strictly-pythagorean.</u>

<u>Proof</u>. We set $k^* = (\Omega|k)^*$ and suppose that k^* is strictly-pythagorean. If $[k^*:k]$ is odd, then every intermediate field is also strictly-pythagorean, and of odd degree over k (compare with the proof of the corollary of theorem 3). But among these intermediate fields there are finite Galois extensions, which, according to chapt.III, lemma 4, corollary 2 have to be of degree 2^t over k. Hence, in the case of $k \neq k^{\times}$, the degree $[k^*:k]$ is even. Let K be a 2-Sylow

field of $k^*|k$. k^* is a proper 2-extension of K, to which every order of K is faithfully extendable. Therefore, k^* equals the pythagorean closure of the non-pythagorean field K relative to K_2 (chapt.II, theorem 6 and §4). Given any intermediate field L of $k^*|K$, the set Q(L) is a fan because of $Q(L) = L \cap (k^*)^2$. We find an element $a \in K^\times$ with $1 + a^2 \notin K^{\times 2}$. By [19], the extension $L = K(\sqrt{1+a^2+\sqrt{1+a^2}})$ is contained in k^*. L is a quadratic extension of $K_1 =$ $= K(\sqrt{1+a^2})$. We have

$$N_{L|K_1}\left(\sqrt{1+a^2} + \sqrt{1+a^2+\sqrt{1+a^2}}\right) = -\sqrt{1+a^2}$$

But neither $-\sqrt{1+a^2}$ nor $\sqrt{1+a^2}$ is a sum of squares in K_1. By lemma 2, Q(L) cannot be a fan: contradiction.

REMARK. Theorem 4 yields a series of examples of fields, which are intersections of real Ω-closures, but are not hereditarily-pythagorean: namely the fields $(\Omega|k)^*$, where k is not strictly-pythagorean.

THEOREM 5. <u>If K is a hereditarily-pythagorean intermediate field of $\Omega|k$, then the group of automorphism $\mathrm{Aut}(K|k)$ is abelian of exponent 2.</u>

<u>Proof</u>. It is sufficient to show that every $\sigma \in \mathrm{Aut}(K|k)$ has the order 2. Let U be the closed subgroup which is generated by σ. Let V be the odd part of U, and K_o the fixed field of V. Since $[K:K_o]$ is odd, K_o is strictly-pythagorean.

But $K|K_o$ is a Galois extension, hence a 2-extension. We get $K = K_o$, and U must be a 2-group. Suppose σ were of infinite order. In this case, $K|K^\sigma$ is a 2-extension with a torsion-free Galois group. We get $K = (K^\sigma)_{pyth} =$ $= ((K^\sigma)_2|K^\sigma)^*$, contradicting theorem 4. Hence, σ is of finite order, and K^σ is h.p. by theorem 3. $K|K^\sigma$ is then a finite Galois extension of h.p. fields. A closer examination of the normal subgroups of $G(\Omega|K^\sigma)$ shows that $G(K|K^\sigma)$ is abelian of exponent 2.

COROLLARY 1. Let K be an intermediate field of $\Omega|k$, which is hereditarily-n-pythagorean $(n=1,\infty)$, and H be a subgroup of $Aut(K|k)$. Then the fixed field K^H is again hereditarily-n-pythagorean.

Proof. H has only elements of order 2. The fixed field of finitely many elements of H has finite index relative to K. Combining theorem 3 and lemma 1, we obtain the desired conclusion.

COROLLARY 2. If K is a minimal hereditarily-n-pythagorean $(n=1,\infty)$ extension of k in Ω, then $Aut(K|k) = 1$.

The following result has already been used in chapter III, §5.

THEOREM 6. A real intermediate field K of $\Omega|k$ is hereditarily-pythagorean relative to Ω iff $G(\Omega|K)$ is meta-abelian.

Proof. It remains to show that K must be h.p., if $G(\Omega|K)$ is meta-abelian. Let $\tilde{F}$ be the maximal abelian extension of K in Ω. By assumption, $G(\Omega|\tilde{F})$ is abelian, moreover $i \in \tilde{F}$. Choose a maximal real intermediate field F of $\tilde{F}|K$. Then $\tilde{F} = F(i)$, $G(\Omega|F(i))$ abelian. This means that F is h.p. relative to Ω. Now the first corollary above says that K is also h.p. relative to Ω, since $F|K$ is a Galois extension.

§2. Applications to stability index and fans

In this section, we shall only consider preorderings of the first level. Let T be such a preordering of the real field k. We denote the reduced Wittring belonging to T by W_T, in the sense of [8], [13;§2]. By the definition of [8], W_T is a subring of $C(X_T,\mathbb{Z})$ where X_T is the topological space of all orders which lie over T. It is known that $C(X_T,\mathbb{Z})/W_T$ is a 2-primary torsion group. If this group has a finite exponent, we set

$$st(T) = \min \{n \mid 2^n C(X_T,\mathbb{Z}) \subset W_T\},$$

otherwise we set $st(T) = \infty$. This number st(T) is called the stability index of T, see [12], [8]. In the case of $T = Q(k)$, we write st(k) instead of st(Q(k)). If T is a fan with a finite index $[K^{\times}:T^{\times}] = 2^n$, then st(T) = n-1 [8 ;Satz 28,Korollar]. L.Bröcker has proved the following result in [13 ;(2.10)].

$$st(k) = \sup\{st(T) \mid T \text{ a fan of } k\}.$$

SAP-fields are characterized by $st(k) \leq 1$ [24], [12], [8]. In [47 ;p.151], Prestel has raised the following problem. Let $F_1|F$ be a finite extension, and assume that F_1 is a SAP-field. Is it true that F must be a SAP-field too? We would like to supply the negative answer. For this purpose, we shall first study the precise relation between fans and strictly-pythagorean fields, because, if K is a strictly-pythagorean extension of k, then the set $T := Q(K) \cap k$ is easily seen to be a fan. We shall prove that every fan arises in this way.

Let $K|k$ be a real extension, T be a fan of k. T is called <u>extendable</u> to K, if there is a fan $\tilde{T}$ of K, such that $\tilde{T} \cap k = T$.

LEMMA 3. <u>If $\tilde{T}$ is an extension of T, then the restriction map</u> Res: $X_{\tilde{T}}(K) \to X_T(K)$, $\tilde{P} \mapsto \tilde{P} \cap k$ <u>is surjective. Moreover, we have</u> $PT = \bigcap_{\substack{\tilde{P}|P \\ \tilde{P}\in X_{\tilde{T}}(K)}} \tilde{P}$ <u>for every $P \in X_T(K)$.</u>

Proof. Given $P \in X_T$ we see $-1 \notin P\tilde{T}$. Hence, $P\tilde{T}$ is a preordering. From chapt. I, theorem 1 $P\tilde{T} = \bigcap_{\tilde{P}|P, \tilde{P} \supset \tilde{T}} \tilde{P}$ follows.

A fan $\tilde{T}$ is called a faithful extension of T, if $\tilde{T} \cap K = T$ holds and the map Res: $X_{\tilde{T}}(K) \to X_T(k)$ is bijective. In the case of a faithful extension, $P\tilde{T}$ is the unique extension of $P \in X_T$ which lies over $\tilde{T}$. Moreover, the restriction map Res: $X_{\tilde{T}} \to X_T$ is a homeomorphism between the topological spaces $X_{\tilde{T}}$ and X_T.

THEOREM 7. Let $\Omega|k$ be a 2-closed Galois extension of the real field k, and T be a fan of k. Then there exists a hereditarily-pythagorean intermediate field K (relative to Ω) satisfying $\Omega = K_{\underline{2}}$, $K = kK^2$, such that the fan K^2 is a faithful extension of T.

COROLLARY. $st(k) = \sup\{st(K)\}$ where K ranges over all hereditarily-pythagorean intermediate field K which satisfy $K = kK^2$.

Proof. From $K = kK^2$ follows $[k^\times : k^\times \cap K^{\times 2}] = [K^\times : K^{\times 2}]$. Using this, the quoted result of L. Bröcker yields $st(k) \geq \sup\{st(K)\}$. But from theorem 7 one derives the inequality $st(k) \leq \sup\{st(K)\}$.

