INTERSECTIONS OF LOCAL ALGEBRAIC EXTENSIONS OF A HILBERTIAN FIELD*

by

Moshe Jarden, Tel Aviv University

* Partially supported by a grant from the G.I.F., the German–Israeli Foundation for Scientific Research and Development., Tel Aviv University

Introduction

An algebraic extension E of a field K is **local** if it is Henselian with respect to a valuation v or it is real closed. We denote the absolute Galois group of K by $G(K)$. If $E_1, \dots, E_m$ are local separable algebraic extensions of K, then we can not say too much about the closed subgroup $\langle G(E_1), \dots, G(E_m)\rangle$ of $G(K)$ which generate by $G(E_1), \dots, G(E_m)$. However, if K is a countable Hilbertian field and we replace each $G(E_i)$ by a conjugate $G(E_i)^{\sigma_i}$ where σ_i is chosen at random, then the groups $G(E_i)^{\sigma_i}$ generating $G_\sigma = \langle G(E_1)^{\sigma_1}, \dots, G(E_m)^{\sigma_m}\rangle$ become free from one another in G_σ.

The following theorem, which is the main result of this work, makes this more precise and say a little more.

THE FREE PRODUCT THEOREM: *Let K be a countable Hilbertian field, $E_1, \dots, E_m$ local separable algebraic extension of K and e a nonnegative integer. Then for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau}) = (\sigma_1, \dots, \sigma_m, \tau_1, \dots, \tau_e) \in G(K)^{m+e}$,*

$$G_{\sigma,\tau} = \langle G(E_1)^{\sigma_1}, \dots, G(E_m)^{\sigma_m}, \tau_1, \dots, \tau_e\rangle$$

is the free product of $G(E_1)^{\sigma_1}, \dots, G(E_m)^{\sigma_m}, \langle \tau_1, \dots, \tau_e\rangle$ and $\langle \tau_1, \dots, \tau_e\rangle$ is the free profinite group on $\tau_1, \dots, \tau_e$.

This means that any map φ_0 of $\bigcup_{i=1}^m G(E_i)^{\sigma_i} \cup \{\tau_1, \dots, \tau_e\}$ into a profinite group A whose restriction to $G(E_i)^{\sigma_i}$ is a homomorphism uniquely extends to a homomorphism of $G_{\sigma,\tau}$ into A.

Here "almost all" is meant in the sense of the Haar measure of $G(K)^{e+m}$.

Ax [A1], proves the free product theorem in the case $K = \mathbb{Q}$, $m = 0$, and $e = 1$. His proof uses cyclic extensions of $\mathbb{Q}$ and therefore can not be generalized to $e > 1$. In [J1, Thm. 5.1], the author of this work replaces Ax's method by Hilbert irreducibility theorem and proves the theorem for $m = 0$, arbitrary e, and arbitrary K. In this case the theorem is called the "free generators theorem". It is one of the main ingredients for the study of the theory of all sentences which are true in $K_s(\tau_1, \dots, \tau_e)$ for almost all $(\tau_1, \dots, \tau_e) \in G(K)^e$ [JK]. Here $K_s(\tau_1, \dots, \tau_e)$ is the fixed field of $\langle \tau_1, \dots, \tau_e\rangle$ in the separable closure K_s of K. Since the free generators theorem is also one of the

ingredients of the proof of free product theorem, this work begins with a quick account of it (Section 0).

Geyer [G], answering a question of Neukirch, proves the free product theorem in the case $e = 0$ and where $E_1, \ldots, E_m$ are the decomposition fields, respectively, of absolute values $w_1, \ldots, w_m$ of K. Thus, each w_i is either a valuation of rank 1 or an archimedean ordering. He also proves the theorem in the case where $E_1, \ldots, E_m$ are real closures of K.

The latter case is one of the main ingredients in the study of the theory of all elementary statements on fields which are true in $E_1^{\sigma_1} \cap \cdots \cap E_m^{\sigma_m} \cap K_s(\boldsymbol{\tau})$ for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G(K)^{m+e}$ [J2].

Another case of the free product theorem is proved in [HJ] (for $K = Q$) and in [EJ] (for arbitrary K) in the case where $E_1, \ldots, E_m$ are p-adic closures of K. We use the theorem in [HJ] to realize every p-adically projective group as the absolute Galois group of a p-adically projective field. Efrat [E] uses the theorem of [EJ] to study the theory of all elementary statements which are true in the field $E_1^{\sigma_1} \cap \cdots \cap E_m^{\sigma_m} \cap K_s(\boldsymbol{\tau})$, for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G(K)^{m+e}$.

In his proof, Geyer considers for each i, a finite Galois extension F_i of E_i and a primitive element x_i for F_i/E_i. The degree $n_i = [F_i : E_i]$ divides the order n of a certain finite group A. The conjugates of x_i over E_i are, say, $x_{i1}, \ldots, x_{in_i}$. So, Geyer chooses integers $k_{i1}, \ldots, k_{i,n/n_i}$ such that the polynomial

$$f_i(X) = \prod_{s=1}^{n_i} \prod_{t=1}^{n/n_i} (X - x_{is} - k_{it})$$

has n distinct roots. Then, Geyer uses the density of K in E_i and the weak approximation theorem for absolute values to find a monic polynomial $g(X) \in K[X]$ of degree n which is w_i-close to $f_i(X)$ for $i = 1, \ldots, m$. By a consequence of Krasner's Lemma (resp., Sturm's algorithm, if w_i is an ordering) each root of $f(X)$ generates F_i over E_i.

If E_i is an arbitrary Henselian field which is separable algebraic over K, then it is an extension of the decomposition field of some valuation w_i of K. In this case K need not be w_i-dense in E_i. Also, the weak approximation theorem need not hold for $w_1, \ldots, w_m$, unless they are independent, an assumption which we do not make.

To circumvent these difficulties we replace $F_1, \ldots, F_m$ by $FE_1, \ldots, FE_m$ for an appropriate finite Galois extension F of K and we replace A by a finite group B with an epimorphism α: $B \to A$ such that $[F : K]$ divides $n = |B|$. Then we take x to be a primitive element of F/K with conjugates $x_1, \ldots, x_d$ and replace the polynomials $f_1, \ldots, f_m$ by a unique one

$$f(X) = \prod_{s=1}^{d} \prod_{t=1}^{n/d} (X - x_s - k_t),$$

with n distinct roots and where $k_1, \ldots, k_{n/d} \in K$. Since the coefficients of $f(X)$ belong to K, it is possible to approximate them simultaneously in the $w_1, \ldots, w_m$ – topologies without assuming that $w_1, \ldots, w_m$ are independent. The need of density theorems of K in E_i also disappears. Then we proceed as in Geyer's original proof.

Most of this work is dedicated to the introduction of that part of valuation theory which is needed in the proof of the free product theorem. The main target is Krasner's lemma over Henselian fields and simultaneous approximation of 0 in separable Hilbert sets. We take advantage of this opportunity and prove also theorems of F.K. Schmidt and Engler which follow from Krasner's lemma, and also the density theorem for Hilbert sets with respect to independent set of valuations and orderings.

The valuations we treat are of arbitrary rank and the orderings we encounter are not necessarily archimedean. We therefore explain and study the notion "finer than" between valuations of a field, and between a valuation and an ordering of a field. We use the properties of this notion which we develop to replace nonarchimedean orderings by valuations, and valuations by coarser ones in order to reduce theorems for sets of valuation and orderings to other sets of valuations which are easier to handle.

Much of our knowledge of valuation theory has come from Ribenboim's book [R]. Another source of inspiration was Prestel and Ziegler's paper [PZ]. We follow their technique of ultraproducts of valued and ordered fields to prove the theorems about the continuity of roots and the weak approximation theorem.

0. The free generators theorem.

A **profinite group** is an inverse limit of finite groups: $G = \varprojlim G_i$. It is a compact, Hausdorff, totally disconnected topological group [FJ, Section 1.2]. Whenever we speak about a homomorphism between profinite groups we mean continuous homomorphism. Also, we use the close "the group generated by a subset S of G" to mean "the smallest closed subgroup of G that contains S". We denote this subgroup by $\langle S\rangle$. In particular we say that G is **finitely generated** if there exist $x_1,\dots,x_e$ in G such that $G = \langle x_1,\dots,x_e\rangle$. Such groups are determined by their finite quotients. That is, if G' is another profinite group and a finite group A is a quotient of G if and only if it is a quotient of G', then $G \cong G'$ [FJ, Prop. 15.4].

A profinite group $\widehat{F}_e$ is **free** on $x_1,\dots,x_e$ if $\widehat{F}_e = \langle x_1,\dots,x_e\rangle$ and each map φ of $\{x_1,\dots,x_e\}$ into a profinite group G extends (necessarily uniquely) to a homomorphism $\varphi\colon \widehat{F}_e \to G$. We call $\{x_1,\dots,x_e\}$ a **basis** for $\widehat{F}_e$. Such a group also emerges from the free discrete group F_e with the free generators $x_1,\dots,x_e$ as $\widehat{F}_e = \varprojlim F_e/N$, where N ranges over all open normal subgroups of F_e [FJ, Section 5.5]. It follows from the preceding paragraph that a profinite group G is isomorphic to $\widehat{F}_e$ if and only if it is generated by e elements and every finite group which is generated by e elements is a quotient of G. For $e = 1$ we get $\hat{\mathbb{Z}} = \widehat{F}_1 = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Every profinite group G admits a unique Haar measure μ [FJ, Prop. 16.5]. It is invariant under translations: $\mu(xA) = \mu(Ax) = \mu(A)$ for each measurable set A, and $\mu(G) = 1$. The family of measurable sets of G is the smallest σ-additive collection $\mathcal{A}$ of subsets of G which contains all Borel sets and which is **complete**. This means that if $A \in \mathcal{A}$ has measure 0, then each subset of A belongs to $\mathcal{A}$.

In particular each coset xH of an open subgroup H is measurable and $\mu(xH) = \mu(H)$. Thus, if $G = \bigcup_{i=1}^{n} x_iH$, then $1 = \mu(G) = \sum_{i=1}^{n} \mu(x_iH) = n\mu(H)$ and therefore $\mu(H) = 1/n$.

The condition, $\mu(G) = 1$, makes G a probability space. So we may use the term **independent sets** for measurable sets $A_1,\dots,A_m$ to mean that $\mu(\bigcap_{i=1}^{m} A_i) = \prod_{i=1}^{m} \mu(A_i)$. An infinite sequence $A_1, A_2, A_3, \dots$, of measurable sets is **independent** if each finite subsequence is independent.

LEMMA 0.1: *Let $A_1, A_2, A_3, \ldots$ be an independent sequence of measurable subsets of a probability space X. If $\sum_{n=1}^{\infty} \mu(A_n) = \infty$, then $\mu(\bigcup_{n=1}^{\infty} A_n) = 1$.*

Proof: The sequence of complements $X - A_1$, $X - A_2$, $X - A_3, \ldots$ is also independent. Hence

$$\mu(X - \bigcup_{n=1}^{\infty} A_n) = \mu(\bigcap_{n=1}^{\infty} X - A_n) = \prod_{n=1}^{\infty} (1 - \mu(A_n)) = 0.$$

Conclude that $\mu(\bigcup_{n=1}^{\infty} = 1$. ∎

We consider, together with each profinite group G, also the direct product G^e of e copies of G. It is a profinite group, and its Haar measure coincides with the product measure of e copies of the Haar measure of G [FJ, Prop. 16.10].

An important example of a profinite group is the **absolute Galois group** $G(K)$ of a field K. It is the Galois group $\mathcal{G}(K_s/K)$ of the separable closure K_s of K over K. The Galois correspondence between closed subgroups of $G(K)$ and separable algebraic extensions of K translates "independence of closed subgroups" into "linear disjointness of separable algebraic extensions of K".

Recall that field extensions $F_1, \ldots, F_n$ of K are **linearly disjoint** if the canonical homomorphism $F_1 \otimes_K \cdots \otimes_K F_n \to F_1 \cdots F_n$ defined by $x_1 \otimes \cdots \otimes x_n \to x_1 \cdots x_n$ is injective. In particular, if $F_1, \ldots, F_n$ are finite over K, then they are linearly disjoint if and only if $[F_1, \ldots F_n : K] = [F_1 : K] \cdots [F_n : K]$. A sequence $F_1, F_2, F_3, \ldots$ of extensions of K is **linearly disjoint**, if and only if each finite subsequence is linearly disjoint. This is the case, if and only if each F_{n+1} is linearly disjoint from $F_1 \cdots F_n$ over K [FJ, Section 9.1].

LEMMA 0.2: *Let $L_1, L_2, L_3, \ldots$ be a sequence of finite separable extensions of a field K.*

(a) *$L_1, L_2, L_3, \ldots$ are linearly disjoint if and only if $G(L_1), G(L_2), G(L_3), \ldots$ are independent.*

(b) *Suppose that L_n/K is Galois. Let $\overline{C}_n$ be a nonempty subset of $\mathcal{G}(L_n/L)^e$ and let $C_n = \{\boldsymbol{\sigma} \in G(K)^e | \ \mathrm{res}_{L_n} \boldsymbol{\sigma} \in \overline{C}_n\}$, $n = 1, 2, 3, \ldots$. If $L_1, L_2, L_e, \ldots$ are linearly disjoint over K, then $C_1, C_2, C_e, \ldots$ are independent. Moreover, if $\sum_{n=1}^{\infty} 1/[L_n : K]^e = \infty$, then $\mu(\bigcup_{n=1}^{\infty} C_n) = 1$.*

Proof of (a): Suppose that $L_1, L_2, L_3, \dots$ are linearly disjoint. Then

$$\mu(\bigcup_{i=1}^{n} G(L_i)) = \mu(G(L_1 \cdots L_n)) = 1/[L_1 \cdots L_n : K] = \prod_{i=1}^{n} 1/[L_i : K] = \prod_{i=1}^{n} \mu(G(L_i)).$$

Hence $G(L_1), G(L_2), G(L_3), \dots$ are independent. Now revers the proof to prove that the later condition implies that $L_1, L_2, L_3, \dots$ are linearly disjoint.

Proof of (b): Now suppose that $L_1, L_2, L_3, \dots$ are as in (b). Then, for $L = L_1 \cdots L_n$, we have $\mathcal{G}(L/K) = \prod_{i=1}^{n} \mathcal{G}(L_i/K)$. Hence

$$C_L = \{\boldsymbol{\sigma} \in \mathcal{G}(L/K)^e | \ \mathrm{res}_{L_i} \boldsymbol{\sigma} \in \overline{C}_i, \ i = 1, \dots, n\}$$

has the same number of elements as $\prod_{i=1}^{n} \overline{C}_i$. Also, $\bigcap_{i=1}^{n} C_i = \{\boldsymbol{\sigma} \in G(K)^e | \ \mathrm{res}_L \boldsymbol{\sigma} \in C_L\}$. Consequently,

$$\mu(\prod_{i=1}^{n} C_i) = |C_L|/[L : K]^e = \prod_{i=1}^{n} |\overline{C}_i|/[L_i : K]^e = \prod_{i=1}^{n} \mu(\overline{C}_i).$$

Hence, $C_1, C_2, C_3, \dots$ are independent.

If $\sum_{n=1}^{\infty} 1/[L_n : K]^e = \infty$, then $\sum_{n=1}^{\infty} \mu(C_n) = \sum_{n=1}^{\infty} |\overline{C}_n|/[L_n : K]^e = \infty$. Conclude from Lemma 0.1 that $\mu(\bigcup_{n=1}^{\infty} C_n) = 1$. ∎

The most convenient tool to generate linearly disjoint sequences over $\mathbb{Q}$ is Hilbert irreducibility theorem. As this theorem holds over many more fields, it makes sense to handle the consequences of this theorem axiomatically. This leads to the definition of "Hilbertian fields".

Consider irreducible polynomials $f_1, \dots, f_m \in K(T_1, \dots, T_r)[X]$ (resp., which are separable in X) and a nonzero polynomial $g \in K[T_1, \dots, T_r]$. The set

$$H_K(f_1, \dots, f_m; g) = \{\mathbf{a} \in K^r | \ f_i(\mathbf{a}, X) \text{ is defined and irreducible in } K[X], \ i = 1, \dots, m \text{ and } g(\mathbf{a} \neq 0\}$$

is called a **Hilbert subset** of K^r (resp., **separable Hilbert subset** of K^r). A field K is said to be **Hilbertian** (resp., **separably Hilbertian**) if all of its Hilbert (resp., separable Hilbert) sets are nonempty (indeed, they are infinite).

By definition, every Hilbertian field is separably Hilbertian. Conversely, a separably Hilbertian field K of positive characteristic is Hilbertian if and only if it is imperfect [FJ, Prop. 11.17].

As we are mainly concerned with separable extensions, we work over separably Hilbertian fields. Basic examples of separably Hilbertian fields are: $\mathbb{Q}$ [FJ, Cor. 12.8], the field $K_o(t)$ of rational functions [FJ, Cor. 12.8 and Thm. 12.10], and the field of power series $K_0((t_1,\dots,t_r))$ in $r \geq 2$ variables over any field K_0. Other separably Hilbertian fields are obtained from the basic ones as appropriate separable algebraic extensions. First of all, each finite separable extension L of a separably Hilbertian field is separably Hilbertian. This follows from [FJ, Cor. 11.7]. The proof of that corollary, applied to separable polynomials yields the following version of the corollary:

LEMMA 0.3: *Let L be a finite separable extension of a field K. Then every separable Hilbert subset of L^r contains a separable Hilbert subset of K^r. In particular, if K is separably Hilbertian, then so is L.*

Several types of infinite separable extensions of a separably Hilbertian field are separably Hilbertian. So is any abelian extension (a theorem of Kuyk [FJ, Thm. 15.6]) and any finite proper extension M of a Galois extension N (A theorem of Weissauer [FJ, Cor. 12.15]).