Theorem 8 presents an analogon to a theorem of Th. Graven [17;Corollary 3]. The proof is essentially based on the following extension lemma. Let T be a fan and A a valuation ring, which is compatible with T, see chapt. I, §2. The induced preordering $\bar{T} := \overline{A \cap T}$ is again a fan of $\bar{A}$.

LEMMA 4. <u>Assume that T is a fan of k, and that A is a valuation ring of k, which is fully compatible with T. Let $(K,\tilde{A})$ be an extension of (k,A). If the ramification index $e(\tilde{A}|A)$ is finite and odd, and if, moreover, the induced fan $\bar{T}$ is faithfully extendable from $\bar{A}$ to $\bar{\tilde{A}}$, then T admits a faithful extension to K, which is fully compatible with $\tilde{A}$.</u>

<u>Proof</u>. Let $\pi_K: \tilde{A} \to \bar{\tilde{A}}$ denote the canonical epimorphism, and $\hat{\bar{T}}$ be a faithful extension of $\bar{T}$ to $\bar{\tilde{A}}$. We set $\tilde{T} := TK^2\pi_K^{-1}(\hat{\bar{T}}^{\times})$. By chapt. I, lemma 9, $\tilde{T}$ is a proper preordering, which is fully compatible with $\tilde{A}$. We have $\bar{\tilde{T}} = \hat{\bar{T}}$, for one concludes $TK^2 \cap \tilde{A}^{\times} = (T \cap A^{\times})\tilde{A}^{\times 2}$, as the ramification index is odd. Being an overpreordering of the fan $K^2\pi_K^{-1}(\hat{\bar{T}}^{\times})$, $\tilde{T}$ is a fan itself. From $\hat{\bar{T}} \cap \bar{A} = \bar{T}$ and the full compatibility of T with A, $\pi_K^{-1}(\hat{\bar{T}}^{\times}) \cap k = T \cap A^{\times}$ follows. Observing that the ramification index is odd, we get $K^2\pi_K^{-1}(\hat{\bar{T}}^{\times}) \cap k = k^2(T \cap A^{\times})$ and, finally, $\tilde{T} \cap k = T$. Given an order $P \supset T$, the set $P\tilde{T}$ is a preordering in any case. We have $\pi_K(P\tilde{T} \cap \tilde{A}) = \bar{P}\bar{\tilde{T}} = \bar{P}\hat{\bar{T}}$. Since $\hat{\bar{T}}$ is a faithful extension

of $\bar{T}$, $\pi_K(\tilde{PT} \cap \tilde{A})$ is the unique extension of $\bar{P}$ to an order over $\hat{\bar{T}}$. $\tilde{PT}$ is also fully compatible with $\tilde{A}$. Hence, the following index-formula is valid:

$$[K^{\times}:(\tilde{PT})^{\times}] = [\bar{\tilde{A}}^{\times}:\overline{(\tilde{PT})^{\times}}][\Gamma_K:v_K((\tilde{PT})^{\times})],$$

where v_K is the valuation belonging to $\tilde{A}$, and Γ_K its value group. For the proof, compare with chapt. I, lemma 4, corollary. As remarked, it holds that $[\bar{\tilde{A}}^{\times}:\overline{(\tilde{PT})^{\times}}] = 2$. We obtain $v_K((\tilde{PT})^{\times}) = v_K(P^{\times})\Gamma_K^2 = \Gamma_k\Gamma_K^2 = \Gamma_K$, since Γ_k has odd index in Γ_K. Hence, $\tilde{PT}$ is an order, and $\tilde{T}$ a faithful extension of T.

COROLLARY. Faithful extensions exist in the following cases:

i) K|k is an odd algebraic extension,

ii) $(K,\tilde{A})$ is the henselian closure of (k,A),

iii) K is the pythagorean closure of k.

Proof. i) It is sufficient to study only finite odd extensions K|k. Because of $[K:k] = \sum_1^g e_i f_i$, there is at least one extension $\tilde{A}$ of A_T, which has odd numbers e, f. Choose such an extension $\tilde{A}$. By chapt. I, theorem 14, $\bar{T}$ is a trivial fan of $\bar{A}_T$. The trivial fan $\bar{T}$ is faithfully extendable to $\bar{\tilde{A}}$, since every order of $\bar{A}_T$ is extendable to an order of the odd extension $\bar{\tilde{A}}$. ii) $(K,\tilde{A})$ is an immediate extension of (k,A). iii) As in the proof of theorem 19, chapt. I, we may confine ourselves to the case of $K = k(\sqrt{1+a^2})$. One sees that A_T is fully decomposed or inert relative to K. In the second case, one further finds that $\bar{\tilde{A}} = \bar{A}_T(\sqrt{1+\bar{\varepsilon}^2})$ for some unit ε, which implies that the trivial fan $\bar{T}$ is faithfully extendable. Now apply lemma 4.

<u>Proof of theorem 8</u>. By Zorn's lemma, we find a maximal faithful extension $(K,\tilde{T})$ of (k,T) in Ω. The corollary of lemma 4 says that $\Omega = K_2$ holds, and that $A_{\tilde{T}}$ is an Ω-henselian valuation ring of K. Suppose there is $\varepsilon \in A_{\tilde{T}}^{\times}$, such that $\bar{\varepsilon} \in \bar{\tilde{T}} \setminus (\bar{A}_{\tilde{T}})^2$. In this case, the trivial fan $\bar{\tilde{T}}$ may be faithfully extended to $\bar{A}_T(\sqrt{\bar{\varepsilon}})$. Consequently, T itself must admit a faithful extension to $K(\sqrt{\varepsilon}) \subset \Omega$. Hence, $\bar{\tilde{T}} = (\bar{A}_{\tilde{T}})^2$. Moreover, the residue field of $A_{\tilde{T}}$ is strictly-pythagorean. Since $A_{\tilde{T}}$ is Ω-henselian, K itself has to be stricIty-pythagorean. Because of $\Omega = K_2$, we see that K is even h.p. relative to Ω. Suppose that $\tilde{T} \neq K^2$, then we find $a \in \tilde{T} \setminus K^2$. Consider the strictly-pythagorean extension $K(\sqrt{a}) \subset \Omega$. It is true that $\tilde{T}$ admits a faithful extension $\tilde{T}'$ to $K(\sqrt{a})$, for example $\tilde{T}' = \bigcap_{\tilde{P} \supset \tilde{T}, \tilde{P} \ni \sqrt{a}} \tilde{P}$. Hence, $\tilde{T} = K^2$.

The result $kK^2 = K$ follows from the fact that, for every $P \in X_T$, the preordering PK^2 is already an order.

For further reflections we need two lemmata.

LEMMA 5. Let T be a preordering of k, and assume that $T[a] = T \cup Ta \neq T$ holds. If $T[a]$ is a fan, the same holds for $T[-a]$.

Proof. Let U be a maximal subgroup, without -1 over $T[-a]$. We shall show $U + U \subset U$. Pick $b \in U$. If $b \in -T[a] = -T \cup -Ta$, then $b \in -Ta$ follows, thus $1 + b \in T[-a]^{\times}$. If $b \notin -T[a]$, then $1 + b \in T[a] \cup T[a]b = T \cup Ta \cup Tb \cup Tab$. $1 + b \in Ta$ cannot hold, as this would imply $b=-(1+t(-a)) \in -T[-a]^{\times} \subset -U$, a contradiction. The same argument applies to the case of $1 + b \in Tab$. Hence, $1 + b \in T^{\times} \cup T^{\times}b \subset U$.

LEMMA 6. Assume that T is a fan and P an archimedean order of k. Set $T_o := T \cap P$, and choose $a \in T \setminus P$. Then the following holds:

$$T = T_o \cup T_o a , \quad P = T_o[-a].$$

Proof. By lemma 5 $T_o[-a]$ is a fan. $T_o[-a]$ must be a trivial one, as there is an archimedean order over it [8 ; Satz 22]. Among the orders over T_o, the orders over $T_o[-a]$ are precisely those, which can be extended to orders of $K := k(\sqrt{-a})$. Because of $N_{K|k}(K) \subset T_o[-a] \cup -T_o[-a]$, we obtain by lemma 2 that $T_o[-a]$ is a fan. The two extensions of P lie over $T_o[-a]$. Since they are archimedean once more, $T_o[-a]$ has to be trivial. But this implies $T_o[-a] = P$.

Now we are able to give some examples for the behaviour of the stability index under algebraic field extensions. Let L be a real algebraic extension of K. By [12; (4.3)], we know that $st(L) \leq st(K) + 1$; using our concepts that can be proved as follows. Let T be a fan of L, A_T the associated valuation ring, and $\bar{T}$ the induced fan of $\bar{A}_T$. Because of the full compatibility, we know that $T_o := L^2\pi_L^{-1}(\bar{T}^\times) \subseteq T$, $\bar{T}_o = \bar{T}$, $A_{T_o} = A_T$. Since $st(T_o) \geq st(T)$ holds, we need only consider fans of the type $T = L^2\pi_L^{-1}(\bar{T}^\times)$. Set $A = A_T \cap K$, $\bar{T}_1 := T \cap \bar{A}$, then $\bar{T}_1$ is a fan, hence $T_1 := K^2\pi_K^{-1}(\bar{T}_1^\times)$ is a fan of K. We have $2^{1+st(T)} = [L^\times:T^\times] = [\Gamma_L:\Gamma^2][\bar{A}_T^\times:\bar{T}^\times]$, $2^{1+st(T_1)} = [\Gamma_K:\Gamma_K^2][\bar{A}^\times:\bar{T}_1^\times]$. Observe that $[\Gamma_L:\Gamma_L^2] = [\Gamma_K:\Gamma_K^2]$, and $[\bar{A}_T^\times:\bar{T}^\times] \leq [\bar{A}^\times:\bar{T}_1^\times]\cdot 2$ holds ($\bar{T}_1$ may be an order). The relation between fans and stability index implies $st(L) \leq$ $\leq st(K) + 1$.

The relation, considering lemma 4, corollary, also yields the following result.

THEOREM 8. Let L be a real algebraic extension of K. It follows that $st(L) \geq st(K)$ in either of the following cases :

i) $L|K$ is an odd extension,

ii) L is contained in the henselian closure of some (real) valuation ring of K,

iii) L is contained in the pythagorean closure of K.

However, we shall now prove

THEOREM 9. Given $1 \leq n < \infty$, $0 \leq r < n$, there exists a pythagorean field with the following properties:

i) there is $a \in K \setminus K^2$, such that $T := K^2 \cup K^2 a$ is a fan and $st(T) = n$ holds,

ii) $\# X_T = 2^n$, $\# X_{K^2[-a]} = 2^r$,

iii) $L := K(\sqrt{-a})$ is not pythagorean, $Q(L)$ is a fan,

iv) $st(K) = n$, $st(L) = r + 1$.

Proof. First we construct a field with $r = 0$, where n is arbitrary. Let $k = \mathbb{Q}(X_1, X_2, \ldots.)$ be the rational function field in countably many indeterminates over $\mathbb{Q}$. k admits a valuation ring with residue field $\mathbb{Q}$ and value group $\Gamma \simeq \bigoplus_{\mathbb{N}} \mathbb{Z}$. Because of $\dim_{\mathbb{F}_2} \Gamma/\Gamma^2 = \aleph_0$, there are fans of arbitrary index over that preordering, which is lifted from the order of $\mathbb{Q}$. Choose a fan T of k of index $[k^{\times}:T^{\times}] = 2^{n+1}$. There are only non-archimedean orders over T. Let L be a strictly-pythagorean extension field of k in k_2, such that L^2 is a faithful extension of T (see theorem 7). We have $[L^{\times}:L^{\times 2}] = 2^{n+1}$, $\# X(L) = \# X_T(K) = 2^n$, $st(T) = st(L) = n$. k can be embedded into $\mathbb{R}$, hence, there is at least one archimedean order P on k. Let E be a euclidean closure of P. Set $K := L \cap E$. We have $K^2 = (K \cap L^2) \cap (K \cap E^2)$. Moreover, $K \cap L^2$ is a fan, and $K \cap E^2$ an archimedean order. Hence, there is $a \in K \setminus K^2$, such that $K \cap L^2 = K^2 \cup K^2 a$ is a fan. By lemma 6, we see that $K \cap E^2 = K^2[-a]$. If an archimedean order lies over some fan of K, then this fan has to be trivial. Otherwise it encloses the fan $K \cap L^2$. Over $K \cap L^2$ there are precisely 2^n orders, because their restriction remains distinct on k. $st(K) = st(K \cap L^2) = n$ follows from all this, and furthermore, we check the statements i), ii) for K.

Now assume that we have constructed a field K, belonging to the data (n,r), which satisfies the first two statements of our theorem. Then a field F with the data (n+1, r+1) can be constructed as follows. We set $F = K((X))$. Using the relation between the orders of K and F (consider the canonical valuation ring of F), one checks that F has the data (n+1, r+1). F is pythagorean again .

Assume next, that a field K with the properties i), ii) is given. By lemma 5, we see that $K^2[-a]$ is a fan. Using the method of the proof of lemma 6, it follows that $Q(L) = K^2[-a]$ holds and that Q(L) is a fan, where $L = K(\sqrt{-a})$. We have $\# X(L) = 2^{r+1}$, as an order of K has none or two extensions to an order of L. Hence, $st(L) = r+1$. If L is pythagorean, then $K^2[-a] = L^2 \cap K = K^2 \cup -K^2a$ follows, which is a contradiction to $\# X_{K^2[-a]} = 2^r < 2^n$.

We would like to remark, that it is quite certain that fields with the properties given in theorem 10 can be constructed by the methods of [14].

§3. Conjugacy of hereditarily-pythagorean extensions

It is well known that two real closures R_1 and R_2 of a real field k are k-isomorphic iff $R_1^2 \cap k = R_2^2 \cap k$ holds, compare with chapt. II, theorem 4. This theorem says how it can be determined as early as in the base field, whether two extensions R_1 and R_2 are conjugate or k-isomorphic. We shall prove analogous criteria for hereditarily-pythagorean fields in this section. The fact that it is possible to prove such criteria supports, for the second time, our conception of considering h.p. fields to be generalized real-closed fields. The structure of the Galois group $G(\Omega|K)$ has been the basic motivation for this view.

We shall study extensions $L|K$ which have the property $L = KL^2$. This can be checked, for example, for the real closures of a real field. For such extensions, we first prove three lemmata, concerning subgroups and preorderings of a higher level (see chapt.I, §1, chapt. II, §5).

LEMMA 7. <u>Let $L|K$ be an extension, such that $L = KL^2$ holds. Then the following statements hold</u>:

i) <u>A maximal subgroup of K, which extends to L, has a unique extension, which is even a faithful extension.</u>
ii) <u>A subgroup U of level n extends to L iff $U \supset K \cap L^{\times 2^n}$ holds.</u>

<u>Proof</u>. i) Assume that U is extendable to L. Let V denote an extension: $U = V \cap K^{\times}$. If $V \supset L^{\times 2^n}$, then $V \supset UL^{\times 2^n}$. From $L^{\times} = K^{\times}L^{\times 2}$, it follows that $L^{\times} = K^{\times}L^{\times 2^n}$, and, furthermore, that the homomorphism $K^{\times} \to L^{\times}/UL^{\times 2^n}$ is surjective. Its kernel is U. Hence, there is an isomorphism $K^{\times}/U \to L^{\times}/UL^{\times 2^n}$. This shows that $L^{\times}/UL^{\times 2^n}$ is cyclic, thus $UL^{\times 2^n}$ is a maximal subgroup. This implies $V = UL^{\times 2^n}$. Moreover, one sees that the exact levels of U and V coincide.
ii) Assume that U is extendable, say, $U = V \cap K^{\times}$. By i), V has also the level n, hence $L^{\times 2^n} \subset V$ and $K^{\times} \cap L^{\times 2^n} \subset U$. Conversely, assume that $K^{\times} \cap L^{\times 2^n} \subset U$ holds. Then $-1 \notin UL^{\times 2^n}$ follows, which implies the existence of an extension.