LEMMA 0.4: *Let K be a separably Hilbertian field and let n be a positive integer. Then K has a linearly disjoint sequence $L_1, L_2, L_3, \dots$ of Galois extensions such that for each i the Galois group $\mathcal{G}(L_i/K)$ is isomorphic to the symmetric group S_n.*

Proof: Suppose by induction that K has a linearly disjoint sequence $L_1,\dots,L_m$ of Galois extensions with Galois group isomorphic to S_n. Then $L = L_1\cdots L_m$ is a finite separable extension of K. The Galois groups of the general polynomial of degree n,

$$f(T_1,\dots,T_n,X) = X^n + T_1X^{n-1} + \cdots + T_n,$$

over $L(\mathbf{T})$ and over $K(\mathbf{T})$ are isomorphic to S_n. By a theorem of Hilbert [FJ, Lemma 12.12], the set of all $\mathbf{a} \in L^r$ (resp. $\mathbf{a} \in K^r$) such that $\mathcal{G}(f(\mathbf{a},X),L) \cong S_n$ (resp., $\mathcal{G}(f(\mathbf{a},X),K) \cong S_n$) contains a separable Hilbert subset H_L (resp., H_K) of L^r (resp.,

K^r). By Lemma 0.3, $H_L \cap H_K$ contains a separable Hilbert subset H of K^r. Choose $\mathbf{a} \in H$ and let L_{m+1} be the splitting field of $f(\mathbf{a}, X)$ over K. Then $\mathcal{G}(L_{m+1}/K) \cong \mathcal{G}(LL_{m+1}/L) \cong S_n$. Hence, L_{m+1} is linearly disjoint from L over K. It follows that $L_1, \ldots, L_m, L_{m+1}$ are linearly disjoint over K. This concludes the induction. ∎

PROPOSITION 0.5 (Free generators theorem): *Let K be a separably Hilbertian field, and let e be a positive integer. Then, for almost all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$ we have $\langle \sigma_1, \ldots, \sigma_e \rangle \cong \widehat{F}_e$.*

Proof: Since there are only countably many finite groups and since the intersection of countably many sets of measure 1 is again a set of measure 1, it suffices to prove that for each finite group A which is generated by e elements the set of all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$ for which A is a quotient of $\langle \sigma_1, \ldots, \sigma_e \rangle$ has measure 1.

Indeed, with $n = |A|$, embed A in S_n. Let $L_1, L_2, L_3, \cdots$ be a linearly disjoint sequence of Galois extensions with Galois group isomorphic to S_n (Lemma 0.4). For each k choose $\sigma_{k1}, \ldots, \sigma_{ke} \in \mathcal{G}(L_k/K)$ such that $\langle \sigma_{k1}, \ldots, \sigma_{ke} \rangle \cong A$. Since $\sum_{k=1}^{\infty} 1/[L_k : K] = \infty$, we may apply Lemma 0.2 to conclude that for almost all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$ there exists k such that $\mathrm{res}_{L_k} \sigma_i = \sigma_{ki}$, $i = 1, \ldots, e$. Thus, $\langle \sigma_{k1}, \ldots, \sigma_{ke} \rangle \cong A$ is a quotient of $\langle \sigma_1, \ldots, \sigma_e \rangle$, as contended. ∎

1. Ordered abelian groups.

An **ordered group** is an abelian (additive) group Γ together with a total ordering $<$ such that $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$ for all $\alpha, \beta, \gamma \in \Gamma$.

In particular, for each positive integer n, the map $\gamma \mapsto n\gamma$ is a monomorphism of Γ into itself.

We introduce an **absolute value** to Γ in the usual way: $|\gamma| = \gamma$ if $\gamma \geq 0$ and $|\gamma| = -\gamma$ if $\gamma \leq 0$.

Examples for ordered groups are the group of integers $\mathbb{Z}$, the group of reals $\mathbb{R}$, and $\mathbb{R} \oplus \mathbb{R}$ with the lexicorgraphic ordering.

An ordered group Γ is **archimedean** if for each $\alpha, \beta > 0$ there exists n such that $n\alpha > \beta$.

LEMMA 1.1: *An ordered group* Γ *is archimedean if and only if it can be embedded (as an ordered group) in* $\mathbb{R}$.

Proof of 1.1: As the condition is obviously necessary we have only to prove that it is also sufficient.

Suppose therefore that Γ is a nontrivial archimedean group. Choose $\alpha > 0$ in Γ and define a map $f\colon \Gamma \to \mathbb{R}$ as follows: For each positive $\beta \in \Gamma$ consider the set $S_\beta = \{m/n |\ m, n \in \mathbb{Z},\ n > 0,\ m\alpha \leq n\beta\}$. Then S_β is nonempty and bounded. Indeed, if $\beta < k\alpha$, then k bounds S_β.

Note that if $m/n \in S_\beta$ and $m'/n' \leq m/n$, then $m'n\alpha \leq mn'\alpha \leq nn'\beta$. Hence $m'\alpha \leq n'\beta$ and therefore m'/n' also belongs to S_β. Define $f(\beta)$ to be the supremum of S_β. For $\beta < 0$ define $f(\beta) = f(-\beta)$.

If $0 < \beta < \gamma$, take $n > 0$ such that $\alpha < n(\gamma - \beta)$. Let m be the minimal integer such that $n\beta < m\alpha$. Then $(m-1)\alpha \leq n\beta$. Hence, $m\alpha \leq n\gamma$, beceause otherwise $n(\gamma - \beta) < m\alpha - (m-1)\alpha = \alpha$, a contradiction. It follows that m/n belongs to S_γ but not to S_β. Hence $f(\beta) < f(\gamma)$.

Finally, observe that $f(\beta + \gamma) = f(\beta) + f(\gamma)$. So, f is an ordered embedding of γ in $\mathbb{R}$. ∎

A subgroup Δ of an ordered group Γ is **convex** if $\delta \in \Delta$ and $\gamma < \delta$ imply $\gamma \in \Delta$. In this case, if $\gamma > 0$ and $\gamma \notin \Delta$, then $\gamma + \delta > 0$ for each $\delta \in \Delta$. Hence, we may define an ordering on the quotient group Γ/Δ by

$$\gamma_1 + \Delta < \gamma_2 + \Delta \text{ if } \gamma_1 < \gamma_2.$$

The canonical map $\Gamma \mapsto \Gamma/\Delta$ is then a homomorphism of ordered groups.

2. Valuations.

Consider a field K and let $K^\times$ be the multiplicative group of nonzero elements of K. A valuation of K is a map v of $K^\times$ onto an ordered group Γ (called the **value group** of v such that

(1a) $v(ab) = v(a) + v(b)$,

(1b) $v(a+b) \geq \min\{v(a), v(b)\}$, and

(1c) v is nontrivial, i.e., there exists $a \in K^\times$ such that $v(a) \neq 0$.

Add the symbol ∞ to Γ with the following convention:

(2a) $\infty + \infty = \alpha + \infty = \infty + \alpha = \infty$, and

(2b) $\alpha < \infty$ for each $\alpha \in \Gamma$.

Extend v to K by defining $v(0) = \infty$ and observe that v still satisfies (1). We call the pair (K, v) a **valued field**.

Next deduce the following properties of v from (1)

(3a) $v(1) = 0$ and $v(a) = v(-a)$ for each $a \in K$.

(3b) If $v(a) < v(b)$, then $v(a+b) = v(a)$.

Otherwise $v(a+b) > v(a)$ and therefore $v(a) \geq \min\{v(a+b), v(-b)\} > v(a)$, a contradiction.

(3c) $v(\sum_{i=1}^m a_i) \geq \min_{1 \leq i \leq m}\{v(a_i)\}$. If $v(a_i) \neq v(a_j)$ for all $i \neq j$, then we have an equality.

(3d) If $\sum_{i=1}^m a_i = 0$ and $m > 1$, then there exist $i \neq j$ such that $v(a_i) = v(a_j)$.

The **valuation ring** of v is $O_v = \{x \in K |\ v(x) \geq 0\}$. It has a unique maximal ideal $M_v = \{x \in K |\ v(x) > 0\}$. The quotient $\overline{K}_v = O_v/M_v$ is the **residue field** of v. It gives a short exact sequence:

$$0 \longrightarrow M_v \longrightarrow O_v \longrightarrow \overline{K}_v \longrightarrow 0.$$

The group of units of O_v is $U_v = \{x \in K |\ v(x) = 0\}$. It gives another short exact sequence:

$$1 \longrightarrow U_v \longrightarrow K^\times \xrightarrow{v} \Gamma_v \longrightarrow 0.$$

The quotient field of O_v is K and for each $x \in K^\times$ we have $x \in O_v$ or $x^{-1} \in O_v$.

EXAMPLE 2.1: *The p-adic valuation.* Let R be a unique factorization domain with a quotient field K. For each prime element p of R we define a valuation v_p of K in the following way: Write each $x \in K$ in the form $x = \frac{a}{b}p^m$ where a and b are relatively prime to p and $m \in \mathbb{Z}$. Then let $v_p(x) = m$. Its value group is $\mathbb{Z}$ and $v(p) = 1$ is the smallest positive element in it.

The first example for a unique factorization domain is $\mathbb{Z}$. Other example of interest are the ring of polynomials in several variables $K_0[X_1, \ldots, X_n]$, and the ring of formal power series $K_0[[X_1, \ldots, X_n]]$ over a field K_0.

In the case where $O = K_0[X]$, there is an additional valuation which is usually denoted by v_∞ and is defined by $v_\infty(f/g) = \deg(g) - \deg(f)$ for $f, g \in O$. ∎

Two valuations v_1 and v_2 of a field K with valuation groups Γ_1 and Γ_2, respectively, are said to be equivalent if there exists an ordered preserving isomorphism $f\colon \Gamma_1 \to \Gamma_2$ such that $f \circ v_1 = v_2$. In particular $v_1(a) > 0$ if and only if $v_2(a) > 0$. Obviously, the later condition is also sufficient for v_1 and v_2 to be equivalent. Note also that v_1 and v_2 are equivalent if and only if they have the same valuation ring. In particular, if p and q are prime elements of a unique factorization domain R and q is not the product of p with a unit, then v_p and v_q are nonequivalent.

If v is a valuation of $\mathbb{Q}$, then $\mathbb{Z} \subseteq O_v$ and $P_v \cap \mathbb{Z}$ is generated by some prime p. So, $O_v = O_{v_p}$ and therefore v is equivalent to v_p. Thus v_p, where p ranges over all rational primes exhaust all equivalent classes of valuations of $\mathbb{Q}$.

In the case $K = K_0(X)$ the valuation v_∞ is equivalent to none of the valuations v_p, where p is a primes element of $R = K_0[X]$. Again it is a simple exercise to show that these valuations exhaust all equivalent classes of valuations v of K which are **trivial** of K_0, (i.e., v satisfies $v(a) = 0$ for each $a \in K_0$).

A **local ring** is a ring R with a unique maximal ideal M. The elements of $R - M$ are then the units of R. For example, if P is a prime ideal of an arbitrary integral domain R, then

$$R_P = \left\{ \frac{a}{b} \middle| \, a, b \in R \text{ and } b \notin P \right\}$$

is a local ring whose maximal ideal is PR_P. It is the **local ring of** R **at** P.

A special kind of a local ring is a **valuation ring** of a field K. It is a proper subring O of K such that if $x \in K^\times$, then $x \in O$ or $x^{-1} \in O$.

In particular $1 \in O$ and K is the quotient field of O. Let M denote the set of all nonunits of O. Then M is a unique maximal ideal of O. Indeed, if $a \in M$ and $r \in O$, then ra is a nonunit of O and therefore belongs to M. Secondly, if $a, b \in M$ are nonzero, then we may assume that $ab^{-1} \in O$. Hence $a + b = b(1 + ab^{-1}) \in M$. Finally, an element $u \in O - M$ is a unit of O. Hence together with M it generates O. So, M is the unique maximal ideal of O. Hence, O is a local ring.

Denote the group of units of O by U. Define an abelian additive group Γ by associating an element a' with each element aU of the multiplicative group $K^\times/U$. Addition in Γ is defined by the law: $a' + b' = c'$ if and only if $abU = cU$. Define an ordering on Γ by: $a' < b'$ if and only if $ba^{-1} \in O$. Then Γ is an ordered group. The map v: $K \to \Gamma$ defined by $v(a) = a'$ and $v(0) = \infty$ is a valuation of K whose value group is Γ and whose valuation ring is O.

Note that if O' is a proper subring of K which contains a valuation ring O, then O' itself is a valuation ring, as follows immediately from the definition.

3. Comparable valuations.

Each valuation v of a field K induces a field topology on K which we call the v-**topology**. A basis for the neighborhoods of a point $a \in K$ consists of the sets $\{x \in K |\ v(x-a) > \alpha\}$, where α ranges over Γ_v. The field operations are continuous in this topology.

Another valuation w of K is **coarser** than v (and v is **finer** than w) if $O_v \subseteq O_w$. This is exactly the case when $M_w \subseteq M_v$. So, for all $x, y \in K$,

(1) $$w(x) < w(y) \text{ implies } v(x) < v(y).$$

In this case M_w is a nonzero prime ideal of O_v. Also,

(2) for each $b \in M_w$ and all $a, x \in K$ we have: $v(x) > v(ab)$ implies $w(x) > w(a)$.

Otherwise, $w(x) \leq w(a)$, hence $w(x) < w(ab)$, and therefore $v(x) < v(ab)$, a contradiction.

Also, $O_{\bar{v}} = O_v/M_w$ is a valuation ring of $\overline{K}_w = O_w/M_w$ with the maximal ideal $M_{\bar{v}} = M_v/M_w$. The corresponding valuation $\bar{v}$ is defined by $\bar{v}(\bar{x}) = v(x)$, for $x \in U_w$

(the bar denotes reduction modulo M_w). Note that if $x, y \in U_w$ and $\bar{x} = \bar{y}$, then $\frac{x}{y} - 1 \in M_w \subseteq M_v$. Thus $x = y + ay$ for some $a \in M_v$ and therefore $v(x) = v(y)$. It follows that $\bar{v}$ is well defined. It is now easy to verify that $\bar{v}$ is indeed a valuation of $\overline{K}_w$. In particular the residue fields of $\bar{v}$ and v coincide. Also, $\Gamma_{\bar{v}} \cong \overline{K}_w^\times / U_{\bar{v}} \cong U_w / U_v$ is a convex subgroup of $\Gamma_v \cong K^\times / U_v$. Thus

$$\overline{K}_v \cong O_{\bar{v}}/M_{\bar{v}} \cong O_v/M_v \qquad \text{and} \qquad \Gamma_w \cong \Gamma_v/\Gamma_{\bar{v}}. \tag{3}$$

The following two diagrams give a convenient way to memorize the relations between the objects we have considered:

$$\begin{array}{ccccc}
K & & & & \\
| & & & & \\
O_w & \longrightarrow & \overline{K}_w & & \\
| & & | & & \\
O_v & \longrightarrow & O_{\bar{v}} & \longrightarrow & \overline{K}_v \\
| & & | & & | \\
M_v & \longrightarrow & M_{\bar{v}} & \longrightarrow & 0 \\
| & & | & & \\
M_w & \longrightarrow & 0 & &
\end{array}
\qquad\qquad
\begin{array}{ccc}
K^\times & & \\
| & & \\
U_w & \longrightarrow & \overline{K}_w^\times \\
| & & | \\
U_v & \longrightarrow & U_{\bar{v}}
\end{array}$$

LEMMA 3.1: *In the setup discussed above, reduction modulo M_w establishes an order preserving bijective correspondence between the valuation rings of K which are properly contained in O_w and contain O_v and the valuation rings of $\overline{K}_w$ that contain $O_{\bar{v}}$.*

Proof: It suffices to prove that the map is onto. Indeed, let O be a valuation ring of $\overline{K}_w$ which contains $O_{\bar{v}}$. Then $A = \{x \in O_w |\ \bar{x} \in O\}$ is a subring of K which lies between O_v and O_w. In particular, since A contains O_v, it is a valuation ring. As $O \neq \overline{K}$, we have $A \neq O_w$. ∎

LEMMA 3.2: *Let v and w be valuations of a field K such that w is coarser than v.*

(a) *The v-topology of K coincides with the w-topology.*

(b) *If w' is another valuation of K which is coarser than v, then w is coarser than w' or w' is coarser than w.*

Proof of (a): Statements (1) and (2) imply that each v-neighborhood of 0 contains a w-neighborhood and conversely. So, the two topologies coincide.

Proof of (b): Note that both M_w and $M_{w'}$ are prime ideals of O_v contained in M_v. If $M_w \not\subseteq M_{w'}$, then there exists $a \in M_w$ such that $a \notin M_{w'}$. Hence $M_{w'} = aM_{w'} \subseteq aM_v \subseteq M_w$. It follows that $O_w \subseteq O_{w'}$, which means that w' is coarser than w. ∎

In particular, if K have only finitely many valuations which are coarser than v, then we may enumerate them as $w_1, \ldots, w_{n-1}$ such that $O_v \subseteq O_{w_1} \subseteq \cdots \subseteq O_{w_{n-1}}$. If no two of these valuations are equivalent, we say that the **rank** of v is n. Thus $\mathrm{rank}(v) = 1$ if K has no valuation which is coarser than v. Also, in the setup of (3), Lemma 3.1 implies that $\mathrm{rank}(v) = \mathrm{rank}(\bar{v}) + 1$.

LEMMA 3.3: *Let v be a valuation of a field K. Then the correspondence $O_w \mapsto M_w$ of valuation rings of valuations w which are coarser than v onto nonzero prime ideals of O_v is a bijective map which is order reversing.*

Proof: In view of Lemma 3.2(b) we have only to prove that the above map is surjective.

Indeed, let P be a nonzero prime ideal of O_v. Consider the local ring of O_v at P:

$$O' = \{a/b |\ a, b \in O_v,\ b \notin P\}.$$

As O' contains O_v it is a valuation ring. Hence, by Section 2, there exists a valuation w of v such that $O_w = O'$. We prove that $M_w = P$. Indeed, if $x \in P$, then $x^{-1} \notin O'$. Otherwise $x^{-1} = a/b$ with $a, b \in O_v$ and $b \notin P$. Then $b = xa \in P$, a contradiction. It follows that $x \in M_w$. Conversely, if $x \in M_w$, then $1/x \notin O'$, hence $x \in P$. ∎

LEMMA 3.4: *A valuation v of a field K is of rank 1 if and only if Γ_v is archimedean.*

Proof: Suppose first that $\mathrm{rank}(v) > 1$. Then K has a valuation w which is coarser than v. Hence, in the above notation, $\Gamma_{\bar{v}}$ is a convex proper subgroup of Γ_v. So, if $0 < \beta \in \Gamma_{\bar{v}}$ and $0 < \gamma \in \Gamma_v - \Gamma_{\bar{v}}$, then $n\beta \in \Gamma_{\bar{v}}$ and therefore $n\beta < \gamma$ for each positive integer n. Conclude that Γ_v is not archimedean.

Conversely, if Γ_v is nonarchimedean, then there exist $\beta, \gamma \in \Gamma_v$ such that $n\beta < \gamma$ for each positive integer n. Observe that $\Delta = \{\alpha \in \Gamma_v |\ \exists n : |\alpha| < n\beta\}$ is a proper

convex subgroup of Γ_v. Hence, Γ_v/Δ is an ordered group. Let $\theta\colon \Gamma_v \to \Gamma_v/\Delta$ be the canonical map. Then $w = \theta \circ v$ is a valuation of K which is coarser than v. ∎

4. The weak approximation theorem.

Two valuations v and v' of a field K are **comparable** if one of them is finer than the other. They are **dependent** if they are finer than a common valuation w. By Lemma 3.2(a) they induce the same topology on K. The following lemma proves the converse.

LEMMA 4.1: *Let v and v' be valuations of a field K. Then v and v' are independent if and only if for each $\alpha' \in \Gamma_{v'}$ there exists $x \in K$ such that $v(x) < 0$ and $v'(x) \geq \alpha'$. In particular, if v and v' are independnet, then the v-topology on K is different from the v'-topology.*

Proof: Suppose first that v and v' are independent. Then $O_{v'} \not\subseteq O_v$. Hence there exists $b \in K$ such that

$$v'(b) \geq 0 \quad \text{and} \quad v(b) < 0. \tag{1}$$

Assume that there exists $a' \in K^\times$ such that with $\alpha' = v'(a')$ we have

$$v(x) < 0 \quad \text{implies} \quad v'(x) < \alpha'. \tag{2}$$

Suppose without loss that $\alpha' > 0$. Then

$$P' = \{x \in O_{v'} \mid \exists n \in \mathbb{N} : nv'(x) \geq \alpha'\}$$

is an ideal of $O_{v'}$. Moreover, P' is a prime ideal. Indeed if $x, y \in O_{v'}$ and $xy \in P'$, then there exists a positive integer n such that $n(v'(x) + v'(y)) = nv'(xy) \geq \alpha'$. Hence $2nv'(x) \geq \alpha'$ or $2nv'(y) \geq \alpha'$. This means that $x \in P'$ or $y \in P'$. As $a' \in P'$, this ideal is not the zero ideal.

We claim that $P' \subseteq O_v$. Indeed, if $x \in P'$, then there exists $n \in \mathbb{N}$ such that $v'(x^n) \geq \alpha'$. Hence, by (2), $nv(x) \geq 0$. Conclude that $v(x) \geq 0$ and therefore $x \in O_v$, as claimed.

Let w be the valuation of K which is coarser than v' such that $M_w = P'$ (Lemma 3.3). Then $O_{v'} \subseteq O_w$. We obtain a contradiction to the assumption that v and v' are independent by proving that $O_v \subseteq O_w$.

If this were not the case there would exist $x \in O_v$ such that $x \notin O_w$. Hence $x^{-1} \in P' \subseteq O_v$ and therefore $v(x) = 0$. Let n be a positive integer such that $v'(x^{-n}) \geq \alpha'$. By (1), $v(bx^{-n}) < 0$. Hence, by (2), $v'(b) + \alpha' \leq v'(b) + v'(x^{-n}) = v'(bx^{-n}) < \alpha'$. Therefore $v'(b) < 0$. This contradiction to (1) completes the proof of the lemma.

Now suppose that v and v' are dependent. Then they are finer than a common valuation w. Choose $b \in K^\times$ such that $w(b) > 0$. Then, for each $x \in K$ we have, by (2) of Section 3, $v'(x) > v'(b)$ implies $w(x) > w(1) = 0$ and therefore $v(x) > 0$. So the above condition is not satisfied. ∎

LEMMA 4.2: *Let $v_1, \ldots, v_m$, with $m \geq 2$, be valuations of a field K. Let $\alpha_i \in \Gamma_{v_i}$, $i = 2, \ldots, m$. Suppose that for each i between 2 and m there exists $a \in K$ such that $v_1(a) \leq \alpha_1$ and $v_i(a) \geq \alpha_i$. Then there exists $x \in K$ such that $v_1(x) \leq \alpha_1$ and $v_i(x) \geq \alpha_i$, $i = 2, \ldots, m$.*

Proof: Suppose without loss that $\alpha_1 < 0$ and $\alpha_i > 0$ for $i = 2, \ldots, m$. The Lemma is true for $m = 2$. So, let $m > 2$ and suppose that the lemma is true for $m - 1$. Then there exist $a, b \in K$ such that

$$\begin{array}{lllll} v_1(a) \leq \alpha_1 & v_2(a) \geq \alpha_2 & v_3(a) \geq \alpha_e & \cdots & v_{m-1}(a) \geq \alpha_{m-1} \\ v_1(b) \leq \alpha_1 & & v_3(b) \geq \alpha_3 & \cdots & v_{m-1}(b) \geq \alpha_{m-1} \quad v_m(b) \geq \alpha_m \end{array}$$

Suppose for example that $v_1(b) \leq v_1(a)$. Then replace b by b^2, if necessary, to assume that $v_1(b) < v_1(a)$. There are four cases to consider:

CASE A: *$v_m(a) \geq 0$ and $v_2(b) \geq 0$.* Take $x = ab$. Then

$$\begin{aligned} v_1(x) &= v_1(a) + v_1(b) \leq 2\alpha_1 < \alpha_1 \\ v_2(x) &= v_2(a) + v_2(b) \geq \alpha_2 \\ v_i(x) &= v_i(a) + v_i(b) \geq 2\alpha_i > \alpha_i, \quad i = 3, \ldots, m-1 \\ v_m(x) &= v_m(a) + v_m(b) \geq \alpha_m \end{aligned}$$

CASE B: $v_m(a) \geq 0$ *and* $v_2(b) < 0$. Take $x = \frac{ab}{1+b}$. Then

$$v_1(x) = v_1(a) + v_1(b) - v_1(1+b) \leq \alpha_1 + v_1(b) - v_1(b) = \alpha_1$$

$$v_2(x) = v_2(a) + v_2(b) - v_2(1+b) \geq \alpha_2 + v_2(b) - v_2(b) = \alpha_2$$

$$v_i(x) = v_i(a) + v_i(b) - v_i(1+b) \geq \alpha_i + \alpha_i > \alpha_i \quad i = 3, \ldots, m-1$$

$$v_m(x) = v_m(a) + v_m(b) - v_m(1+b) \geq \alpha_m$$

CASE C: $v_m(a) < 0$ *and* $v_2(b) \geq 0$. Take $x = \frac{ab}{1+a}$ and replace the roles of a and b in Case B.

CASE D: $v_m(a) < 0$ *and* $v_2(b) < 0$. Take $x = \frac{ab}{1+a+b}$. Then

$$v_1(x) = v_1(a) + v_1(b) - v_1(1+a+b) \leq \alpha_1 + v_1(b) - v_1(b) = \alpha_1$$

$$v_2(x) = v_2(a) + v_2(b) - v_2(1+a+b) \geq \alpha_2 + v_2(b) - v_2(b) = \alpha_2$$

$$v_i(x) = v_i(a) + v_i(b) - v_i(1+a+b) \geq \alpha_i + \alpha_i > \alpha_i, \quad i = 3, \ldots, m-1$$

$$v_m(x) = v_m(a) + v_m(b) - v_m(1+a+b) \geq v_m(a) + \alpha_m - v_m(a) = \alpha_m$$

Thus, in each case there is $x \in K$ which satisfies the requirements. ∎

We apply Lemma 4.2 in two cases:

(3a) $v_1, \ldots, v_m$ are **independent**, i.e., each pair of them is independent and $\alpha_1, \ldots, \alpha_m$ are arbitrary, and

(3b) $v_1, \ldots, v_m$ are **incomparable**, i.e., for each $i \neq j$, v_i is neither finer nor coarser than v_j, $i = 1, \ldots, m$.

LEMMA 4.3: *Let $v_1, \ldots, v_m$ be independent valuations of a field K. Let $\alpha_i \in \Gamma_{v_i}$, $i = 1, \ldots, m$. Then there exists $x \in K$ such that $v_1(x) \leq \alpha_1$ and $v_i(x) \geq \alpha_i$, $i = 2, \ldots, m$.*

Proof: Obviously, we may assume that $\alpha_1 < 0$ and $\alpha_i > 0$ for $i = 2, \ldots, m$. By Lemma 4.2 it suffices to consider the case $m = 2$. Let a be an element of K such that $v_1(a) = \alpha_1$. By Lemma 4.1, there exists $y \in K$ such that $v_1(y) < 0$ and $v_2(y) \geq \alpha_2 - v_2(a)$. Then $x = ay$ satisfies $v_1(x) < \alpha_1$ and $v_2(x) \geq \alpha_2$, as desired. ∎

PROPOSITION 4.4 (Weak approximation theorem for independent valuations): *Let v_1, $\ldots, v_m$ be independent valuations of a field K. Let $a_1, \ldots, a_m$ be elements of K, and*

for each i let $\alpha_i \in \Gamma_{v_i}$. Then there exists $x \in K$ such that

$$v_i(x - a_i) = \alpha_i, \qquad i = 1, \ldots, m.$$

Proof: For each i choose $b_i \in K$ such that $\alpha_i = v_i(b_i)$ and $c_i = a_i + b_i \neq 0$. Lemma 4.2 gives $z_i \in K$ such that

$$v_i(z_i) < -|\alpha_i - v_i(c_i)| \qquad \text{and} \qquad v_j(z_i) > |\alpha_j - v_j(c_i)| \text{ for } j \neq i.$$

Let $t_i = \frac{z_i}{z_i+1}$. Then $t_1 - 1 = \frac{-1}{z_i+1}$ and

$$v_i(t_i - 1) = -v_i(z_i + 1) = -v_i(z_i) > |\alpha_i - v_i(c_i)| \geq \alpha_i - v_i(c_i)$$
$$v_i(t_j) = v_i(z_j) - v_i(z_j + 1) = v_i(z_j) > |\alpha_i - v_i(c_j)| \geq \alpha_i - v_i(c_j) \text{ for } j \neq i.$$

Let $x = \sum_{j=1}^{m} t_j c_j$. Then

$$v_i(x - c_i) \geq \min_{j \neq i}\{v_i(t_i - 1) + v_i(c_i),\ v_i(t_j) + v_i(c_j)\} > \alpha_i.$$

Hence, $v_i(x - a_i) = v_i((x - c_i) + b_i) = \alpha_i$. ∎

PROPOSITION 4.5 (Weak approximation theorem for incomparable valuations): *Let v_1, $\ldots, v_m$ be incomparable valuations of a field K. Then, for each $z \in K^\times$ there exists $x \in K$ such that $v_1(x) = v_1(z)$ and $v_i(x) > v_i(z)$, $i = 2, \ldots, m$.*

Proof: Let i be an integer between 1 and m. By assumption there exists $a \in K$ such that $v_1(a) \leq 0$ and $v_i(a) > 0$. Also, there exists $b \in K$ such that $v_1(b) < 0$ and $v_i(b) \geq 0$. Let $c_i = ab$, $\alpha_1 = \max\{v_1(c_2), \ldots, v_1(c_m)\}$, and $\alpha_i = v_i(c_i)$ for $i = 2, \ldots, m$. Then $v_1(c_i) \leq \alpha_1 < 0$ and $v_i(c_i) = \alpha_i > 0$ for $i = 2, \ldots, m$. By Lemma 4.2, there exists $t \in K$ such that $v_1(t) \leq \alpha_1$ and $v_i(t) \geq \alpha_i$, $i = 2, \ldots, m$. Then $x = z(1 + t^{-1})^{-1}$ satisfies $v_1(x) = v_1(z)$ and $v_i(x) > v_i(z)$, $i = 2, \ldots, m$, as desired. ∎

REMARK 4.6: Ribenboim [R, p. 131] proves a stronger form of the weak approximation theorem for incomparable valuation which is, however, somewhat difficult to apply. ∎

5. Places.

Let F be a field. Adjoin the symbol ∞ to F together with the following rules for $a \in F$:

$$a + \infty = \infty, \quad a \cdot \infty = \infty \text{ if } a \neq 0,$$

$$\infty \cdot \infty = \infty, \quad 1/0 = \infty, \quad , \text{ and } 1/\infty = 0.$$

The expressions $\infty + \infty$, $0 \cdot \infty$ and ∞/∞ are undefined.

A **place** φ of a field K into a field F is a mapping $\varphi\colon K \to F \cup \{\infty\}$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ whenever the expressions on the right sides of these formulas are defined, and such that $\varphi(1) = 1$. The place φ is **trivial** if $\varphi(a) \neq 0$ for every $a \in K$. In this case φ is an embedding of K into F.

For an arbitrary place φ of K the set of **finite** elements $O = \{x \in K |\ \varphi(x) \neq \infty\}$ is a valuation ring whose maximal ideal is $M = \{x \in K |\ \varphi(x) = 0\}$. The residue field $\overline{K} = O/M$ is isomorphic to the subfield $\varphi(O)$ of F.

Conversely, if O is a valuation ring of K with a maximal ideal M, then the map $\varphi\colon K \to M/O$ which maps each element $x \in O$ onto its residue class $\bar{x}$ modulo O and $\varphi(x) = \infty$ if $x \in K - O$ is a place of K whose valuation ring is O.

Two places φ_1, φ_2 of a field K with residue fields $\overline{K}_1$ and $\overline{K}_2$, respectively, are **equivalent** if there exists an isomorphism $\sigma\colon \overline{K}_1 \to \overline{K}_2$ such that $\sigma \circ \varphi_1 = \varphi_2$. This happens exactly if the valuation rings of φ_1 and φ_2 coincide.

EXAMPLE 5.1: *The p-adic place.* Let R be a unique factorization domain with a quotient field K. To each prime element p of R we attach a place φ_p of K into $\overline{K}_p = R/pR$ by the following rule:

$$\varphi_p\left(\frac{a}{b}p^m\right) = \begin{cases} 0 & \text{if } m > 0 \\ \bar{a}/\bar{b} & \text{if } m = 0 \\ \infty & \text{if } m < 0. \end{cases}$$

Here $a, b \in R$ are relatively prime to p, $\bar{a}$ is the residue class of a modulo p and $m \in \mathbb{Z}$. Observe that the places φ_p bijectively correspond to the valuations v_p defined in Example 2.1

EXERCISE 5.2: Let φ be a place of a field F and let $x_1, \ldots, x_n$ be elements of F. Prove that there exists i between 1 and n such that φ is finite at $x_1/x_i, \ldots, x_n/x_i$.

Let R be a **valuation ring** of a field K (Section 1) with a maximal ideal M. The map φ that maps each $x \in R$ onto its residue modulo M and $x \in F - R$ onto ∞ is a place of F whose valuation ring is R.

Let now (K, v) be a valued field. Denote the corresponding place by φ_v. Let L be a field extension of K and let w be a valuation of L. Suppose that $K \cap O_w = O_v$. Then, replacing w with an equivalent valuation, if necessary, we may consider Γ_v as an ordered subgroup of Γ_w, and then w is an extension of v. We say that (L, w) is an **extension** of (K, v). Similarly, we may embed $\overline{K}_v$ in $\overline{L}_w$ and change φ_w to an equivalent valuation such that φ_w is an extension of φ_v. We show below that it is always possible to extend a valuation from K to L.

LEMMA 5.3: *Let φ be a homomorphism of an integral domain R into an algebraically closed field F and let x be a nonzero element of a field that contains R. Then φ extends to a homomorphism of $R[x]$ or of $R[x^{-1}]$ into F.*

Proof: Let $P = \mathrm{Ker}(\varphi)$. Extend φ to R_P by

$$\varphi\big(\frac{a}{b}\big) = \frac{\varphi(a)}{\varphi(b)} \text{ for } a \in R,\ b \in R - P.$$

So, we may assume that R is a local ring and P is its maximal ideal.