In the proof of the theorems 10 and 11 we shall have to solve the following problem. Assume that $K|E$ is an extension, such that $K = EK^2$, let M be an intermediate field. Assuming that the subsets $E \cap K^{2^n}$ are known, the problem is to obtain informations from this about $M \cap K^{2^n}$.

By lemma 7, we have $E^{\times} \cap K^{\times 2^n} = \bigcap U$, where U ranges over all subgroups of level n of K, which are extendable to E.

Such a subgroup has a unique extension $\tilde{\tilde{U}}$ to L. We have the result: $K^{\times 2^n} = \cap \tilde{\tilde{U}}$, where U is a subgroup of level n of K, such that $U \supset K^{2^n} \cap E$. Hence, $M^{\times} \cap K^{\times 2^n} = \cap (M^{\times} \cap \tilde{\tilde{U}})$. The subgroup $M^{\times} \cap \tilde{\tilde{U}}$ is a faithful extension of U to M. Because of $K = MK^2$, lemma 1 applies and says that $M \cap \tilde{\tilde{U}} =: \tilde{U}$ is the unique faithful extension of U, which encloses $M^{\times} \cap K^{2^n}$. Thus we have: $E^{\times} \cap K^{\times 2^n} = \cap U$, $M^{\times} \cap K^{\times 2^n} = \cap \tilde{U}$.

Assume next, in addition, that K is strictly-∞-pythagorean. This means that, for every subgroup U of a higher level, the set $P := U \cup \{0\}$ is an ordering of higher level. In this case K^{2^n} is a preordering of level n. Hence, we may restrict ourselves to orderings of level n in order to give presentations for $E \cap K^{2^n}$ and $M \cap K^{2^n}$. Let P be an ordering of level n of K, such that $P \supset E \cap K^{2^n}$. Then P has, by lemma 7, a unique faithful extension $\tilde{\tilde{P}}$, where $\tilde{\tilde{P}}$ is an ordering of higher level of E, and a unique faithful extension to an ordering $\tilde{P}$ of higher level of M, such that $\tilde{P} \supset M \cap K^{2^n}$ holds. As before, we have: $E \cap K^{2^n} = \cap P$, $M \cap K^{2^n} = \cap \tilde{P}$, where P ranges over all orderings P of level n of E, which extends to K.

In the following two lemmata, the extensions $\tilde{U}$ and $\tilde{P}$ will be described in a special case.

LEMMA 8. <u>Let K be a real extension of the strictly-pythagorean field E, such that $K = EK^2$ holds. Assume that</u>

$M = E(\sqrt{a})$ is a proper quadratic extension, where $\sqrt{a} \in K^{2^n}$. Then the following statements hold.

i) A maximal subgroup $U \supset E^{\times} \cap K^{2^n}$ has precisely two faithful extensions to M.

ii) $\tilde{U}$ is that faithful extension which contains the element $\sqrt{a}$.

Proof. By chapt. III, §3, lemma 9, U has precisely two faithful extensions to M. They can be distinguished by noting whether they contain $\sqrt{a}$ or not. From $\tilde{U} \supset M^{\times} \cap K^{2^n}$ and $\sqrt{a} \in K^{2^n}$, ii) follows.

Using chapt.I, §4, theorem 22, this time, instead of chapt. III, §3, lemma 9, one proves the following lemma in a similar manner, observing that $a \in P$ implies $(\sqrt{a})^2 \in P$ and $\sqrt{a} \in \tilde{P} \cup -\tilde{P}$.

LEMMA 9. Let K be a strictly-∞-pythagorean extension of the real field E, such that $K = EK^2$ holds. Assume that $M = E(\sqrt{a})$ is a proper quadratic extension, where $\sqrt{a} \in K^{2^n}$. Then the following statements hold.

i) An ordering P of level n of K, which satisfies $P \supset E \cap K^{2^n}$, has precisely two faithful extensions to M.

ii) P is that faithful extension, which contains the element $\sqrt{a}$.

The following theorem 10 yields our first criterion for conjugacy. We consider a 2-closed extension $\Omega|k$ and an intermediate field K, which is h.p. relative to Ω. Let L be a real extension of K in Ω. From the particular structure of the Galois group $G(\Omega|K)$, one derives that there exists a unique maximal intermediate field of $L|K$, which has odd degree over K. This field will be denoted by $(L|K)_U$ or - for short - L_U.

THEOREM 10. Let $\Omega|k$ be a 2-closed Galois extension of the real field k, and K be an intermediate field, which is hereditarily-pythagorean relative to Ω. Let L and F be real extensions of K in Ω, such that $L = KL^2$ and $F = KF^2$ hold. Then the following holds:

$$L \underset{K}{\simeq} F \iff L_U \underset{K}{\simeq} F_U \ , \quad \bigwedge_{n \in \mathbb{N}} L^{2^n} \cap K = F^{2^n} \cap K \ .$$

Proof. It remains to show the implication " $\Leftarrow$ ". Let $\varphi: L_U \to F_U$ be a K-isomorphism, which exists by assumption. We shall show: (*) $\bigwedge_{n\in\mathbb{N}} \varphi(L^{2^n} \cap L_U) = F^{2^n} \cap \varphi(L_U)$. By chapt. III, lemma 4, corollary 1, we have $L_U = KL_U^2$, since $L_U|K$ is an odd extension. It follows that $L_U = KL_U^{2^n}$ holds for every $n \in \mathbb{N}$. Assume that $x \in L$ satisfies $x^{2^n} \in L_U$. Thus, $x^{2^n} = \alpha y^{2^n}$ for some $\alpha \in K$, $y \in K$. This implies $L^{2^n} \cap L_U = L_U^{2^n}(L^{2^n} \cap K)$. Correspondingly, $F^{2^n} \cap F_U = F_U^{2^n}(F^{2^n} \cap K)$. Hence, the assertion is proved. We shall now study pairs (E,ψ), where E is an intermediate field of

$L|L_U$ and ψ a monomorphism $E \to F$, such that the following holds:

$$(**) \qquad \psi|L_U = \varphi, \quad \bigwedge_{n\in\mathbb{N}} \psi(L^{2^n} \cap E) = F^{2^n} \cap \psi(E).$$

The existence of a maximal pair (E,ψ) follows from Zorn's lemma. We assert $E = L$. Suppose $E \subsetneqq L$. Then a proper quadratic extension $E(\sqrt{a})$ has to be contained in L. We have $a \in E \cap L^2$, hence, $\psi(a) \in F^2$ and $\psi(E)(\sqrt{\psi(a)}) \subset F$. ψ has two extensions $E(\sqrt{a}) \to \psi(E)(\sqrt{\psi(a)})$. We shall prove that one of these extensions also satisfies the condition (**). Thus, we shall obtain a contradiction. Because of $L^\times = K^\times L^{\times 2}$, there exists $\alpha \in K^\times$, such that $\alpha\sqrt{a} \in L^2$. Hence $\alpha^2 a \in L^4 \cap E$. From the properties of ψ, it follows that $\alpha^2\psi(a) \in F^4 \cap \psi(E)$. Therefore, there is a root $\alpha\sqrt{\psi(a)} \in F^2$. This root is to be fixed in the sequel. We may assume $\sqrt{a} \in L^2$, $\sqrt{\psi(a)} \in F^2$, substituting $\sqrt{a}$ by $\alpha\sqrt{a}$ if necessary. Define $\hat{\psi}$: $E(\sqrt{a}) \to \psi(E)(\sqrt{\psi(a)})$ by $\hat{\psi}|E = \psi$, $\hat{\psi}(\sqrt{a}) = \sqrt{\psi(a)}$. Given $n \in \mathbb{N}$, we have to compute $\hat{\psi}(L^{2^n} \cap E(\sqrt{a})^\times)$. Because of $L^\times = K^\times L^{\times 2^n}$, there is $\beta \in K$, such that $\beta\sqrt{a} \in L^{\times 2^n}$, $\beta^2 a \in L^{\times 2^{n+1}} \cap E$. Hence, $\beta^2\psi(a) \in F^{2^{n+1}} \cap \psi(E)$, which implies $\beta\sqrt{\psi(a)} \in F^{2^n}$ or $-\beta\sqrt{\psi(a)} \in F^{2^n}$. If $-\beta\sqrt{\psi(a)} \in F^{2^n}$, then $-\beta \in F^2$ as $\sqrt{\psi(a)} \in F^2$ holds. But this would imply $-\beta \in L^2$ and, in view of $\beta\sqrt{a} \in L^2$, the statement $\sqrt{a} \in -L^2$, which contradicts our choice of $\sqrt{a}$. Thus we have proved

$\hat{\psi}(\beta\sqrt{a}) = \beta\hat{\psi}(\sqrt{a}) \in F^{2^n}$. By lemma 8 and its foregoing remarks, we have $L^{2^n} \cap E(\sqrt{a}) = \cap \tilde{U}$, where U ranges over those subgroups of a higher level which lie above $L^{2^n} \cap E$. By $\tilde{U}$, we denote that faithful extension, which contains $\beta\sqrt{a}$. From this, it follows that $\hat{\psi}(L^{2^n} \cap E(\sqrt{a})^{\times}) = \cap \hat{\psi}(U) = F^{2^n} \cap \psi(E)(\sqrt{\psi(a)})$. As $\hat{\psi}(\tilde{U}) | \psi(U)$, $\beta\sqrt{a} \in \hat{\psi}(\tilde{U})$, and, because of $\psi(L^{2^n} \cap E) = F^{2^n} \cap \psi(E)$, ψ induces a bijection between the subgroups of level n of E, which lie over $L^{2^n} \cap E$, and the subgroups of level n of $\psi(E)$, which enclose $F^{2^n} \cap \psi(E)$.

The assumption $E \subsetneqq L$ has thus been led to a contradiction. Hence, there is a monomorphism $\psi: L \to F$, such that $\psi(L)^{2^n} = \psi(L^{2^n}) = \psi(L) \cap F^{2^n}$ for every $n \in \mathbb{N}$. Because of $\psi(L) \supset F_U$, F is contained in the maximal 2-extension of $\psi(L)$. But $\psi(L) \cap F^2 = \psi(L)^2$ implies that $\psi(L)$ is quadratically closed relative to F. Thus, $F = \psi(L)$.

In the following theorem, we shall drop the assumption that the base field is h.p. Rather than that, we shall be concerned with the following situation: <u>$\Omega|k$ is a 2-closed extension, k is real, K, L are hereditarily-pythagorean intermediate fields subject to the conditions</u>:

1) <u>$kK^2 = K$, $kL^2 = L$ 2) $\Omega|K$, $\Omega|L$ 2-extensions</u>
3) <u>$K^{2^n} + K^{2^n} = K^{2^n}$, $L^{2^n} + L^{2^n}$ for every $n \in \mathbb{N}$.</u>

Under assumption 2), the condition 3) is equivalent to the statement that K and L are hereditarily-strictly-∞-pythagorean relative to Ω. In order to prove this, use theorem 10 of chapt. III and theorem 27, corollary 2, of chapt. I.

THEOREM 11. <u>On the foregoing assumptions, it follows that</u>

$$K \underset{k}{\cong} L \Leftrightarrow \bigwedge_{n\in\mathbb{N}} K^{2^n} \cap k = L^{2^n} \cap k.$$

<u>Proof</u>. As in the proof of theorem 10, we consider pairs (E,φ), such that the following holds:

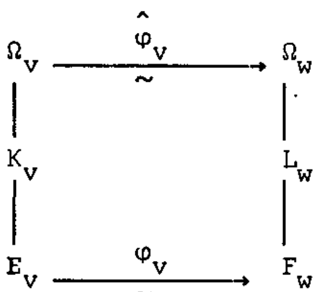
(*) $k \subset E \subset K$, $\varphi: E \to L$, $\varphi|k = id$, $\bigwedge_n (K^{2^n} \cap E) = L^{2^n} \cap \varphi(E)$.

Let (E,φ) be a maximal pair. Using lemma 9 this time, instead of lemma 8 (K and L are strictly-∞-pythagorean), one proves, such as with theorem 10, that E is quadratically closed relative to K. From $\varphi(K^2 \cap E) = L^2 \cap \varphi(E)$, it results that $F := \varphi(E)$ is quadratically closed in L, too. This closedness implies that E and F are themselves strictly-∞-pythagorean. To prove this, show that E^{2^n} and F^{2^n} are fans. By the above quoted theorem 27, corollary 2, E^2 (respectively F^2) is a strongly-homogeneous fan. Hence $A_{E^2} = A(E^2)$, and the residue field of A_{E^2} is euclidean. Correspondingly, we obtain $A_{F^2} = A(F^2)$, and the fact that $\bar{A}_{F^2}$ is euclidean. It also holds that $A_{K^2} = A(K^2)$, $A_{F^2} = A(F^2)$, $\bar{A}_{K^2}$ and $\bar{A}_{F^2}$ are euclidean. Since $\Omega|K$ and $\Omega|L$ are 2-extensions, the rings $A(K^2)$ and $A(L^2)$ are Ω-henselian. As E is quadratically closed in K, and F in L, it follows that $A(K^2) \cap E = A(E^2)$, $A(L^2) \cap F = A(F^2)$. Hence, one finds in K a Ω-henselian closure $\hat{E}$ of $A(E^2)$, correspondingly a Ω-henselian closure $\hat{F}$ of $A(F^2)$ in L. Because of $\varphi(A(E^2)) = A(F^2)$, φ extends to an isomorphism $\hat{\varphi}: \hat{E} \to \hat{F}$. We want to show that $(\hat{E},\hat{\varphi})$ satisfies the condition (*), too. From this, it will follow that $\hat{E} = E$, $\hat{F} = F$. $\hat{E} = E\hat{E}^2$, $\hat{F} = F\hat{F}^2$ results from the henselian lemma. Hence, every ordering P of a higher level of E, which satisfies $P \supset K^{2^n} \cap E (= E^{2^n})$, can be extended uniquely to an ordering of $\hat{E}$. Thus, $\tilde{P}$ is the uniquely determined extension of P to $\hat{E}$. The same holds for the orderings of F. Because of $\varphi(K^{2^n} \cap E) = \varphi(E^{2^n}) = F^{2^n} = L^{2^n} \cap F$, φ induces a bijection between the orderings of E and F, which preserves the exact level. From $\hat{\varphi}(\tilde{P}) \cap F = \varphi(P)$, it follows that $\hat{\varphi}(\tilde{P}) = \varphi(P)$. This shows, as explained before lemma 8, that $\hat{\varphi}(K^{2^n} \cap \hat{E}) = L^{2^n} \cap \hat{F}$ for every $n \in N$.

With that, we have proved that $A(E^2)$ and $A(F^2)$ are Ω-henselian valuation rings of E and F. From this, we shall obtain that E admits no odd extension in K. But this will mean that $\Omega|E$ must be a 2-extension as, by the theorems of Sylow, the 2-group $G(\Omega|K)$ may be extended to a 2-Sylow group of $G(\Omega|E)$. The fact that $\Omega|E$ is a 2-extension combined with the quadratic closedness of E in K implies $E = K$ and $\varphi(E) = L$ (see the proof of theorem 10).

In order to prove that E admits no odd extensions in K, we first adopt a more convenient notation. Let v be a valuation of Ω, which belongs to the unique extension of $A(E^2)$ to Ω. The restriction of v to an intermediate field M may also be denoted by v. We write M_v for its residue field.