We prove that at least one of the ideals $P \cdot R[x]$ and $P \cdot R[x^{-1}]$ of the rings $R[x]$ and $R[x^{-1}]$ respectively is proper. Otherwise there exist positive integers m and n and elements $a_i, b_j \in P$ such that

$$(1a) \qquad 1 = a_0 + a_1 x + \cdots + a_m x^m$$

$$(1b) \qquad 1 = b_0 + b_1 x^{-1} + \cdots + b_n x^{-n}$$

Assume that m and n are minimal positive integers that satisfy (1). Observe that $1 - a_0$ is a unit of R. We may therefore bring a_0 to the left hand side of (1a) and multiply by $(1 - a_0)^{-1}$ to obtain an equation of the form

$$(2a) \qquad 1 = c_1 x + \cdots + c_m x^m, \qquad c_i \in P.$$

Similarly (1b) can be transposed to

$$(2b) \qquad 1 = d_1 x^{-1} + \cdots + d_n x^{-n}, \qquad d_j \in P.$$

Assume that $m \geq n$. Then multiply (2b) by x^m and substitute in (2a) to obtain an equation of the form (2a) of smaller degree. This contradiction to the minimality of m proves our assertion.

Suppose therefore that $P \cdot R[x]$ is a proper ideal of $R[x]$. By Zorn's lemma, $R[x]$ has a maximal ideal M that contains P. As $M \cap R = P$, we may embed $\overline{K} = \varphi(R)$ into $R[x]/M$. Let $\bar{x} = x + M$. Then $\overline{K}[\bar{x}] = R[x]/M$ and the canonical map $R[x] \to \overline{K}[\bar{x}]$ extends φ. Furthermore, $\overline{K}[\bar{x}]$ is a field. Hence $\bar{x}$ is algebraic over $\overline{K}$ and therefore lies in F. ∎

PROPOSITION 5.4 (Chevalley): *Let φ be a homomorphism of an integral domain R into an algebraically closed field F. Let K be a field that contains R. Then φ extends to a place of K into F.*

Proof: Consider the set Φ of all pairs (R_i, φ_i) where R_i is a subring of K that contains R and φ_i is a homomorphism of R_i into F that extends φ. Define a partial ordering on this set by $(R_i, \varphi_i) \leq (R_j, \varphi_j)$ if $R_i \subseteq R_j$ and φ_j extends φ_i. By Zorn's Lemma Φ contains a maximal element (R', φ'). From the maximality, R' is a local ring and $\mathrm{Ker}(\varphi')$ is its unique maximal ideal. By Lemma 5.3, for each $x \in K$ either $x \in R'$ or $x^{-1} \in R'$. If $R' = K$, then φ' is a monomorphism of K into F. Otherwise, the extension of φ' to K that maps each $x \in K - R'$ to ∞ is a place of K into F that extends φ. ∎

COROLLARY 5.5: *Let v be a valuation of a field K and let L be an extension of K. Then v can be extended to a valuation of L.*

PROPOSITION 5.6: Let φ be a monomorphism of an integral domain R into a field F. Let L be a field containing R and algebraic over the quotient field of R. Then every place of L that extends φ is trivial.

Proof: Let ψ be a place of L which extends φ. If ψ is nontrivial, there exists $x \in L$ such that $\psi(x) = \infty$. Since φ is a monomorphism, we may assume that x satisfies an equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with coefficients in R. Divide this equation by x_n and apply ψ. As $\psi(x^{-1}) = 0$ this leads to a contradiction $1 = 0$. Conclude that ψ is trivial. ∎

EXAMPLE 5.7: *Transcendental extensions of a valued field* $(K, \bar{v})$.

(a) *Field of rational functions.* Let t be a transcendental element over K. Extend $\bar{v}$ to a function v: $K[t] \to \Gamma_{\bar{v}}$ by

$$v(\sum_{i=0}^{n} a_i t^i) = \min_{0 \le i \le n} \bar{v}(a_i).$$

Then $v(f+g) \ge \min\{v(f), v(g)\}$ and $v(fg) = v(f) + v(g)$. The latter equality is essentially **Gauss' lemma**. It follows in the following way.

Suppose that $f(t) = \sum_{i=0}^{m} a_i t^i$ and $g(t) = \sum_{j=0}^{n} b_j t^j$. Choose a minimal k between 0 and m such that $\bar{v}(a_i) \ge \bar{v}(a_k)$ for all $1 \le i \le m$. Choose a minimal l between 0 and n such that $\bar{v}(b_j) \ge \bar{v}(b_l)$ for all $1 \le j \le n$. For each (i,j) we have $\bar{v}(a_i b_j) \ge \bar{v}(a_k b_l)$. If $i + j = k + l$ and $(i,j) \ne (k,l)$, then either $i < k$ or $j < l$. Hence, by the minimality of (k,l), $\bar{v}(a_i b_j) = \bar{v}(a_i) + \bar{v}(b_j) > \bar{v}(a_k) + \bar{v}(b_l) = \bar{v}(a_k b_l)$. It follows that $\bar{v}(\sum_{i+j=k+l} a_i b_j) = \bar{v}(a_k) + \bar{v}(b_l) = v(f) + v(g)$. Hence $v(fg) = v(f) + v(g)$, as contended.

Now extend v to $K(t)$ by $v(f/g) = v(f) - v(g)$. The extended function is a valuation of $K(t)$ which extends v.

(b) *Fields of power series.* Order $\mathbb{Z} \times \Gamma_v$ lexicoraphically:

$$(m, \alpha) < (n, \beta) \quad \text{if and only if} \quad m < n \text{ or } m = n \text{ and } \alpha < \beta.$$

Extend $\bar{v}$ to a valuation v: $K((t))^\times \to \mathbb{Z} \times \Gamma_{\bar{v}}$ by

$$v(\sum_{i=m}^{\infty} a_i t^i) = (m, \bar{v}(a_m)) \qquad \text{if } a_m \ne 0.$$

Then $O_v = \{\sum_{i=0}^{\infty} a_i t^i |\ \bar{v}(a_i) \ge 0\}$, $M_v = \{\sum_{i=0}^{\infty} a_i t^i |\ \bar{v}(a_i) > 0\}$ and $U_f = \{\sum_{i=0}^{\infty} a_i t^i |\ \bar{v}(a_0) = 0\}$.

Define a valuation w: $K((t)) \to \mathbb{Z}$ by

$$w(\sum_{i=m}^{\infty} a_i t^i) = m \qquad \text{if } a_m \ne 0.$$

Then $\overline{K}_w = K$ and $O_w = \{\sum_{i=0}^{\infty} a_i t_i |\ a_i \in K,\ i = 0, 1, 2 \ldots\}$ contains O_v. Hence w is coarser than v. If $f = \sum_{i=0}^{\infty} a_i t_i \in U_w$, then $a_0 \ne 0$ and $v(f) = \bar{v}(a_0) = \bar{v}(\bar{f})$, where $\bar{f} = f + M_w$. Thus, $\bar{v}$ is the reduction of v in the sense of Section 3. ∎

6. Algebraic extensions.

Let L/K be extension of fields. By Chevalley's theorem (Proposition 5.4), each valuation v of K extends to a valuation of L. More can be said about the extensions of v to L if L/K is algebraic.

Let R be a subring of K. Recall that an element x of L is **integral** over R if it satisfies an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + x_0 = 0 \tag{1}$$

with coefficients $a_i \in R$. A subring S of L which contains R is **integral** over R if each $x \in S$ is integral over R. We say that a prime Q of L **lie over** a prime P of R if $P = R \cap Q$.

PROPOSITION 6.1: *Let R be a local integral domain with quotient field K, and with a maximal ideal P. Let φ_P: $R \to R/P$ the canonical homomorphism. Let L be an algebraic extension of R. Then an element x of L is integral over R if and only if $\varphi(x)$ is finite for each valuation φ of L which extends φ_P.*

Proof: Suppose first that x is integral over R and satisfies (1). Let φ be an extension of φ_P. If $\varphi(x) = \infty$, then $\varphi(x^{-1}) = 0$. Divide (1) by x^n and apply φ to get a contradiction: $1 = 0$. Conclude that $\varphi(x)$ is finite.

Conversely, suppose that $\varphi(x)$ if finite for each place φ of L which extends φ_P. Then the ideal of $R[x^{-1}]$ generated by P and x^{-1} is the entire ring. Otherwise $R[x^{-1}]$ has a maximal ideal M which contains P and x^{-1}. In particular $R \cap M = P$. Hence, the canonical map φ_M: $R[x^{-1}] \to R[x^{-1}]/M$ extends φ_P. Extend φ_M to a place φ of L (Proposition 5.4). Then $\varphi(x^{-1}) = 0$ and therefore $\varphi(x) = \infty$, a contradiction.

So, $1 = a_0 + a_1x^{-1} + \ldots + a_nx^{-n}$ with $a_0 \in P$ and $a_1, \ldots, a_n \in R$. In particular $1 - a_0$ is a unit of R. So, bring a_0 to the left hand side and multiply the equation by $(1 - a_0)^{-1}$ to get and equation of the form $1 = b_1x^{-1} + \cdots + b_nx^{-n}$ with $b_i \in R$. Hence $x^n = b_1x^{n-1} + \cdots + b_n$ and x is integral over R. ∎

It follows that the set of all elements of L which are integral over R is a ring. (Of course this is true for an arbitrary integral domain R and not only for a local ring.) It

is the **integral closure** of R in L. We may therefore reformulate Proposition 6.1 as follows:

COROLLARY 6.2: *Let R be a local integral domain with quotient field K, and with a maximal ideal P. Let L be an algebraic extension of R. Then the integral closure of R in L is the intersection of all valuation rings of L which contain R whose maximal ideal contain P.*

LEMMA 6.3: *Let R be an intergral domain with quotient field K. Let L be an algebraic extension of K and let S be the integral closure of R in L.*

(a) *If R is a field, then S is also a field.*

(b) *If M is a maximal ideal of R and N is an ideal of S lying over M, then N is also maximal.*

Proof of (a): Each $x \in S$, $x \neq 0$, satisfies an equation of the form $x^n + a_{n-1}x^{n-1} \cdots + a_0 = 0$ with $a_0 \neq 0$. Hence, x^{-1} satisfies $a_0^{-1} + a_0^{-1}a_{n-1}x^{-1} + \cdots + x^{-n} = 0$. Hence $x^{-1} \in S$. Conclude that S is a field.

Proof of (b): S/N is integral over the field R/M. Hence, by (a), S/N is a field. Conclude that N is maximal. ∎

PROPOSITION 6.4: *let (L, w) be an algebraic extension of a valued field (K, v). Denote the integral closure of O_v in L by R and let $P = R \cap M_w$. Then P is a maximal ideal of R and O_w is the local ring of R at P.*

Proof: As $O_v \cap P = M_v$ is maximal, Lemma 6.3 implies that P is maximal. By Corollary 6.2, $R \subseteq O_w$. Hence $R_P \subseteq O_w$. So, we consider $x \in O_w$ and prove that it belongs to R_P.

Indeed x satisfies an equation

$$a_n x^n + \cdots + a_0 = 0 \text{ with } a_i \in K,\ i = 0, \ldots, n \text{ and } a_n = 1. \tag{2}$$

Let k be an integer between 0 and n such that $v(a_k) \leq v(a_i)$ for $i = 0, \ldots, k$ and $v(a_k) < v(a_i)$ for $i = k+1, \ldots, n$. Put $b_i = a_i/a_k$. Then $b_1, \ldots, b_{k-1} \in O_v$, $b_k = 1$, and

$b_{k+1}, \ldots, b_n \in M_v$. Devide (2) by $a_k x^k$ to get

$$(3) \qquad (b_n x^{n-k} + \cdots + b_{k+1}x + 1) + x^{-1}(b_{k-1} + \cdots + b_0 x^{-k+1}) = 0.$$

Let $y = b_n x^{n-k} + \cdots + b_{k+1}x + 1$ and $z = b_{k-1} + \cdots + b_0 x^{-k+1}$. Then $y + x^{-1}z = 0$. We prove that $y, z \in S$ and $y \notin P$.

Let φ be a place of L which extends φ_v. Suppose first that $\varphi(x)$ is finite. As y is a polynomial in x with coefficients in R, $\varphi(y)$ is finite. Hence φ is also finite on $z = -xy$.

Secondly suppose that $\varphi(x) = \infty$. Then $\varphi(z)$ is finite, since z is a polynomial in x^{-1} with coefficients in R. Hence φ is also finite on $y = -x^{-1}z$.

So, in both cases, φ is finite on y and z. Hence, by Proposition 6.1, $y, z \in R$. Finally, since $x \in O_w$ and $b_{k+1}, \ldots, b_n \in M_w$, we have $y = b_n x^{n-k} + \cdots + b_{k+1}x + 1 \notin M$. Hence $y \notin P$. Conclude that x belongs to R_P. ∎

LEMMA 6.5: *Let R and S be integral domains such that S is integral over R. Let P be a prime ideal of R and Q_1, Q_2 be two prime ideals of S lying over P. If $Q_1 \subseteq Q_2$, then $Q_1 = Q_2$.*

Proof: There is a canonical homomorphism φ of S/Q_1 onto S/Q_2 which is the identity on R/P. Since both S/Q_1 and S/Q_2 are algebraic over R/P, φ must be injective (Lemma 5.6). Conclude that $Q_1 = Q_2$. ∎

COROLLARY 6.6: *Let (K, v) be a valued field, let L be a separable algebraic extnesion, and let v' and v'' be inequivalent extensions of v to L. Then v' and v'' are incomparable.*

Proof: Let R be the integral closure of O_v in L. By Proposition 6.4, $O_{v'}$ (resp., $O_{v''}$) is the local ring of R at $P_{v'} = R \cap M_{v'}$ (resp., $P_{v''} = R \cap M_{v''}$). Assume that $O_{v'} \subseteq O_{v''}$. Then $M_{v''} \subseteq M_{v'}$ and therefore $P_{v''} \subseteq P_{v'}$. As both $P_{v'}$ and $P_{v''}$ lie over M_v, they are equal (Lemma 6.6). Conclude that $O_{v'} = O_{v''}$. ∎

COROLLARY 6.7 (Chinese remainder theorem): *(a) Let $I_1, \ldots, I_n$ be distinct ideals of a commutative ring R with 1 such that $I_i + I_j = R$ for all $i \neq j$ (In particular this assumption holds if $I_1, \ldots, I_m$ are distinct maximal ideals.) Then, for all $a_1, \ldots, a_n \in R$ there exists $x \in R$ such that $x - a_i \in I_i$, $i = 1, \ldots, n$.*

(b) *Let (K, v) be a valued field, L a finite separable extension, and $w_1, \dots, w_n$ distinct (=nonequivalent) extensions of v to L. Then, for all $a_i \in O_{w_i}$, $i = 1, \dots, n$, there exists $x \in L$ such that $w_i(x - a_i) > 0$, $i = 1, \dots, n$.*

(c) *In the notation of (b) there exists $x \in L$ such that $w_1(x) = 0$ and $w_i(x) > 0$ for $i = 2, \dots, n$.*

Proof of (a): By assumption there exist $y_{ij} \in I_i$ and $z_{ij} \in I_j$ such that $y_{ij} + z_{ij} = 1$. Hence, $y_i = \prod_{j \neq i} z_{ij} \equiv 0 \bmod I_k$ for $k \neq i$ and $y_i = \prod_{j \neq i}(1 - y_{ij}) \equiv 1 \bmod I_i$. Conclude that $x = y_1 a_1 + \cdots + y_n a_n$ satisfies $x \equiv a_i \bmod I_i$ for $i = 1, \dots, n$.

Proof of (b): Let R be the integral closure of O_v in L. By Proposition 6.4, $P_i = R \cap M_{w_i}$ is a maximal ideal of R and O_{w_i} is the local ring of R at P_i, $i = 1, \dots, n$. Hence, $P_1, \dots, P_n$ are distinct. Also, there exist $b_i, c_i \in R$ such that $c_i \notin P_i$ and $a_i = b_i/c_i$. Since P_i is maximal, there exists $c_i' \in R$ such that $c_i' c_i \equiv 1 \bmod P_i$. Hence, $a_i' = c_i' b_i \in R$ satisfies $w_i(a_i' - a_i) > 0$, $i = 1, \dots, n$.

By (a) there exists $x \in R$ such that $w_i(x - a_i') > 0$, $i = 1, \dots, n$. Conclude that $w_i(x - a_i) > 0$, $i = 1, \dots, n$, as desired.

Proof of (c): Take $a_1 = 1$ and $a_2 = \cdots = a_n = 0$ in (b). ∎

7. Residue degrees and ramification indices.

Let $(L,w)/(K,v)$ be an extension of valued fields. Then $O_v \cap M_w = M_v$ and therefore $\overline{K}_v$ naturally embeds in $\overline{L}_w$. Also, $K^\times \cap U_w = U_v$ and therefore Γ_v naturally embeds in Γ_w. The degree $f(w/v) = [\overline{L}_w : \overline{K}_v]$ is the **residue degree** of the extension, and $e(w/v) = (\Gamma_w : \Gamma_v)$ is its **ramification index**. The following lemma proves that both of them are finite if L/K is a finite extension.

LEMMA 7.1: *Let $(L,w)/(K,v)$ be a finite extension of valued fields. Then $e(w/v)f(w/v) \leq [L:K]$. In particular $e(w/v), f(w/v) \leq [L:K]$.*

Proof: Let $x_1, \ldots, x_e$ be elements of $L^\times$ such that $w(x_1), \ldots, w(x_e)$ represent distinct cosets of Γ_w modulo Γ_v. Let $u_1, \ldots, u_f$ be elements of U_w whose reduction $\bar{u}_1, \ldots, \bar{u}_f$ modulo M_w are linearly independent over $\overline{K}_v$. It suffices to prove that the ef elements $x_i u_j$ are linearly independent over K.