Since $\Omega|k$ is Galois, the monomorphism $\varphi: E \to F$ extends to a k-automorphism $\hat{\varphi}: \Omega \to \Omega$. Thus the valuation $w := \hat{\varphi}(v)$ belongs to the unique extension of $A(F^2)$ to Ω. Concerning the notation, we deal with w such as with v. φ and $\hat{\varphi}$ induce isomorphisms φ_v, $\hat{\varphi}_v$ of the residue fields, and one obtains the following diagramm



As already noted, the fields E_v, K_v, F_w, L_w are euclidean. Because of assumption 2), $\Omega_v|K_v$ and $\Omega_w|F_w$ are 2-extensions. Hence, $\Omega_v = K_v(i)$ and $\Omega_w = L_w(i)$. This means that K_v and L_w are real closures of E_v in Ω_v and of F_w in Ω_w. Since E_v and F_w are euclidean, it must hold that $E_v^2 = K_v^2 \cap E_v$, $F_w^2 = L_w^2 \cap F_w$, $\varphi_v(E_v^2) = F_w^2$. By chapt. III, theorem 4, there exists an extension of $\varphi_v: E_v \to F_w$ to an isomorphism $\sigma: K_v \to L_w$.

Now assume M to be a finite odd intermediate field of K|E. Let P be an ordering of higher level of E, and P' a faithful extension of P to M. We shall show: $P' = \tilde{P} \Leftrightarrow \bar{P}' = M_v \cap K_v^2$. The necessity follows from $\bar{\tilde{P}} = K_v^2$ which implies $\bar{\tilde{P}} = M_v \cap K_v^2$. In order to prove the converse, we apply chapt. I, § 4, lemma 12, which yields that P has only one faithful extension P', such that $\bar{P}' = \bar{\tilde{P}}$. An analogous criterion is valid for the extensions of orderings of F to an odd extension N|F, where $N \subset L$ holds. Assume, for a moment, that an extension $\psi: M \to N$ of $\varphi: E \to L$ is given, where $F \subset N \subset L$. By the properties of v and w, we must have $\psi(v) = w$. Hence, ψ induces an isomorphism $\psi_v: M_v \to N_v$, which extends φ_v. If, additionally, it holds that $\psi_v = \sigma|M_v$, then, given any ordering P of E, it follows that $\overline{\psi(\tilde{P})} = \psi_v(\bar{\tilde{P}}) = \psi_v(M_v \cap K_v^2) = N_w \cap L_w^2$. This implies $\psi(\tilde{P}) = \varphi(P)$ and, finally, $\psi(M \cap K^{2^n}) = N \cap L^{2^n}$ for $n \in \mathbb{N}$. The maximality of (E,φ) thus yields $M = E$.

We shall now construct such an extension $\psi: M \to N$. First assume that (M,v) is unramified over (E,v). From the henselian lemma, applied to w, the existence of an intermediate field N of L|F follows, such that $N_w = \sigma(M_v)$. At the same time, we get an isomorphism $\psi: M \to N$, such that $\psi_v = \sigma|M_v$.

With that we have shown that every odd extension M of $K|E$ is purely **ramified**, moreover, tamely purely ramified . In the case of $M \neq E$, there exists $a \in E$ and an odd number e, such that $E(\sqrt[e]{a}) \subset M$, $E(\sqrt[e]{a}):E = e$. We may assume that $M = E(\sqrt[e]{a})$. Since $\Omega|L$ is a 2-extension, the equation $x^e - \varphi(a) = 0$, which is reducible over Ω, has already to be reducible over L. This means that L contains a root $\sqrt[e]{\varphi(a)}$. This root is even unique, since L is real. Define $\psi: M \to L$ by means of $\psi(\sqrt[e]{a}) = \sqrt[e]{\varphi(a)}$, $\psi|E = \varphi$. Because of the pure ramification , it obviously holds that $\psi_v = \varphi_v = \sigma|u_v$.

We apply this theorem to the real Ω-closures $(R,\tilde{P})$, associated with an ordering P of higher level of k (see chapt.II, § 2). The theorem 5 of that place, and its proof shows that R satisfies the conditions 2) and 3). However, the condition 1) is also satisfied, for if we choose $\alpha \in k$, such that $\alpha^{2^{n-1}} \in -P$, then we have $\alpha^{2^{n-1}} \in -\tilde{P}$, in particular $\alpha \notin R^2$. Now note that $-R^{x^2}$, αR^{x^2} generate the group R^x/R^{x2} by chapt. II, § 2, theorem 5,i).

THEOREM 12. <u>Let $\Omega|k$ be a 2-closed Galois extension of the real field k, and P be an ordering of higher level of k. Given any two real Ω-closures $(R_i,\tilde{P}_i)$, i=1,2 , of (k,P), the following holds:</u>

$$R_1 \underset{k}{\simeq} R_2 \iff \bigwedge_n R_1^{2^n} \cap k = R_2^{2^n} \cap k .$$

If, for instance, P is an order, then R_1 and R_2 are euclidean, which implies $R_i^{2^n} = R_i^2$, $R_i^{2^n} \cap k = P$ and, in virtue of the theorem 12, $R_1 \simeq R_2$. Thus, our theorem 12 extends the well-known theorem of Artin and Schreier [4 ; Satz 8]. In the case of orderings of an exact level $n \geq 2$, there are, in general, non-isomorphic real Ω-closures $(R,\tilde{P})$. We shall now attend to the problem of describing the isomorphy classes more detailed.

THEOREM 13. Let P be an ordering of the exact level $m \geq 2$ of k, and $\Omega|k$ be a 2-closed Galois extension. Let v be the valuation belonging to A(P), and Γ its value group. Then the following statemants hold.

i) The mapping $(R,\tilde{P}) \mapsto \{v(R^{2^n} \cap k^x)\}_{n\in\mathbb{N}}$ yields a bijection between the set of isomorphy classes of real Ω-closures $(R,\tilde{P})$ of (k,P), and the set of all those families $\{\Gamma_n\}_{n\in\mathbb{N}}$ of subgroups of Γ, which are subject to the conditions

α) $\Gamma_n \supseteq \Gamma_{n+1}$ β) Γ_n/Γ_{n+1} is cyclic of order 2^n

γ) $v(P^x) = \Gamma_{m-1}$.

ii) Any two real Ω-closures of (k,P) are isomorphic over k iff $[\Gamma:\Gamma^2] = 2$ holds.

iii) If there is more than only one isomorphy class, there are in fact infinitely many classes.

Using this theorem, we can characterize those fields, which admit for every ordering of higher level only one isomorphy class of real closures.

COROLLARY. Every ordering of higher level of k has a single isomorphy class of real Ω-closures iff it holds for every real valuation ring of k, with value group Γ, that $[\Gamma:\Gamma^2] \doteq 2$.

Proof of the corollary. Assume that there is a single isomorphy class for every ordering. Let A denote a real valuation ring, such that $[\Gamma:\Gamma^2] \geq 2$. By chapt. I, § 2, theorem 11, there exists an ordering P of an exact level $n \geq 2$, which is compatible with A. Thus, $A(P) \subset A$, and Γ is seen to be a factor group of a group Γ', where $[\Gamma':\Gamma'^2] = 2$. Hence, $[\Gamma:\Gamma^2] = 2$ too.

In particular, the uniqueness occurs in the case of Pasch-fields (= SAP-fields, see chapt. I, § 3), for instance, in the case of algebraic function fields F over $\mathbb{R}$, such that $tr(F|\mathbb{R}) = 1$. But the uniqueness may also occur for other fields; consider a field k_o, which has only archimedean orders (e.g. $k_o = \mathbb{Q}$). Then every real valuation ring Γ of $k_o(X)$ has $\mathbb{Z}$ as its value group. Thus, $[\Gamma:\Gamma^2] = 2$. In the case of $k = \mathbb{Q}(X,Y)$, there is generally no uniqueness, since there are real valuation rings, such that $[\Gamma:\Gamma^2] = 4$ holds.

Proof of theorem 14. i) Let $(R,\tilde{F})$ be a real Ω-closure of (k,P), and α an element of k^x, such that $\alpha^{2^{m-1}} \in -P$. As noted before theorem 12, the cosets $-R^{\times 2}$ and $\alpha R^{\times 2}$ generate the group $R^{\times}/R^{\times 2}$. Moreover, R has the two orders $\tilde{P}_1{}^{+} = R^2 \cup \alpha R^2$, $\tilde{P}_1{}^{-} = R^2 \cup -\alpha R^2$, and for every $n \geq 2$, the unique ordering of the exact level n is given by $\tilde{P}_n = R^{2^n} \cup -\alpha^{2^{n-1}} R^{2^n}$. It further holds that $R^{2^{n-1}} = R^{2^n} \cup \alpha^{2^{n-1}} R^{2^n}$ (chapt. I, theorem 16, corollary 2 and chapt. II, theorem 5). From chapt. I, lemma 14, and the corollary 2 of chapt. I, theorem 27, one derives $A(R^2) = A(R^{2^n}) = A(\tilde{P}_n)$ for every $n \in \mathbb{N}$. Since $\Omega|R$ is a 2-extension, $A(R^2)$ proves to be a Ω-henselian valuation ring. Its residue field is euclidean by chapt. II, theorem 5. Thus $\bar{\tilde{A}}^{\times} = \bar{\tilde{A}}^{\times 2^n} \cup -\bar{\tilde{A}}^{\times 2^n}$, where $\tilde{A} = A(R^2)$, $n \in \mathbb{N}$. Let $\tilde{v}$ be the valuation belonging to $\tilde{A}$, and $\tilde{\Gamma}$ its value group. Then, for every $n \in \mathbb{N}$: $\tilde{v}(\tilde{P}^{\times}_{n+1}) = \tilde{v}(R^{\times 2^n}) = \tilde{\Gamma}^{2^n}$, $\tilde{\Gamma}/\tilde{\Gamma}^{2^n}$ is cyclic of order 2^n. The valuation $v := \tilde{v}|k$ belongs to the valuation ring $\tilde{A} \cap k = A(\tilde{P}_m) \cap k = A(\tilde{P}_m \cap k) = A(P)$. Let Γ be its value group. From $\Gamma\tilde{\Gamma}^2 = \tilde{\Gamma}$, it follows that $\Gamma/\Gamma \cap \tilde{\Gamma}^{2^n}$ is cyclic of order 2^n. We have $\Gamma \cap \tilde{\Gamma}^{2^n} = v(R^{2^n} \cap k^{\times}) = v(\tilde{P}_{n+1} \cap k^{\times})$. To prove this, one makes use of the relation $A(P)^{\times} \subset (R^{2^n} \cap k^{\times}) \cup -(R^{2^n} \cap k^{\times})$, which results from $\bar{\tilde{A}}^{\times} = \bar{\tilde{A}}^{\times 2^n} \cup -\bar{\tilde{A}}^{\times 2^n}$. It is now easily checked that the family $\{\Gamma_n\}_{n \in \mathbb{N}}$, where $\Gamma_n = v(R^{2^n} \cap k^{\times})$, satisfies α), β), γ).

The preorderings $T_n := R^{2^n} \cap k^{\times}$ can be re-obtained from the family $\{\Gamma_n\}$, for, if $n \geq m$, then $T_n^{\times} = v^{-1}(\Gamma_n) \cap P$

follows from $A(P)^{x} \subset T_n^{x} \cup -T_n^{x}$. If $n < m$, then one recursively constructs T_m by means of $T_{m-1} = T_m \cup \alpha^{2^{m-1}} T_m$, $T_{m-1} = T_{m-2} \cup \alpha^{2^{m-2^m}} T_{m-2}$ etc. Taking theorem 12 into account we thus obtain the fact that the map $(R,\tilde{P}) \mapsto \{v(R^{2^n} \cap k)\}_{n\in\mathbb{N}}$ is injective. In order to prove that this map is surjective too, we consider objects $\{L, \tilde{P}, \{\tilde{\Gamma}_n\}_{n\in\mathbb{N}}\}$, consisting of a faithful extension $(L,\tilde{P})$ of (k,P) in Ω, a family $\{\Gamma_n\}_{n\in\mathbb{N}}$ of subgroups $\tilde{\Gamma}$, subject to the conditions α), β), γ), and $\tilde{\Gamma}_n \cap \Gamma = \Gamma_n$, $\tilde{v}(\tilde{\Gamma}_{m-1}) = \tilde{P}$, where $\tilde{v}$ belongs to $A(P)$ and $\tilde{\Gamma}$ is the value of $\tilde{v}$. Zorn's lemma proves the existence of a maximal object, denoted by $\{R, \tilde{P}, \{\tilde{\Gamma}_n\}\}$. We shall show that $(R,\tilde{P})$ is a real Ω-closure of (k,P). By the first part of the proof, it then follows that $v(R^{2^n} \cap k) = \Gamma_n$. To prove the assertion on $(R,\tilde{P})$, we apply the extension theory of chapt.I, § 4. $A(\tilde{P})$ has to be Ω-henselian, since, otherwise, the Ω -henselian closure of $(R, A(\tilde{P}))$ would lead to the construction of a proper greater object; for $\tilde{P}$ is faithfully extendable to the Ω-henselian closure, which is an intermediate extension. Denote the extension of $A = A(\tilde{P})$ to Ω by B. Thus, $\bar{B}|\bar{A}$ is a 2-closed Galois extension. Choose a real $\bar{B}$-closure to the order $\bar{\tilde{P}}$ of $A.\tilde{P}$ is faithfully extendable to every such finite unramified extension of R in Ω, the residue field of which is contained in this real $\bar{B}$-closure. The same obviously holds for $\{\Gamma_n\}$. Hence, $\bar{A}$ is indeed real-closed in $\bar{B}$, i.e. $\bar{B} = \bar{A}(i)$, $\bar{A}$ is euclidean. Let L be a proper odd extension of R in Ω. Then L has to be a purely ramified extension with an odd ramification index. It is possible to construct extensions of $\tilde{P}$ and $\{\tilde{\Gamma}_n\}$ to L. Hence, $\Omega|R$ has to be a 2-extension. Choose $\alpha \in k^x$ with $\alpha^{2^{n-1}} \in -P^x$. Since $\tilde{\Gamma}/v(\tilde{P}^x)$ is cyclic of order 2^m, it follows that $\tilde{v}(\alpha) \notin \tilde{\Gamma}$. Choose $a \in R^x$, such that $\tilde{v}(b) \notin \tilde{\Gamma}^2 \cup v(\alpha)\tilde{\Gamma}^2$. It is possible to extend $\tilde{P}$ and $\{\tilde{\Gamma}_n\}$ to $R(\sqrt{b})$. Thus, $[\tilde{\Gamma}:\tilde{\Gamma}^2] = 2$. This yields $[R^x:R^{x2}] = 4$, as $\bar{A}$ is euclidean and A is Ω-henselian. Observing $Q_n(R) = R^{2^n}$, we apply chapt. I, lemma 14, to R, and get the structure of R relative to their orderings. Moreover, the refletions at the beginning of chapt. I, § 4, show that $\tilde{P}$ has no faithful extension in Ω. Hence, $(R,\tilde{P})$ is a real Ω-closure of (k,P).

ii), iii) It remains to study the families $\{\Gamma_n\}_{n\in\mathbb{N}}$, such that $v(P^x) = \Gamma_{m-1}$. Since Γ/Γ_{m-1} is cyclic, the groups Γ_i, $i=1,..,m-2$, are determined by Γ_{m-1}. Therefore, we have to construct all groups $\Gamma_m \subset \Gamma_{m-1}$, such that Γ/Γ_m is cyclic of order 2^m. Let $\alpha\Gamma_{m-1}$ be a generator of Γ/Γ_{m-1}. If Γ/Γ_m is cyclic, it is generated by $\alpha\Gamma_m$. In this case, it follows that $\alpha^{2^{m-1}} \in \Gamma_{m-1} \setminus \Gamma_m$. Hence, we have to find all characters $\chi: \Gamma_{m-1} \to \{1,-1\}$, such that $\chi(\alpha^{2^{m-1}}) = -1$. These characters correspond bijectively with the characters of $\Gamma_{m-1}/\Gamma^2_{m-1} \cup \alpha^{2^{m-1}}\Gamma^2_{m-1}$. The inclusion $\Gamma_{m-1} \to \Gamma$ induces an isomorphism of the latter factor group with $\Gamma/\Gamma^2 \cup \alpha\Gamma^2$. From this, one concludes that there exists only one of the required characters iff $[\Gamma:\Gamma^2] = 2$ holds. Otherwise, one can construct at least two of the desired groups. These reflections are valid for every **n**, hence, it follows that ii) and iii) hold. The statement iii) can even be strengthened to the following result: there is only one single or at least $2^{\aleph_0}$-many isomorphy classes.