Indeed, assume that there exist elements $a_{ij} \in K$, not all zero, such that

$$\sum_{i=1}^{e} \sum_{j=1}^{f} a_{ij} x_i u_j = 0. \tag{1}$$

Assume without loss that $w(a_{11}x_1) \leq w(a_{ij}x_i)$ for all i,j. Then $w(a_{11}x_1) < w(a_{ij}x_i)$ for $i > 1$, because an equality for some $i > 1$ and j will imply that $w(x_1)$ and $w(x_i)$ lie in the same coset modulo Γ_v, in contrast to their choice. Let $y_{ij} = a_{ij}x_i/a_{11}x_1$. Then $y_{11} = 1$, $y_{1j} \in K$, and $w(y_{ij}) > 0$ if $i > 1$. Divide (1) by $a_{11}x_1$ and reduce it modulo M_w:

$$\sum_{j=1}^{f} \bar{y}_{1j} \bar{u}_j = 0. \tag{2}$$

Since $\bar{u}_1, \ldots, \bar{u}_j$ are linearly independent over $\overline{K}$ all the coefficients of (2) are 0. In particular $1 = \bar{y}_{11} = 0$, a contradiction. Conclude that the $x_i u_j$ are linearly independent over K, as desired. ∎

COROLLARY 7.2: *Let $(L,w)/(K,v)$ be an algebraic extension of valued fields. Then Γ_v is cofinal in Γ_w. That is, for each $\alpha \in \Gamma_w$ there exists $\beta \in \Gamma_v$ such that $\alpha < \beta$.*

Proof: Suppose without loss that $\alpha \geq 0$. Choose $x \in L$ such that $w(x) = \alpha$. Then the ramification index e of the restriction of w to $K(x)$ over K is finite. It follows that $\beta = e\alpha \in \Gamma_v$. Obviously $\beta > \alpha$. ∎

8. Galois extensions.

An integral domain R with quotient field K is **integrally closed** if it coincides with its integral closure in K. That is, each element of K which is integral over R belongs to R. If L is a Galois extension of K and S is the integral closure of R in L, then S is invariant under the action of $\mathcal{G}(L/K)$. If P is a prime ideal of R and Q is a prime ideal of S which lies over P, then for each $\sigma \in \mathcal{G}(L/K)$, Q^σ is also a prime ideal of S which lies over P. The converse is also true:

PROPOSITION 8.1: *Let R be an integrally closed integral domain with quotient field K. Let L be a Galois extension of K and let S be the integral closure of R in L. Let P be a prime ideal of R and let Q, Q' be two prime ideals of S which lie over P. Then there exists $\sigma \in \mathcal{G}(L/K)$ such that $Q^\sigma = Q'$.*

Proof: The case where L/K is of infinite degree can be reduced to the case where the degree is finite by Zorn's lemma. So, we assume that $G = \mathcal{G}(L/K)$ is finite.

Let $Q_1, \ldots, Q_m$ be the distinct conjugates of Q over K. Assume that Q' is not one of them. By Lemma 6.6, for each i between 1 and m and for each $j \neq i$, $Q' \not\subseteq Q_i$ and $Q_j \not\subseteq Q_i$. Hence $Q'Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_m \not\subseteq Q_i$. Therefore, there exists $x_i \in Q' \cap Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_m$ such that $x_i \notin Q_i$. Let $y = x_1 + \cdots + x_m$. Then $y \in Q'$ but $y \notin Q_1, \ldots, Q_m$. It follows that $y^\sigma \notin Q_1, \ldots, Q_m$ for each $\sigma \in G$. For otherwise there would exist j such that $y^\sigma \in Q_j$ and therefore $y \in Q_j^{\sigma^{-1}}$, which is some of the Q_i's, a contradiction. It follows that $z = N_{L/K}y = \prod_{\sigma \in G} y^\sigma \notin Q_1, \ldots, Q_m$. On the other hand, as R is integrally closed, $z \in K \cap S = R$ and therefore $z \in R \cap Q' = P \subseteq Q_1$. Conclude from this contradiction that Q' is conjugate to Q. ∎

COROLLARY 8.2: *Let K be a field with a valuation v. Let L be a Galois extension of K with two extensions w and w' of v. Then there exist $\sigma \in \mathcal{G}(L/K)$ such that $O_w^\sigma = O'_w$.*

Proof: Denote the integral closure of O_v in L by R. Then O_w is the local ring of R at

$P_w = R \cap M_w$ (Proposition 6.4). Similarly, $O_{w'}$ is the local ring of R at $P_{w'} = R \cap M_{w'}$. Both prime ideals lie over M_v. Hence, by Proposition 8.1, there exists $\sigma \in \mathcal{G}(L/K)$ such that $P_w^\sigma = P_{w'}$. So, $O_w^\sigma = O_{w'}$. ∎

In the setup of Corollary 8.2 we call $D_w = \{\sigma \in \mathcal{G}(L/K) |\ O_w^\sigma = O_w\}$ the **decomposition group** of w over K. It is a subgroup of $\mathcal{G}(L/K)$ whose fixed field in L is the **decomposition field** of w over K.

We say that a valuation v of a field K has a **unique extension** to an algebraic extension L of K, if any two extensions of v to L are equivalent.

COROLLARY 8.3: *Let L/K be a Galois extension and let w be a valuation of L. Denote the decomposition field of w over K by L_0 and let w_0 be the restriction of w to L_0. Then w_0 has a unique extension to L.*

Proof: If w' is an extension of w_0 to L, then there exists $\sigma \in \mathcal{G}(L/L_0)$ such that $O_w^\sigma = O_{w'}$ (Corollary 8.2). But, as $\mathcal{G}(L/L_0)$ is the decomposition group of w over K, we have $O_w^\sigma = O_w$. Hence $O_{w'} = O_w$, and therefore w and w' are equivalent, as asserted. ∎

REMARK 8.4: *Purely inseparable extensions.* If L/K is a purely inseparable extension and v is a valuation of K, then v has a unique extension to L. Indeed, if w and w' are extensions of v to L and $x \in L$, then there exists a power q of $\mathrm{char}(K)$ such that $x^q \in K$. Hence, $qw(x) = v(x^q) = qw'(x)$ and therefore $w(x) = w'(x)$.

Likewise one proves that if v' is another valuation of K which is coarser than v, then the unique extension of v' to L is coarser than w. ∎

Suppose that w is a valuation of a field L which is algebraic over K. Then each isomorphism σ of L over K into the algebraic closure $\widetilde{K}$ of K defines a valuation w^σ of L^σ by the formula $w^\sigma(x) = w(x^{\sigma^{-1}})$. It satisfies $O_w^\sigma = O_{w^\sigma}$.

Now suppose that L is a finite Galois extension of K, let v be the restriction of w to K. By Proposition 8.2, $\{w^\sigma |\ \sigma \in \mathcal{G}(L/K)\}$ is the set of all extensions of v to L. Let L_0 be the decomposition field of w over K. Denote the restriction of w to L_0 by w_0. Let $\sigma_1, \ldots, \sigma_m \in \mathcal{G}(L/K)$ be representatives for the left cosets of $\mathcal{G}(L/K)$ modulo $\mathcal{G}(L/L_0)$.

COROLLARY 8.5: *In the above notation,*

(a) $w^{\sigma_1^{-1}}, \ldots, w^{\sigma_m^{-1}}$ *are the distinct extensions of* v *to* L, *and*

(b) *with* $\sigma_1 = 1$, *the restriction of* $w^{\sigma_i^{-1}}$ *to* L_0 *is not equivalent to* w_0, $i = 2, \ldots, m$; *in particular, if* $m \geq 2$, *then* v *has at least two extensions to* L_0.

Proof: Statement (a) follows from Corollary 8.2 and from the definition of L_0. Statement (b) follows from (a) and from Corollary 8.3. ∎

An extension of valued fields $(L, w)/(K, v)$ is **immediate** if the residue field and the value group of (L, w) coincide with those of (K, v).

PROPOSITION 8.6: *Let* $(L, w)/(K, v)$ *be a Galois extension of valued fields. Let* L_0 *be the decomposition field of* w *over* K *and denote the restriction of* w *to* L_0 *by* w_0. *Then* (L_0, w_0) *is an immediate extension of* (K, v).

Proof: (Ax) Let $w_0, v_1, \ldots, v_k$ be the nonequivalent extensions of v to L_0. By Corollary 8.5(b), and with its notation, the restriction of $w^{\sigma_j^{-1}}$ to L_0 belongs to $\{v_1, \ldots, v_k\}$ for $j = 2, \ldots, m$. The rest of the proof breaks up in two parts.

PART A: *The residue field of* L_0 *with respect to* w_0 *is* $\overline{K}_v$. Indeed, let $z \in L_0$ be an element with $w_0(z) \geq 0$. By the Chinese remainder theorem (Proposition 6.8) there exists $y \in L_0$ such that

$$w_0(y - z) > 0 \text{ and } v_i(y) > 0 \text{ for } i = 1, \ldots, k. \tag{1}$$

The trace $a = y + y^{\sigma_2} + \cdots + y^{\sigma_m}$ of y belongs to K. For each $2 \leq j \leq m$, (1) implies $w(y^{\sigma_j}) = w^{\sigma_j^{-1}}(y) = v_i(y) > 0$ for some $i \in \{1, \ldots, k\}$. Hence $w_0(a - y) = w(a - y) > 0$. So, by (1), $w_0(a - z) > 0$. Conclude that $\overline{L}_{0,w_0} = \overline{K}_v$.

PART B: *The value group of* L_0 *with respect to* w_0 *is* Γ_v. We have to find for each $x \in L_0^\times$ a $d \in K^\times$ such that $w_0(x) = w_0(d)$. Apply (1) with $z = 1$ to find $s \in L_0^\times$ such that $w_0(s) = 0$ and $v_i(s) > 0$ for $i = 1, \ldots, k$. Hence $w(s) = 0$ and $w(s^{\sigma_j}) > 0$ for $j = 2, \ldots, m$. Then $w((sx)^{\sigma_j}), w((s^2x)^{\sigma_j}), \ldots$ is an infinite sequence of elements of Γ_w for $j = 2, \ldots, m$. Hence, there exists a positive integer n such that

$w(s^n x) \neq w((s^n x)^{\sigma_2}), \ldots, w((s^n x)^{\sigma_m})$. Replace therefore x by $s^n x$, if necessary, to assume that $w(x) \neq w(x^{\sigma_2}), \ldots, w(x^{\sigma_m})$.

Under this assumption reenumerate $\sigma_2 \ldots, \sigma_m$ if necessary to find an integer k between 1 and m such that

$$w(x^{\sigma_2}), \ldots, w(x^{\sigma_k}) < w(x) < w(x^{\sigma_{k+1}}), \ldots, w(x^{\sigma_m}). \tag{2}$$

(note that $k = 1$ means that only the right inequalities exists, while $k = m$ means that only the left inequalities exist.) Then consider the fundamental symmetric polynomial of degree $k - 1$:

$$b = x^{\sigma_2} \cdots x^{\sigma_k} + \sum x^{\tau_2} \cdots x^{\tau_k},$$

where $\{\tau_2, \ldots, \tau_k\}$ ranges over all subsets of $\{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ of cardinality $k - 1$ which are different from $\{\sigma_2, \ldots, \sigma_k\}$. Thus, there exists i such that τ_i is not in $\{\sigma_2, \ldots, \sigma_k\}$. Hence, by (2), $w(x^{\sigma_2} \cdots x^{\sigma_k}) < w(x^{\tau_2} \cdots \tau^{\tau_k})$. It follows that $w(b) = w(x^{\sigma_2} \cdots x^{\sigma_k})$.

Likewise consider the fundamental symmetric polynomial of degree k:

$$c = x x^{\sigma_2} \cdots x^{\sigma_k} + \sum x^{\tau_1} x^{\tau_2} \cdots x^{\tau_k},$$

where $\{\tau_1, \ldots, \tau_k\}$ ranges over all subsets of $\{\sigma_1, \ldots, \sigma_m\}$ of cardinality k which are different from $\{\sigma_1, \ldots, \sigma_k\}$. As in the preceding paragraph, (2) implies that $w(c) = w(x x^{\sigma_2} \cdots x^{\sigma_k})$.

Both b and c belong to K. Hence $d = c/b$ is an element of K for which $w(d) = w(x)$, as desired. ∎

PROPOSITION 8.7: *Let $(L, w)/(K, v)$ be a Galois extension of valued fields. Then, $\overline{L}_w/\overline{K}_v$ is a normal extension. For each $\sigma \in D_w$ let $\bar{\sigma}$ be the automorphism of $\overline{L}_w$ over $\overline{K}_v$ defined by*

$$\bar{\sigma}\bar{x} = \overline{\sigma x}, \qquad x \in O_w \tag{3}$$

(bar means reduction modulo M_w). Then, the map $\sigma \mapsto \bar{\sigma}$ is an epimorphism of D_w onto $\mathrm{Aut}(\overline{L}_w/\overline{K}_v)$. *The kernel I_w of this epimorphism is the* **inertia group** *of w over K.*

Proof: Consider an element x in the integral closure R of O_v in L and let $f = \mathrm{irr}(x, K)$. Then $f(X) = \prod(X - x_i)$ with x_i in R. Then $\bar{f}(X) = \prod(X - \bar{x}_i)$ decomposes in $\overline{L}_w$

into linear factors and $\bar{f}(\bar{x}) = 0$. By Proposition 6.4, $\overline{R} = R/(R \cap M_w) = \overline{L}_w$. Conclude that $\overline{L}_w$ is a normal extension of $\overline{K}_v$.

Note that the right hand side of (3) does not depend on the lifting x of $\bar{x}$ to O_w. Indeed, if $y \in O_w$ satisfies $\bar{y} = \bar{x}$, then $y - x \in M_w$. Hence, $\sigma y - \sigma x \in M_w$ and therefore $\overline{\sigma y} = \overline{\sigma x}$.

To prove that each $\tau \in \mathrm{Aut}(\overline{L}_w/\overline{K}_v)$ lifts to an element of D_w we may first consider the restriction of τ to the maximal separable extension of $\overline{K}_v$ in $\overline{L}_w$ (which is a Galois extension), and then assume that it is finite. The general case will follow by Zorn's lemma (alternatively, by taking inverse limit).

So, we may assume that the maximal separable extension of $\overline{K}_v$ in $\overline{L}_w$ has the form $\overline{K}_v(a)$. Let $f_0 = \mathrm{irr}(a, \overline{K}_v)$. Let x be an element of O_w such that $\bar{x} = a$ and let $f = \mathrm{irr}(x, L_0)$, where L_0 is the decomposition field of w over K. By Proposition 8.6, $\bar{f} \in \overline{K}_v[X]$. Also $\bar{f}(a) = 0$ and therefore f_0 divides f. It follows that f has a root y such that $\bar{y} = \tau a$. Choose an element $\sigma \in \mathcal{G}(L/L_0) = D_w$ such that $\sigma x = y$. Then $\bar{\sigma} a = \bar{y} = \tau a$. Conclude that $\bar{\sigma} = \tau$ and the map is surjective. ∎

9. Comparable valuations under Galois extensions.

Our goal in this section is to extend comparable valuations of a field K to comparable valuations of an algebraic extension of K. This will be done with the well known going up and going down theorems of Cohen – Seidenberg.

LEMMA 9.1: (a) *If a field L is integral over an integral domain R, then R is also a field.*

(b) *Let $R \subseteq S$ be integral domains, I an ideal of R, and J an ideal of S which lies over I. If S is integral over R and J is maximal, then so is I.*

Proof: Statement (b) follows from (a), so we prove (a).

Any nonzero element x of R has an inverse x^{-1} in L. By assumption x satisfies an equation

$$x^{-n} + a_{n-1}x^{-(n-1)} + \cdots + a_0 = 0$$

with $a_i \in R, \quad i = 0, \ldots, n-1$. Hence $x^{-1} = -a_{n-1} - a_{n-2}x - \cdots - a_0 x^{n-1} \in R$. Conclude that R is a field. ∎

LEMMA 9.2 (Going up theorem of Cohen-Seidenberg): *Let $R \subseteq S$ be integral domains such that S is integral over R. Suppose that $Q \subseteq P$ are prime ideals of R. Let Q' be a prime ideal of S which lies over Q. Then S has a prime ideal P' which lies over P and contains Q'.*

Proof: Divide R by Q and S by Q' if necessary to assume that $Q = Q' = 0$. Then replace R and S, respectively, by their localizations: $R_P = \{a/b|\ a, b \in R,\ b \notin P\}$ and $S_P = \{x/b|\ x \in S,\ b \in R - P\}$, to assume that R is a local domain and P is its maximal ideal.

Let Q be a maximal ideal of S. By Lemma 9.1, $R \cap Q$ is a maximal ideal of R. Hence $R \cap Q = P$. ∎

LEMMA 9.3 (Going down theorem of Cohen-Seidenberg): *Let $R \subseteq S$ be integral domains such that S is integral over R. Suppose that $P' \subseteq P$ are prime ideals of R. Let Q be a prime ideal of S which lies over P. Then Q contains a prime ideal Q' of S that lies over P'.*

Proof: Let K (resp, L) be the quotient field of R (resp, S). We prove only the case we need, namely when L/K is separable. In this case consider the Galois closure $\widehat{L}$ of L/K. Let $\widehat{S}$ be the integral closure of R in $\widehat{L}$. By Lemma 9.2, $\widehat{S}$ has a prime ideal J' that lies over P'. Apply Lemma 9.2 again to find a prime ideal J of $\widehat{S}$ that lies over P and contains J'. Now apply Lemma 9.2 for the third time to find a prime ideal Q_1 of $\widehat{S}$ that lies over Q. As both J and J_1 lies over P there exists $\sigma \in \mathcal{G}(\widehat{L}/K)$ such that $J^\sigma = J_1$ Let $J_1' = J'^\sigma$ and $Q' = S \cap J_1'$. Then Q' is a prime ideal of S which is contained in Q and lie over P', as desired. ∎

We apply the going down theorem to valuations.