References

[1] Artin, E.: Kennzeichnung des Körpers der reellen algebraischen Zahlen. Abh. Math. Sem. Univ. Hamburg 3 (1924), 319-323.

[2] Artin, E.: Über die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Univ. Hamburg 5 (1927), 100-115.

[3] Artin, E. und Schreier, O.: Eine Kennzeichnung der reell-abgeschlossenen Körper. Abh. Math. Sem. Univ. Hamburg 5 (1927), 225-231.

[4] Artin, E. und Schreier, O.: Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Univ. Hamburg 5 (1927), 85 -99

[5] Baer, R.: Über nicht-archimedisch geordnete Körper. Sitz.-Ber. d. Heidelberger Akademie 1927, 8. Abhandl.

[6] Becker, E.: Euklidische Körper und euklidische Hüllen von Körpern. J. reine angew. Math. 268-269 (1974), 41-52.

[7] Becker, E. und Spitzlay, K.-J.: Zum Satz von Artin-Schreier über die Eindeutigkeit des re-

ellen Abschlusses eines angeordneten Körpers. Comment. Math. Helvetici 50 (1975), 81 -87.

[8] Becker, E. und Köpping, E.: Reduzierte quadratische Formen und Semiordnungen reeller Körper. Abh. Math. Sem. Univ. Hamburg 46, to appear.

[9] Bourbaki, N.: Algèbre, Chap. VI, Paris 1952.

[10] Bredikhin, S. V., Ershov, Yu.L. and Kal'nei, V.E.: Fields with two linear orderings. Math. Notes 7 (1970), 319-325.

[11] Bröcker, L.: Über eine Klasse pythagoreischer Körper. Arch. Math. 23 (1972), 405-407.

[12] Bröcker, L.: Zur Theorie der quadratischen Formen über formal reellen Körpern. Math. Ann. 210 (1974), 233-256.

[13] Bröcker, L.: Characterization of fans and hereditarily pythagorean fields. Math.Z. 151 (1976), 149-163.

[14] Bröcker, L.: Über die Anzahl der Anordnungen eines Körpers. Arch. Math., to appear.

[15] Brown, R.: Superpythagorean fields. J. Algebra 42 (1976), 483-494.

[16] v. Chossy, R. und Priess-Crampe,S.: Ordnungsverträgliche Bewertungen eines angeordneten Körpers. Arch. Math. 26 (1975), 372-387.

[17] Craven, Th.: The Boolean space of orderings of a field. Trans. AMS 209 (1975), 225-235.

[18] Deuring, M.: Algebren. Berlin 1935.

[19] Diller, J. und Dress, A.: Zur Galoistheorie pythagoreischer Körper. Arch. Math. 16 (1965), 148-152.

[20] Dress, A.: Metrische Ebenen über quadratisch perfekten Körpern. Math. Z. 92 (1966), 19-29.

[21] Dubois, D.W.: A note on David Harrison's theory of preprimes. Pac. J. Math. 21 (1967), 15-19.

[22] Dubois, D.W.: Second note on David Harrison's theory of preprimes. Pac. J. Math. 24 (1968), 57-68.

[23] Dubois, D.W.: Infinite primes and ordered fields. Dissertationes Mathematicae, LXIX, Warschau 1970.

[24] Elman, R. and Lam, T.-Y.: Quadratic forms over formally real fields and pythagorean fields. Amer. J. Math. 94 (1972), 1155-1194.

[25] Elman, R. and Lam, T.-Y. and Prestel, A. : On some Hasse principles over formally real fields. Math. Z. (1973), 291-301.

[26] Endler, O.: Valuation theory. Berlin-Heidelberg-New York 1972.

[27] Geyer, W.-D.: Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist. J. Number Theory 1 (1969), 346-374.

[28] Griffin, M.: Galois Theory and ordered fields. Queen's University, Kingston, Ontario. Preprint No. 1972 - 18, June 1972.

[29] Gross, H. and Hafner, P.: Über die Eindeutigkeit des reellen Abschlusses eines angeordneten Körpers. Comment. Math. Helvetici 44 (1969), 491-494.

[30] Hall Jr., M.: The theory of groups. 5th printing, New York: The Macmillan Company 1964.

[31] Halter-Koch, F.: Über Radikalerweiterungen I. Acta arithmetica, to appear.

[32] Hardy, G.H. and Wright, E.M.: An introduction to the theory of numbers, 4th ed., Oxford, 1960.

[33] Hewitt, E. and Ross, K.A.: Abstract Harmonic Analysis I. Berlin-Göttingen-Heidelberg 1963.

[34] Hilbert, D.: Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Zahl n-ter Potenzen (Waringsches Problem). Math. Ann. 67 (1909), 281-300.

[35] Hochschild, G. and Serre, J.P.: Cohomology of group extensions. Trans. AMS 74 (1953), 110 - 134.

[36] Iwasawa, K.: On solvable extensions of algebraic number fields. Annals. Math. 58 (1953), 548 - 572.

[37] Jacobson, N.: Lectures in Abstract Algebra, Vol. III, 1964.

[38] Joly, J.-R.: Sommes de puissance d-ièmes dans un anneau commutatif. Acta arithmetica XVII (1970), 37-114.

[39] Knebusch, M.: On the uniqueness of real closures and the existence of real places. Comment. Math. Helvetici 47 (1972), 260-269.

[40] Knebusch, M. and Wright, M.J.: Bewertungen mit reeller Henselierung. J. reine angew. Math. 268/289 (1976), 314-321.

[41] Knebusch, M.: Generalization of a theorem of Artin-Pfister to arbitrary semilocal rings, and related topics. J. Algebra 36 (1975), 46-57.

[42] Krull, W.: Allgemeine Bewertungstheorie. J. reine angew. Math. 167 (1932), 160-196.

[43] Lam, T.Y.: The Algebraic theory of Quadratic Forms. Reading 1973.

[44] Pejas, W.: Die Modelle des Hilbertschen Axiomensystems der absoluten Geometrie. Math. Ann. 143 (1961), 212-235.

[45] Pfister, A.: Quadratische Formen in beliebigen Körpern. Invent. Math. 1 (1966), 116-132.

[46] Prestel, A.: Quadratische Semi-Ordnungen und quadratische Formen. Math. Z. 133 (1973), 319-342.

[47] Prestel, A.: Lectures on formally real fields. IMPA-Lecture notes, Rio de Janeiro, 1975.

[48] Prestel, A. und Ziegler, M.: Erblich euklidische

Körper. J. reine angew. Math. 274/275 (1975), 196-205.

[49] Ribenboim, P.: Théorie des Valuations. 2^e edition. Les Presses de l'Université de Montréal, 1968.

[50] Ribes, L.: Introduction of profinite groups and galois cohomology. Queen's paper in pure and applied mathematics, No. 24. Queen's University, Kingston, Ontario 1970.

[51] Scharlau, W.: Über die Brauer-Gruppe eines Hensel-Körpers. Abh. Math. Sem. Univ. Hamburg 33 (1969), 243-249.

[52] Schinzel, A.: On linear dependence of roots. Acta arithmetica 28 (1975), 163-175.

[53] Ware, R.: When are Witt rings group rings. Pac. J. Math. 49 (1973), 279-284.

[54] Whaples, G.: Algebraic extensions of arbitrary fields. Duke Math. J. (1957), 201-204.