LEMMA 9.4: *Let v and w be valuations of a field K such that v is finer than w. Let L be a separable algebraic extension of K.*

(a) *Let v' be an extension of v to L. Then w extends to valuation w' of L which is coarser that v'.*

(b) *Let w' be an extension of w to L. Then v extends to a valution v' of L which is finer than w'.*

Proof of (a): Let R be the integral closure of O_v in L. Let $P_{v'} = R \cap M_{v'}$. By Proposition 6.4, $O_{v'}$ is the local ring of R at $P_{v'}$. By Lemma 9.3, $P_{v'}$ contains a prime ideal Q of R which lies over M_w. Then $M = QO_{v'}$ is a prime ideal of $O_{v'}$ which lies over Q and therefore also over M_w. By Lemma 3.3, L has a valuation w' such that $M_{w'} = M$. This valuation is coarser than v' and extends w.

Proof of (b): Assume without loss that L is Galois over K. Take any extension v'' of v to L. By (a), w extends to a valuation w'' of L such that $O_{v''} \subseteq O_{w''}$. By Corollary 8.2, there exists $\sigma \in \mathcal{G}(L/K)$ such that $O_{w'} = O^{\sigma}_{w''}$. Then $O^{\sigma}_{v''} \subseteq O_{w'}$ is a valuation ring of a valuation v' of L which extends v, as desired. ∎

PROPOSITION 9.5: *Let L/K be a Galois extension. Let v and w be valuations of L such that v is finer than w.*

(a) *The decomposition group G_v of v over K is contained in G_w.*

(b) *The decomposition field of w over K is contained in that of v.*

Proof: Statement (b) follows from statement (a). So, let us prove (a).

Let $\sigma \in G_v$. Then $O^{\sigma}_v = O_v$ and therefore both O_w and O^{σ}_w contain O_v. By Lemma 3.2(b), $O_w \subseteq O^{\sigma}_w$ or $O^{\sigma}_w \subseteq O_w$. Replace σ by σ^{-1} if necessary to assume that $O^{\sigma}_w \subseteq O_w$. Apply σ repeatedly on both sides to conclude that $O^{\sigma^n}_w \subseteq O^{\sigma^{n-1}}_w$ for each positive integer n.

Now consider an element $x \in O_w$. This element is contained in a finite Galois extension of K. Hence, there exists n such that $x^{\sigma^n} = x$. It follows that $x \in O^{\sigma^n}_w \subseteq O_w$. Conclude that $O_w = O^{\sigma}_w$, as asserted in (a). ∎

10. Ultrapowers of valued fields.

We say that a valuation v of a field K is **unbounded** if it is finer that no valuation of rank 1 of K. Such a valuation has the advantage that the set of all nonzero prime ideals of O_v forms a basis for the neighborhoods of 0 in K. This is the content of the following result:

LEMMA 10.1: *Let v be an unbounded valuation of a field K. Let $a_1, \dots, a_n$ be elements of $K^\times$. Then, for each $\alpha \in \Gamma_v$ there exists a valuation w of K which is coarser than v such that $w(a_1), \dots, w(a_n) \geq 0$ and*

$$w(z) > 0 \quad \textit{implies} \quad v(z) > \alpha.$$

Proof: * The set W of all valuations of K which are coarser than v is linearly ordered by the relation "finer that" (Lemma 3.2). Hence, by Lemma 3.3, the set $\{M_w |\ w \in W\}$ of the corresponding prime ideals of O_v is linearly ordered by inclusion. It follows that the intersection $\bigcap_{w \in W} M_w$ is a prime ideal of O_v, which must be 0, since otherwise it will be the maximal ideal of a valuation in W of rank 1 (Lemma 3.3).

Choose now $a \in K^\times$ such that $v(a) = \alpha$. Then there exists $w_0 \in W$ such that $a \notin M_{w_0}$. Also, there exists $w_i \in W$ such that $a_i^{-1} \notin M_{w_i}$, $i = 1, \dots, n$. Let w the coarsest valuation among $w_0, \dots, w_n$. Then $a, a_1^{-1}, \dots, a_n^{-1} \notin M_w$. Thus $w(a) \leq 0$ and $w(a_1), \dots, w(a_n) \geq 0$. If $w(z) > 0$, then $w(z) > w(a)$ and therefore $v(z) > v(a) = \alpha$, as desired. ∎

It turns out, that as far as elementary statements are concerned, each valuation may be replaced by an unbounded one. Here we use a multisorted first order language which includes a domain for a field K, a domain for an ordered group Γ and a function symbol for a valuation v: $K^\times \to \Gamma$. Of course, each sentence in the multisorted language can be rephrased in a usual first order language with a domain for a field K and a unary predicate symbol for the valuation ring O_v. Eventually, we extend our language to include domains and function symbols for several valuations, and also function symbols for orderings of the field.

---

* The proof of the lemma emerged from a discussion with Wulf-Dieter Geyer.

We refer to [FJ, Chap. 6] for the basic notions of model theory and ultraproducts. In particular we freely use Łoš theorem [FJ, Prop. 6.11] that an ultrapower $\mathcal{A}^* = \mathcal{A}^I/\mathcal{D}$ of any structure $\mathcal{A}$ is an **elementary extension** of $\mathcal{A}$. This means that a sentence with parameters in the domain A of $\mathcal{A}$ is true in $\mathcal{A}$ if and only if it is true in $\mathcal{A}^*$. Also, we use the term "almost all $i \in I$" in this context to mean that i ranges over a subset of A which belongs to $\mathcal{D}$.

LEMMA 10.2: *Each nonprincipal ultrapower $\Gamma^* = \Gamma^{\mathbb{N}}/\mathcal{D}$ of an ordered group Γ satisfies: for each $\alpha > 0$ there exists $\gamma > 0$ such that $n\alpha < \gamma$ for all $n \in \mathbb{N}$.*

Proof: Let $(\alpha_1, \alpha_2, \alpha_3, \ldots)$ be a sequence of elements of Γ that represents α modulo $\mathcal{D}$. Then $\alpha_n > 0$ for almost all $n \in \mathbb{N}$. Denote the element of Γ^* that represents $(\alpha_1, 2\alpha_2, 3\alpha_3, \ldots)$ by γ. For each $n \in \mathbb{N}$ and for almost all $r > n$ we have $ra_r > na_r$. Hence $\gamma > n\alpha$, as desired. ∎

LEMMA 10.3: *Let $(K^*, v^*) = (K^{\mathbb{N}}/\mathcal{D}, v^{\mathbb{N}}/\mathcal{D})$ be a nonprincipal ultrapower of a valued field (K, v). Then v^* is unbounded valuation of the field K.*

Proof: We have to prove that if a valuation w of K^* is coarser than v^*, then Γ_w is nonarchimedean (Lemma 3.4). Indeed choose $b \in M_w$, $b \neq 0$. By (2) of Section (3), for all $a, x \in K$ we have

$$v^*(x) > v^*(ab) \quad \text{implies} \quad w(x) > w(a). \tag{1}$$

Use Lemma 10.2 to choose an element $0 \neq x \in K^*$ such that $v^*(x) > nv^*(b)$ for all $n \in \mathbb{N}$. Then, by (1), $w(x) > (n-1)w(b)$ for all integers $n \geq 2$. Conclude that $w((K^*)^\times) \not\subseteq \mathbb{R}$, that is, Γ_w is nonarchimedean. ∎

11. Henselian fields.

Kurt Hensel defined the field of p-adic numbers $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic valuation v_p. He observed that v_p uniquely extends to a valuation of $\mathbb{Q}_p$ with the same residue field, $\mathbb{F}_p$, and valuation group, $\mathbb{Z}$, as $\mathbb{Q}$. He proved what we now call Hensel's lemma, which relates the solutions of a polynomial equation over $\mathbb{Q}_p$ to the solutions of the same equation over $\mathbb{F}_p$. It was later proved that v_p has a **unique extension** to each algebraic extension L of $\mathbb{Q}_p$.

We show in the following Proposition that those properties of $\mathbb{Q}_p$ are equivalent and we take them as a definition for a "Henselian field".

PROPOSITION – DEFINITION 11.1: *The following statements on a valued field (K, v) are equivalent. If they are satisfied, we say that (K, v) is a* **Henselian field** *(or also that K is* **Henselian** *with respect to v). Here we set $O = O_v$, $U = U_v$, $\overline{K} = \overline{K}_v$, and use a bar to denote reduction modulo $M = M_v$.*

(a) (Hensel's Lemma) *For each polynomial $f \in O[X]$ and for each $a \in O$ such that $\bar{f}(\bar{a}) = 0$ and $\overline{f'}(\bar{a}) \neq 0$ there exists $x \in O$ such that $f(x) = 0$ and $\bar{x} = \bar{a}$.*

(b) *The valuation v extends uniqely to each algebraic extension of K.*

(c) *For each monic polynomial $f \in O[X]$ and for all monic relatively prime polynomials $g_0, h_0 \in \overline{K}[X]$ such that $\bar{f} = g_0 h_0$ there exist monic polynomials $g, h \in O[X]$ such that $f = gh$, $\bar{g} = g_0$, and $\bar{h} = h_0$.*

(d) *If a monic polynomial $f \in O[X]$ is irreducible in $K[X]$, then $\bar{f}$ is a power of an irreducible polynomial in $\overline{K}[X]$.*

(e) *For each monic polynomial $f \in O[X]$, $a \in O$, and $\gamma \in \Gamma$ such that $\gamma \geq 0$ and $v(f(a)) > 2v(f'(a)) + \gamma$ there exists $x \in O$ such that $f(x) = 0$ and $v(x - a) > v(f'(a)) + \gamma$.*

Proof: We state two additional auxiliary statements which we prove to be equivalent to the statements (a) – (e).

(1a) For each monic polynomial $f \in O[X]$ and for each $a \in O$ such that $\bar{f}(\bar{a}) = 0$ and $\overline{f'}(\bar{a}) \neq 0$ there exists $x \in O$ such that $f(x) = 0$ and $\bar{x} = \bar{a}$.

(1b) Each polynomial $g(Y) = c_n Y^n + \cdots + c_2 Y^2 + c_1 Y + c_0 \in O[Y]$ such that $n \geq 1$,

$\bar{c}_0, \bar{c}_1 \neq 0$, and $\bar{c}_2 = \cdots = \bar{c}_n = 0$ has a root in O.

Proof of (a) implies (1a): Clear.

Proof of (1a) implies (b): By Remark 8.4 it suffices to prove that v uniquely extends to sparable extensions of K. Obviously it suffices to prove the uniqueness only for finite separable extensions. So, let L/K be a finite separable extension and assume without loss that L/K is Galois. Let w be an extension of v to L. Let L_0 be the decomposition field of w over L. By Corollary 8.5, the number of distinct extensions of v to L is $[L_0 : K]$.

Assume $[L_0 : K] > 1$. Denote the restriction of w to L_0 be w_0. Then there are $\sigma \in \mathcal{G}(L/K) \setminus \mathcal{G}(L/L_0)$. For each such σ we have $w_0^{\sigma^{-1}} \neq w_0$. By the Chinese remainder theorem (Proposition 6.7) there is $x \in L_0$ with $w_0(x) = 0$ and $w_0(x^\sigma) > 0$ for each $\sigma \in \mathcal{G}(L/K) \setminus \mathcal{G}(L/L_0)$. Let $x_1, x_2, \ldots, x_r$ with $x_1 = x$ be the distinct conjugates of x over K. Then $2 \leq r \leq [L_0 : K]$. For each $2 \leq i \leq [L_0 : K]$ there is $\sigma \in \mathcal{G}(L/K) \setminus \mathcal{G}(L/L_0)$ with $x_i = x^\sigma$. Thus, $w_0(x_i) > 0$.

Let $f(X) = \mathrm{irr}(x, K) = X^r + a_1 X^{r-1} + \cdots + a_r = \prod_{i=1}^r (X - x_i)$ be the irreducible polynomial of x over K. Then $-a_1 = x_1 + x_2 + \cdots + x_r$. Therefore $v(a_1) = w_0(x_1) = 0$. For $i > 1$, $a_i = \pm \Sigma x_{k_1} \cdots x_{k_r}$, where $(k_1, \ldots, k_r)$ ranges over all i-tuples of distinct integers between 1 and m. Hence, $v(a_i) > 0$.

Thus, $-\bar{a}_1$ is a simple root of $\bar{f}(X) = X^r(X + \bar{a}_1)$. Hence, by (1a), $f(X)$ has a root in K. As f is irreducible, $r = 1$. Conclude from this contradiction that v has only one extension to L.

Proof of (b) implies (c): Denote the splitting field of f by L and let $f(X) = \prod_{i=1}^n (X - x_i)$ the factorization of f into a product of linear factors in L. Reenumerate the roots such that $g_0(X) = \prod_{i=1}^m (X - \bar{x}_i)$ and $h_0(X) = \prod_{i=m+1}^n (X - \bar{x}_i)$. Let $g(X) = \prod_{i=1}^m (X - x_i)$ and $h(X) = \prod_{i=m+1}^n (X - x_i)$. Then $\bar{g} = g_0$, $\bar{h} = h_0$ and $f = gh$. It remains to show that $g, h \in O[X]$.

Let σ be an automorphism of L/K. By assumption v has a unique extension w to L. Hence, $O_w^\sigma = O_w$ and $M_w^\sigma = M_w$. So, σ induces an automorphism $\bar{\sigma}$ of $\overline{L}_w/\overline{K}_v$, such that $\bar{\sigma}\bar{u} = \overline{\sigma u}$. For each i between 1 and n there exists j such that $x_i^\sigma = x_j$. If

$i \le m$, then also $j \le m$. Otherwise, $\bar{g}(x_j) = \bar{g}(\bar{x}_i^{\bar{\sigma}}) = \bar{g}(\bar{x}_i)^{\bar{\sigma}} = 0$, and hence $\bar{x}_j$ will be a common root of $\bar{g}$ and $\bar{h}$. But this contradicts the assumption that $\bar{g}$ and $\bar{h}$ are relatively prime. Hence, indeed, $j \le m$.

It follows that $g^\sigma = g$. Likewise $h^\sigma = h$. So, both polynomials have coefficients in a purely inseparable extension of K. If $\mathrm{char}(K) \neq 0$, it has a power q such that $g^q, h^q \in K[X]$. As $\bar{g}$ and $\bar{h}$ are relatively prime, so are g and h and therefore also g^q and h^q. It follows from the equality $f^q = g^q h^q$ and from the unique factorization in $K[X]$ that both g^q and h^q are q-powers of polynomials in $K[X]$. So, $g, h \in K[X]$.

Finally, as the roots of g and h belong to O_w their coefficients belong to O_v, as desired.

Proof of (c) implies (1a): The assumption of (1a) implies that $\bar{f}(X) = (X - a)h_0(X)$ with $a \in \overline{K}$ where $h_0 \in \overline{K}[X]$ is a monic polynomial which does not vanish at a. So, $h_0(X)$ is relatively prime to $X - a$. Hence, by (c), $f(X) = (X - x)h(X)$ with $\bar{x} \in O$, and $\bar{x} = a$. In particular $f(x) = 0$.

Proof of (1a) implies (1b): Let $g(X) = c_n Y^n + \cdots + c_2 Y^2 + c_1 Y + c_0 \in O[X]$ be a plyonomial with $n \ge 1$, $\bar{c}_0, \bar{c}_1 \neq 0$, and $\bar{c}_2 = \cdots = \bar{c}_n = 0$. Set $f(X) = c_0 X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n$. Then $\bar{f}(X) = \bar{c}_0 X^n + \bar{c}_1 X^{n-1} = (\bar{c}_0 X + \bar{c}_1) X^{n-1}$. The element $-\bar{c}_1/\bar{c}_0$ is a simple root of $\bar{f}(X)$. As, $c_0 \in U$, we may therefore apply (1a) to $c_0^{-1} f(X)$ and conclude the existence of $x \in O$ such that $f(x) = 0$ and $\bar{x} = -\bar{c}_1/\bar{c}_0 \neq 0$. Hence $y = x^{-1} \in O$ and $g(y) = x^{-n} f(x) = 0$, as desired.

Proof of (1b) implies (a): Let $f(X)$ be as in (a). If $f(a) = 0$, take $x = a$. Otherwise, $b = f(a) \neq 0$ but $\bar{b} = 0$. Let $g(Y) = b^{-1} f(bY + a)$. Then $g(0) = b^{-1} f(a) = 1$ and $g'(0) = f'(a) \in U$. For $k \ge 2$ we have $g^{(k)}(0) = b^{k-1} f^{(k)}(a) \in M$. Thus $g(Y) \in O[Y]$ and $\bar{g}(Y) = \bar{f}'(\bar{a})Y + 1$. So, (1b) implies the existence of $y \in O$ such that $g(y) = 0$. Obviously $x = by + a$ is then a root of f for which $\bar{x} = \bar{a}$.

Proof of (a) implies (e): Let f and a be as in (e). Then $g(X) = f(X + a) = X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0$ is a monic polynomial with coefficients in O such that

$$v(g(0)) > 2v(g'(0)) + \gamma. \tag{1}$$

This means that $v(c_0/c_1^2) > \gamma \geq 0$. Now consider the polynomial

$$h(X) = \frac{1}{c_1^2} g(c_1 X) = c_1^{n-2} X^n + c_1^{n-3} c_{n-1} X^{n-1} + \cdots + c_2 X^2 + X + \frac{c_0}{c_1^2}.$$

with coefficients in O. It satisfies $\bar{h}(0) = \overline{c_0/c_1^2} = 0$ and $\bar{h}'(0) = 1$. Hence, by (a), there exists $y \in O$ such that $h(y) = 0$ and $\bar{y} = 0$. Then $x = c_1 y + a$ satisfies $f(x) = 0$ and $v(x-a) > v(c_1) = v(g'(0)) = v(f'(a))$.

For $z = x - a$ we have $g(z) = 0$, $v(z) > v(g'(0))$. Thus, there exists $q \in O[X]$ such that $g(X) = (X - z)q(X)$. Hence, $g'(X) = q(X) + (X - z)q'(X)$ and $g'(0) = q(0) - zq'(0)$. Since $v(zq'(0)) \geq v(z) > v(g'(0))$, we have $v(q(0)) = v(g'(0))$. Hence, form $g(0) = -zq(0)$ and from (1) we deduce

$$v(x-a) = v(z) = v(g(0)) - v(q(0)) > 2v(g'(0)) + \gamma - v(g'(0)) = v(g'(0)) + \gamma,$$

as desired.

Proof of (e) implies (1a): Let f and a be as in (1a). Then $v(f(a)) > 0 = 2v(f'(a))$. Hence, by (e), f has a root $x \in a$ such that $v(x-a) > 0$.

Proof of (c) implies (d): Let $f \in O[X]$ be a monic irreducible polynomial. If $\bar{f}$ is not a power of irreducible polynomial in $\overline{K}[X]$, then it decomposes into a product of two monic relatively prime polynomials of positive degree. By (c), f decomposes accordingly in $O[X]$, a contradiction. Hence, $\bar{f}$ is a power of irreducible polynomial in $\overline{K}[X]$.

Proof of (d) implies (c): Let f, g_0, h_0 be as in (c). Decompose f into a product of monic irreducible polynomials in $O[X]$ (Gauss' Lemma), $f = f_1 \cdots f_m$. By (d), each $\bar{f}_i$ is a power of an irreducible polynomial in $\overline{K}[X]$. As g_0 and h_0 are relatively prime, each $\bar{f}_i$ either divides g_0 and is relatively prime to h_0 or divides h_0 and is relatively prime to g_0. Assume without loss that $\bar{f}_1, \ldots, \bar{f}_k$ divide g_0 and $\bar{f}_{k+1}, \ldots, \bar{f}_m$ divide h_0. Then $f_1 \cdots f_k = g_0$ and $\bar{f}_{k+1} \cdots \bar{f}_m = h_0$. Let $g = f_1 \cdots f_k$ and $h = f_{k+1} \cdots f_m$. Then, both g, h are monic polynomials in $O[X]$, $f = gh$, $\bar{g} = g_0$ and $\bar{h} = h_0$, as desired. ∎

Remark: (a) The element x in Proposition 11.1(a) is unique with the given properties. Indeed, if y is another root of f such that $\bar{y} = \bar{a}$, then $\bar{a}$ is a double root of $\overline{f'}$. This contradicts the assumption that $\overline{f'}(\bar{a}) \neq 0$.

(b) The element x in Proposition 11.1(e) is unique with the given properties. Indeed, assume that f has another root $y \in O$ with $v(y-a) > v(f'(a)) + \gamma$. Then $f(X) = (X-x)(X-y)g(X)$ for some $g \in O[X]$. Taken derivatives on both sides, we get $f'(a) = (a-y)g(a) + (a-x)g(a) + (a-x)(a-y)g'(a)$. Hence, $v(f'(a)) > v(f'(a)) + \gamma > v(f'(a))$, which is a contradiction. ∎

Here is an immediate application of Definition 11.1(a):

COROLLARY 11.2: *Let (E,v) a Henselian field and let K be a subfield of E. Then $K_s \cap E$ is Henselian with respect to the restirction of v to it.*

And here is an application of Definition 11.1(b) and Remark 8.4:

COROLLARY 11.3: *A separably closed field E is Henselian with respect to any valuation of itself.*

12. Krasner's lemma.

Let (E,v) be a valued Henselian field. Denote its unique extension to E_s also by v. For each $\sigma \in G(E)$, v^σ is also an extension of v to E_s and therefore, by Definition 11.1(b), $v = v^\sigma$. This means that $v(x^\sigma) = v(x)$ for each $x \in E_s$. As a result we prove in this section that polynomials with coefficients in E whose coefficients are v-close decompose over E in the same way.

LEMMA 12.1 (Krasner): *Let (E,v) be a Henselian valued field. Let $x = x_1, \ldots, x_n$ be a complete set of conjugates of an element $x \in E_s$. If $y \in E_s$ satisfies*

$$v(y-x) > \max_{i \geq 2} v(x_i - x),$$

then $E(x) \subseteq E(y)$.

Proof: Assume that $E(x)$ is not contained in $E(y)$. Then there exists $\sigma \in G(E)$ such that $y^\sigma = y$ but $x^\sigma \neq x$. Hence, $x^\sigma = x_i$ with $i \geq 2$. It follows from the identity $y - x_i = (y-x) + (x-x_i)$ and from $v(y-x) > v(x_i - x)$ that $v(x_i - x) = v(y - x_i) = v(y^\sigma - x^\sigma) = v(y-x) > v(x_i - x)$. Conclude from this contradiction that $E(x) \subseteq E(y)$. ∎

Let (E, v) be a valued field and $f(X) = \sum_{i=0}^{n} a_i X_i$, $g(X) = \sum_{i=0}^{n} b_i X^i$ polynomials in $E[X]$. Then we write $v(f-g) = \min_{0 \le i \le n}\{v(a_i - b_i)\}$. ∎

PROPOSITION 12.2 (Continuity of roots): *Let (E, v) be a valued field and extend v to a valuation of $\widetilde{E}$. Consider a monic polynomial $f \in \widetilde{E}[X]$ of degree n with n roots $x_1, \ldots, x_n \in \widetilde{E}$ such that $x_1, \ldots, x_m$ are the distinct elements of the set $\{x_1, \ldots, x_n\}$. Then, for each $\alpha \in v(\widetilde{E}^\times)$ there exists $\beta \in v(E^\times)$ such that if $g \in \widetilde{E}[X]$ is a polynomial of degree n and if $v(g-f) > \beta$, then the roots of g can be enumerated as $y_1, \ldots, y_n$ such that $v(y_i - x_i) > \alpha$, $i = 1, \ldots, n$. Moreover, $y_1, \ldots, y_m$ are distinct.*

Proof: Since $v(E^\times)$ is cofinal in $v(\widetilde{E}^\times)$ (Corollary 7.2) we may replace E by $\widetilde{E}$, if necessary, to assume tht E is algebraically closed.

The statement of the Proposition is elementary. So, we may use Lemma 10.3 and replace (E, v) by a nonprincipal ultrapower, if necessary, to assume that v is unbounded. Suppose without loss that

$$\alpha > \max_{1 \le i < j \le m}\{v(x_i - x_j)\}. \tag{1}$$

By Lemma 10.1, E has a valuation w which is coarser than v with $w(x_1), \ldots, w(x_n) \ge 0$ and for each $z \in E$

$$w(z) > 0 \quad \text{implies} \quad v(z) > \alpha. \tag{2}$$

In particular $f(X) = \prod_{i=1}^{n}(X - x_i) \in O_w[X]$. By Lemma 3.2, there exists $\beta \in \Gamma_v$ such that

$$v(z) > \beta \quad \text{implies} \quad w(z) > 0. \tag{3}$$

Denote the reduction modulo M_w by a bar.

Suppose now that $g \in E[X]$ is a monic polynomial of degree n such that $v(g-f) > \beta$. By (3), $w(g-f) > 0$. Hence $g \in O_w[X]$ and $\bar{g} = \bar{f}$. So, the roots of g can be enumerated as $y_1, \ldots, y_n$ such that $\bar{y}_i = \bar{x}_i$, $i = 1, \ldots, n$. This means that $w(y_i - x_i) > 0$ and therefore, by (2), $v(y_i - x_i) > \alpha$, $i = 1, \ldots, n$. Conclude from (1) that $y_1, \ldots, y_m$ are distinct. ∎

It is often useful to combine Krasner's lemma and the proposition about the continuity of roots:

PROPOSITION 12.3: *Let (E, v) be a Henselian valued field. Consider a monic polynomial $f \in E[X]$ of degree n with n distinct roots $x_1, \ldots, x_n$. Then for each $\alpha \in \Gamma_v$ there exists $\gamma \in \Gamma_v$ such that the following holds: If $g \in E[X]$ is a monic polynomial of degree n with $v(g-f) > \gamma$, then the roots of g are distinct and can be enumerated as $y_1, \ldots, y_n$ such that $v(y_i - x_i) > \alpha$ and $E(x_i) = E(y_i)$. In particular the splitting fields of f and g coincide and therefore they have the same Galois groups over E. Also, $f(X)$ and $g(X)$ factor over E in the same way: $f(X) = \prod_{j=1}^{m} f_j(X)$, $g(X) = \prod_{j=1}^{m} g_j(X)$, where $f_j, g_j \in E[X]$ are irreducible and $\deg(f_j) = \deg(g_j)$. In particular, if f is irreducible over E, then so is g.*

Moreover, if K is algebraic over a subfield K_0, then γ can be chosen in $v(K_0^\times)$.

Proof: Suppose without loss that

$$\alpha > \max_{i \neq j} \{v(x_i - x_j)\}. \tag{5}$$

Choose $\gamma \in v(E_s^\times)$ as in Proposition 12.2. Thus, if $g \in E[X]$ is a polynomial of degree n such that $v(g - f) > \gamma$, then the roots of g are distinct and can be enumerated as $y_1, \ldots, y_n$ such that

$$v(y_i - x_i) > \alpha, \qquad i = 1, \ldots, n. \tag{6}$$

In particular $y_1, \ldots, y_n$ are separable over E. Moreover, for each i, y_i is the unique root of g that satisfies (6). If $x_j = x_i^\sigma$, for some $\sigma \in G(E)$, then $v(y_i^\sigma - x_j) = v((y_i - x_i)^\sigma) = v(y_i - x_i) > \alpha$. So, by the uniqueness, $y_i^\sigma = y_j$. Thus, y_i has at least as many conjugates over E as x_i has. As this holds for each i, y_i and x_i have the same number of conjugates over E. In other words, $[E(y_i) : E] = [E(x_i) : E]$. By Lemma 12.1 and by (5), $E(x_i) \subseteq E(y_i)$. Hence $E(x_i) = E(y_i)$. It follows that the splitting field $E(y_1, \ldots, y_n)$ of g over E coincides with the splitting field $E(x_1, \ldots, x_n)$ of f over E.

Let now $f(X) = \prod_{j=1}^{m} f_j(X)$ be the factorization of $f(X)$ into a product of irreducible factors over E. For each j let $f_j(X) = \prod_{i \in I_j} (X - x_i)$. Then $\{x_i |\ i \in I_j\}$ is a complete system of conjugates over E. By the preceding paragraph $\{y_i |\ i \in I_j\}$ is also a complete system of conjugates over E. Hence $g_j(X) = \prod_{i \in I_j} (X - y_i)$ is irreducible of the same degree as f_j, and $g(X) = \prod_{j=1}^{m} g_j(X)$.

Finally if E is algebraic over a field K, then $v(K^\times)$ is cofinal in $v(\widetilde{E}^\times)$ (Corollary 7.2). Hence we may choose γ in $v(K^\times)$. ∎

13. A theorem of F.K. Schmidt.

Suppose that v and w are valuations of a field K such that v is finer than w. Use the notation of Section 3. In particular $\bar{x}$ denotes the reduction of an element $x \in O_w$ modulo M_w.

PROPOSITION 13.1: *The valued field (K, v) is Henselian if and only if both (K, w) and $(\overline{K}_w, \bar{v})$ are Henselian.*

Proof: Suppose first that (K, v) is Henselian. We prove that $(\overline{K}_w, \bar{v})$ is Henselian. Indeed, let $f_0 \in O_{\bar{v}}[X]$ be a monic polynomial and let $a_0 \in O_{\bar{v}}$ such that $\bar{v}(f_0(a_0)) > 0$ and $\bar{v}(f_0'(a_0)) = 0$. If $f_0(a_0) = 0$, then we are done.

So, assume that $f_0(a_0) \neq 0$. Then there exists a monic polynomial $f \in O_v[X]$ and an element $a \in O_v$ such that $\bar{f} = f_0$ and $\bar{a} = a_0$. Hence, $\overline{f(a)} = f_0(a_0)$, $\overline{f'(a)} = f_0'(a_0)$, and therefore both $f(a)$ and $f'(a)$ belong to U_w. It follows that $v(f(a)) = \bar{v}(f_0(a_0)) > 0$ and $v(f'(a)) = \bar{v}(f_0'(a_0)) = 0$. By Hensel's lemma (Definition 11.1(e)), there exists $x \in O_v$ such that $f(x) = 0$ and $x = a + b$ with $b \in M_v$. Hence $f_0(\bar{x}) = 0$ and $\bar{x} = \bar{a} + \bar{b}$ with $\bar{b} \in M_{\bar{v}}$. Conclude that $(\overline{K}_w, \bar{v})$ is Henselian.

Now we use Definition 11.1(b) to prove that (K, w) is Henselian. Let L be a seaparable algebraic extension. Suppose that w' and w'' are extensions of w to L. By Lemma 9.4(b), v extends to valuations v' and v'' of L which are respectively finer than w' and w''. As (K, v) is Henselian, $O_{v'} = O_{v''}$. Hence, by Lemma 3.2, w' and w'' are comparable. It follows from Corollary 6.7 that $O_{w'} = O_{w''}$. Conclude that (K, w) is Henselian.

Now suppose that (K, w) and $(\overline{K}_w, \bar{v})$ are Henselian and use Hensel's lemma to prove that (K, v) is Henselian.

So, consider a monic polynomial $f \in O_v[X]$ and an element $a \in O_v$ such that $v(f(a)) > 0$ and $v(f'(a)) = 0$. Then $w(f(a)) \geq 0$ and $w(f'(a)) = 0$. There are two cases to consider:

CASE A: $w(f(a)) > 0$. As (K, w) is Henselian, there exists $x \in O_w$ such that $f(x) = 0$ and $w(x - a) > 0$. Hence, also $v(x - a) > 0$.

CASE B: $w(f(a)) = 0$. Then $\bar{v}(\bar{f}(\bar{a})) = v(f(a)) > 0$ and $\bar{v}(\bar{f}'(\bar{a})) = v(f'(a)) = 0$. As $(\overline{K}_w, \bar{v})$ is Henselian, there exists $y \in O_v$ such that $\bar{f}(\bar{y}) = 0$ and $\bar{v}(\bar{y} - \bar{a}) > 0$. It follows that $v(y - a) > 0$ and $\bar{f}'(\bar{y}) \neq 0$. As (K, w) is Henselian, there exists $x \in O_w$ such that $f(x) = 0$ and $w(x - y) > 0$. Hence $v(x - y) > 0$ and therefore $v(x - a) > 0$. The latter inequality also implies that $x \in O_v$.

Conclude that (K, v) is Henselian. ∎

The following result and its consequences were originally proved by F.K. Schmidt [S] for valuation of rank 1. Engler [E] generalized them to valuations of arbitrary rank.

LEMMA 13.2: *If a field K which is not separably closed is Henselian with respect to two valuations v and v', then v and v' are dependent.*

Proof: By assumption there exists a monic separable irreducible polynomial $f \in K[X]$ of degree $n > 1$. Let $g(X) = (X - a_1) \cdots (X - a_n)$, where $a_1, \ldots, a_n$ are distinct elements of K (as a valued field K must be infinite). If v and v' were independent, then by the weak approximation theorem (Proposition 4.4) there would exists a monic polynomial $h \in K[X]$ of degree n which is arbitrarily v-close to f and arbitrarily v'-close to g. In particular, by Krasner's Lemma (Proposition 12.3), we would be able to choose h such that its splitting field over K coincides on one hand with that of f and on the other hand with that of g. Howerver, the latter field is K while the former one is a proper extension of K. This contradiction proves that v and v' are dependent. ∎

REMARK 13.3: *Valuations of rank 1.* If v and v' are inequivalent valuations of K of rank 1, then they are also independent. Thus, a special case of Lemma 13.2 says that a non separably closed field K cannot be Henselian with respect to inequivalent valuations v and v' of rank 1. This is the original theorem of F.K. Schmidt. The following result supplies more information about valuations of higher rank. ∎

PROPOSITION 13.4: *If a field K which is not separably closed is Henselian with respect to incomparable valuations v and v', then $\overline{K}_v$ and $\overline{K}_{v'}$ are separably closed. Moreover,*

K has a valuation w with a separably closed residue field such that $O_v, O_{v'} \subseteq O_w$.

Proof: By Lemma 13.2, v and v' are dependent valuation. Hence the ring O generated by O_v and $O_{v'}$ is properly contained in K. It is therefore the valuation ring O_w of a valuation w of K. The residue field $\overline{K}_w$ is obviously generated by the valuations rings $O_{\bar{v}} = O_v/M_w$ and $O_{\bar{v}'} = O_{v'}/M_w$ of the corresponding valuations $\bar{v}$ and $\bar{v}'$ of $\overline{K}_w$. This means that $\bar{v}$ and $\bar{v}'$ are independent. By Proposition 13.1, both $(\overline{K}_w, \bar{v})$ and $(\overline{K}_w, \bar{v}')$ are Henselian. Hence, by Lemma 13.2, $\overline{K}_w$ is separably closed. As $\overline{K}_v$ and $\overline{K}_{v'}$ are residue fields of $\overline{K}_w$ they are also separably closed. ∎

PROPSITION 13.5: *Let $(L, w)/(K, v)$ be a Galois extension of valued fields. Suppose that (L, w) is Henselian and its residue field $\overline{L}_w$ is not separably closed. Then (K, v) is Henselian.*

Proof: Since w has a unique extension to each algebraic extension of K it suffices to prove that w is the unique extension of v to L. Assume that w' is an extension of v to L which is inequivalent to w. Then w' is conjugate to w over K (Proposition 8.1) and therefore L is also Henselian with respect to w'. By Corollary 6.7, w and w' are incomparable.

As $\overline{L}_w$ is not separably closed, so is L. By Proposition 13.4, L has a valuation u with a separably closed residue field $\overline{L}_u$ such that $O_w, O_{w'} \subseteq O_u$. Let $\bar{w}$ be the valuation of L_u that corresponds to the valuation ring O_w/M_u of L_u. Then the residue field of $\bar{w}$ which is equal to $\overline{L}_w$ is separably closed. Conclude from this contradiction to the assumption of the proposition that the assumption about the existence of w' is false. ∎

REMARK 13.6: *Valuations of rank 1.* If $\text{rank}(w) = 1$, then it suffices to assume in Proposition 13.5 that L is not separably closed. Indeed, replace Proposition 13.4 in the proof of Proposition 13.5 by Remark 13.3 to obtain the stronger result. ∎

14. Henselization of a valued field.

Definition 11.1(b) allows us to construct the "Henselian closure" of a valued field:

PROPOSITION 14.1: *Each valued field (K,v) has a separable algebraic extension (K_v^h, v^h) with the following properties:*

(a) *(K_v^h, v^h) is Henselian,*

(b) *If (L,w) is a Henselian extension of (K,v) then (K_v^H, v^h) can be embedded in (L,w) over K.*

The valued field (K_v^h, v^h) is unique up to K-isomorphism. It is the **Henselization** *of (K,v).*

Proof: Let v_s be an extension of v to K_s. Denote the decomposition field of v_s over K by K_v^h and let v^h be the restriction of v_s to K_v^h. By Corollary 8.3, v^h has a unique extension to each algebraic extension of K_v^h. Hence, by Definition 11.1(b), (K_v^h, v^h) is Henselian.

Next, suppose that (L,w) is a Henselian extension of (K,v). Use Corollary 11.2 and replace L if necessary by $K_s \cap L$ to assume that L/K is separable algebraic. Then extend w to a valuation w_s of K_s. As both v_s and w_s extend v there exists $\sigma \in G(K)$ such that $v_s^\sigma = w_s$ (Corollary 8.2). The automorphism σ maps (K_v^h, v^h) onto a valued field (K', v') such that w_s extends v' and K' is the decomposition field of w_s over K.

As (L,w) is Henselian, $w_s^\tau = w_s$ for each $\tau \in G(L)$. Hence $\tau \in G(K')$. Conclude that $K' \subseteq L$. Since w is the restriction of w_s to L and v' is the restriction of w_s to K' conclude that v' is the restriction of w to K'.

These completes the proof of (a) and (b). To prove the uniqueness of (K_v^h, v^h) suppose that (L,w) above satisfies both (a) and (b). Apply an approperiate automorphism on (L,w) to assume that it is a subvalued field of (K_v^h, v^h). As in the preceding paragraph one proves that each $\tau \in G(L)$ belongs to $G(K_v^h)$. Hence $(L,w) = (K_v^h, v^h)$, and the proof is completed. ∎

The proof of Proposition 14.1 identifies the Henselization of a valued field (K,v) as the decomposition field over K of an extension v_s of v to K_s. So, the following result is a special case of Corollary 8.6:

COROLLARY 14.2: *The Henselization (K^h, v^h) of a valued field (K, v) is an immediate extension.*

COROLLARY 14.3: *In the notation of Corollary 14.2 let $x \in K^h$, $x \neq 0$. Then there exists $a \in K$ such that $v(x-a) > v(x)$. Moreover, the later inequality is equivalent to $v(x-a) > v(a)$.*

Proof: Since $v(K_v^h) = v(K)$ (Corollary 14.2), there exists $b \in K^\times$ such that $v(x) = v(b)$. As $\overline{K}_v{}^h = \overline{K}_v$ (Corollary 14.2), there exists $c \in K$ such that $v(\frac{x}{b} - c) > 0$. Take $a = bc$ and observe that $v(c) = 0$. Hence $v(a) = v(b)$ and therefore $v(x-a) > v(a)$. Conclude that $v(x) = v(a)$ and $v(x-a) > v(x)$. ∎

Likewise the following result is a special case of Proposition 9.5:

COROLLARY 14.4: *Let v and w be valuations of a field K such that v is finer than w. Then K_w^h can be embedded in K_v^h over K.*

Proof: Use Lemma 9.4 to extend v and w to valuations v_s and w_s, respectively, of K_s such that v_s is finer than w_s. Then apply Proposition 9.5 on v_s, w_s, and K_s instead of v, w, and L to conclude the proof. ∎

The Henselization of a field is rigid over the field:

PROPOSITION 14.5: *Let (K^h, v^h) be the Henselization of a valued field (K, v). If $\overline{K}_v$ is not separably closed, then K^h/K has no automorphism ecxept the identity.*

Proof: If $\mathrm{Aut}(K^h/K)$ were nontrivial, then K^h would be Galois over a proper subfield E which contains K. By Proposition 14.2, the residue field of K^h with respect to v^h is $\overline{K}_v$. So it is not separably closed. By Proposition 13.5, E is Henselian with respect to the restriction w of v^h to E. Hence, there exists a K-isomorphism τ of K^h such that $\tau(K^h) \subseteq E$.

So, for each $x \in E$, τ maps the set of zeros of $\mathrm{irr}(x, K)$ contained in K^h injectively into the set of zeros of $\mathrm{irr}(x, K)$ contained in E. But since the later map is contained in the former, this set is bijective. In particular $x \in E$. Hence $K^h = E$, a contradiction. ∎

REMARK 14.6: *Valuations of rank 1.* If $\text{rank}(v) = 1$, then the use of Proposition 13.5 in the proof of Proposition 14.5 can be replaced by the use of Remark 13.6. So, in this case, we can replace the condition "$\overline{K}_w$ is not separably closed" in Proposition 14.5 by the weaker one "L is not separably closed".

15. Real Closures of a field.

An **ordering** of a field K is a binary relation $<$ on K which satisfies the usual conditions for inequality:

(1a) For each $x, y \in K$, either $x < y$, or $x = y$, or $y < x$.

(1b) If $x < y$ and $y < z$, then $x < z$.

(1c) If $x < y$, then for each $z \in K$ we have $x + z < y + z$ and if $0 < z$, then also $xz < yz$.

We call the pair $(K, <)$ an **ordered field**.

It is easy to deduce from these conditions all other rules for inequality like "$x < y$ implies $-x > -y$", etc. In particular, the **positive cone** $P = \{x \in K |\ x > 0\}$ satisfies:

(2a) K is the disjoint union of $-P$, $\{0\}$, and P, and

(2b) $x, y \in P$ implies that $x + y, xy \in P$.

In particular $x < y$ if and only if $y - x \in P$. So P determines $<$.

Observe that for each positive integer n the sum of n times 1 is $1^2 + \cdots + 1^2$. It belongs to P and is therefore not 0. Thus $\text{char}(K) = 0$.

Observe also, that -1 is not the sum of squeres in K. A field K which satisfies the latter property is **formally real**. Such a field admits an ordering. Indeed, the set S of sum of squeres in K satisfies:

(3a) $S \cap -S = \emptyset$, and

(3b) If $x, y \in S$, then $x^{-1}, x + y, xy \in S$.

By Zorn's lemma there exists a maximal set P which contains S and satisfies (3). If $x \in K$, $x \neq 0$, and $-x \notin P$, then the set

$$P' = \left\{ \frac{a + bx}{c + dx} \middle|\ a, b, c, d \in P \cup \{0\},\ (a, b) \neq (0, 0),\ (c, d) \neq (0, 0) \right\}$$

contains P and satisfies (3). Hence $P' = P$ and therefore $x \in P$. Conclude that P is the positive cone of an ordering of K.

A field K is **real closed** if it is formally real but no proper algebraic extension of K is formally real.

PROPOSITION 15.1: (a) ([L, p. 274]) *If R is a real closed field, then the set of all nonzero squeres is the positive cone of the unique ordering of R. Moreover, $\widetilde{R} = R(\sqrt{-1})$.*

(b) (Artin [L, p. 194]) *If a field R is not separably closed and $[R_s : R] < \infty$, then R is real closed.*

COROLLARY 15.2: *Let $(L, w)/(K, v)$ be a finite separable extension of valued fields. Suppose that (L, w) is Henselian and $\overline{L}_w$ (resp., L) is neither separably closed nor real closed (resp., if* $\mathrm{rank}(v) = 1$*). Then (K, v) is Henselian.*

Proof: Let N be the Galois closure of L/K. Denote the unique extension of w to N by w. Then (N, w) is Henselian, and N/K is a finite Galois extension. By Proposition 13.5, (K, v) is Henselian unless $\overline{N}_w$ (resp., N) is separably closed. As $[\overline{M}_w : \overline{L}_w] \leq [M : L] < \infty$ (Lemma 7.1), Proposition 15.1 would imply that $\overline{L}_w$ (resp., L) is either separably closed or real closed, in contrast to our assumption. ∎

COROLLARY 15.3: *Let (K, v) be a valued field such that $\overline{K}_v$ (resp., K) is neither separably closed nor real closed. Then K_v^h is a proper finite extension of no field E which contains K.*

Proof: By Proposition 14.1, K^h/K is a separable algebraic extension. Also, $\overline{K_v^h} = \overline{K}_v$ (Corollary 14.2). So, if E is a field such that $K \subseteq E \subset K_v^h$ and $[K_v^h : E] < \infty$, then E is Henselian with respect to the restriction of v^h to E. But then K_v^h could be K-embedded in E. As in the second paragraph of the proof of Proposition 14.5, this would lead to a contradiction. Conclude that such an E does not exist. ∎

As usual, we associate an **absolute value** to an ordering $<$ of a field K: $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. The ordering induces a topology on R whose basic open sets are the open intervals $\{x \in R |\ |x - a| < c\}$, with $a, c \in R$ and $c > 0$. This topology naturally extends to $\widetilde{R}$.

The point of view of topology offers an analogy between orderings and valuations. Thus we may consider the unit disc $O_< = \{x \in K| \ |x| \leq 1\}$ as the analog of the valuation ring O_v of a valuation v. Likewise, the open unit disc $M_< = \{x \in K| \ |x| < 1\}$ may be taken as the analog of the maximal ideal M_v of O_v. However, $O_<$ is not a ring. So, the analogy between valuations and orderings should be done with cautious.

Although real closed fields behave in many respects as Henselian fields, the analog of Krasner's lemma (Lemma 12.1) does not hold for real closed fields. Indeed, take a positive element c in R, $y = 0$ and $x = c\sqrt{-1}$. Then $\bar{x} = -c\sqrt{-1}$ is the only conjugate of x over R, $|y - x| = c$, $|x - \bar{x}| = 2c$ but $R(x) = \widetilde{R}$ is not conained in $R(y) = R$.

Nevertheless, due to Sturm's algorithm, consequences of Krasner's lemma do hold:

The **Sturm sequence** of a polynomial $f \in R[X]$ is the sequence $\{f, f', f_2, \ldots, f_m\}$ defined by the Euclidean algorithm:

$$\begin{aligned} f &= q_1 f' - f_2 \qquad \deg(f_2) < \deg(f') \\ f' &= q_2 f_2 - f_3 \qquad \deg(f_3) < \deg(f_2) \\ &\ldots \\ f_{m-2} &= q_{m-1} f_{m-1} - f_m \qquad \deg(f_m) < \deg(f_{m-1}) \\ f_{m-1} &= q_m f_m. \end{aligned}$$

For each $x \in R$ which a root of none of the polynomials in the Sturm's sequence we denote the number of variations of signs in the sequence $\{f(x), f'(x), f_2(x), \ldots, f_m(x)\}$ by $w_f(x)$.

PROPOSITION 15.4 (Sturm [L, p. 276]): *Let R be a real closed field, let $f \in R[X]$, and let $a < b$ be elements which are roots of no polynomial in the Sturm sequence of f. Then the number of roots of f in the interval $[a, b]$ is $w(a) - w(b)$.*

We write $|g - f| < \varepsilon$ for two polynomials $f, g \in R[X]$ if the absolute values of the difference of their respective coefficients are less than ε.

LEMMA 15.5: *Let R be a real closed field and $f \in R[X]$ be a nonzero monic polynomial of degree n. Then there exists $0 < \varepsilon \in R$, such that each monic polynomial $g \in R[X]$*

of degree n which satisfies $|f - g| < \varepsilon$ has the same number of roots in R as f. In particular, f and g factor in the same manner in $R[X]$.

Proof: Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ and let c be an upper bound on $|a_0|, \ldots, |a_{n-1}|$ such that $c > 1$. If $x \in R$ is a root of f, then $|x| \leq 2nc$. Otherwise $x^n = -(a_{n-1}x^{n-1} + \cdots + a_0)$, hence $1 = -(a_{n-1}x^{-1} + \cdots + a_0x^{-n})$, and therefore $1 \leq |a_{n-1}||x^{-1}| + \cdots + |a_0||x^n| \leq nc \cdot \frac{1}{2cn} = \frac{1}{2}$, a contradiction.

Next note that the coefficients of the polynomials in the Sturm sequence of f are rational functions of its coefficients whose denominators are bounded powers of n. Hence, they are continuous functions of $a_{n-1}, \ldots, a_0$. So, if g is a monic polynomial of degree n which is close enough to f, then the elements of its Sturm sequence are respectively close to those of f. In particular, the absolute value of the coefficients of g will be at most $2c$. By the preceding paragraph all the roots of g will lie in the interval $[-4nc, 4nc]$. Also, $w_g(-4nc) = w_f(-4nc)$ and $w_g(4nc) = w_f(4nc)$. Conclude from Sturm's theorem (Proposition 15.4) that g has the same number of roots in the interval $[-4nc, 4nc]$ and therefore in R as f. ∎

An ordered field $(L, <')$ is an **extension** of $(K, <)$ if $K \subseteq L$ and if the relation $<'$ extends $<$. If L is real closed and algebraic over K, then we say that it is a **real closure** of K. If in this case $<'$ extends $<$, we also say that L is a **real closure** of $(K, <)$.

PROPOSITION 15.6 ([L, p. 277]): *Each valued field $(K, <)$ has a real closure $\overline{K}$. If K' is another real closure of $(K, <)$, then there exists a unique K-isomorphism $\sigma\colon \overline{K} \to K'$. In particular* $\mathrm{Aut}(\overline{K}/K) = 1$.

16. Nonarchimedean orderings.

An ordering $<$ of a field K is **archimedean** if for all $a, b > 0$ there exists a positive integer n such that $na > b$. For a valuation v of K, we say that v is **coarser** than $<$ if for each $x \in K$

$$v(x) > 0 \text{ implies } |x| < 1. \tag{1}$$

With $O_< = \{x \in K | \ |x| \leq 1\}$ (which is the analog of O_v) this condition is equivalent to $O_< \subseteq O_v$. So, the relation "coarser" between a valuation and an ordering is the analog of the same relation between valuations. This analogy goes further with the following analog of Corollary 14.4:

LEMMA 16.1: *Let $(K, <)$ be an ordered field. Suppose that v is a valuation of K which is coarser than $<$. Then* $\mathrm{char}(\overline{K}_v) = 0$ *and $<$ is nonarchimedean. Moreover, $<$ extends to an ordering of K_v^h.*

Proof: As an ordered field, K must have characteristic 0. If $\mathrm{char}(\overline{K}_v) = p$, then $\bar{p} = 0$, hence $v(p) > 0$, and therefore, by (1), $|p| < 1$. On the other hand, the restriction of $<$ to $\mathbb{Q}$ is the usual ordering, for which $p > 1$. This contradiction proves that $\mathrm{char}(\overline{K}_v) = 0$.

To extend $<$ to K_v^h consider $x \in K_v^h$, $x \neq 0$. Use Corollary 13.3 to choose $a \in K$ such that

$$v(x - a) > v(x) = v(a). \tag{2}$$

Define

$$x >' 0 \text{ if and only if } a > 0. \tag{3}$$

If a' is another element of K that satisfies $v(x - a') > v(x) = v(a')$, then $v(a - a') \geq \min\{v(a - x), v(x - a')\} > v(x) = v(a')$. Hence $v(\frac{a}{a'} - 1) > 0$, and therefore, by (1), $\left|\frac{a}{a'} - 1\right| < 1$. Thus $|a - a'| < |a'|$. If, say, $a' > 0$, then $a = a' + (a - a') \geq a' - |a - a'| > 0$. It follows that definition (3) is independent of the a satisfying (2).

Obviously, for each $x \in K$, either $x <' 0$, or $x = 0$, or $x >' 0$. Also, if $x \in K$, then $x >' 0$ if and only if $x > 0$. So, to conclude the proof that $<'$ is an ordering of K_v^h it suffices to prove that if $x, y \in K_v^h$ satisfy $x, y >' 0$, then $x + y >' 0$ and $xy >' 0$.

Indeed, let a be as in (2) with $a > 0$ and take $b \in K$ such that

$$v(y-b) > v(y) = v(b) \text{ and } b > 0. \tag{4}$$

Suppose that $v(a) \leq v(b)$. Then $v(a+b) = v(a)$. Otherwise $v(a+b) > v(a)$ and hence $v(1+\frac{b}{a}) > 0$. By (1), $\left|1+\frac{b}{a}\right| < 1$. Hence $a = |a| > |a+b| \geq a+b$ and therefore $b < 0$. This contradicts (4). It follows that

$$v((x+y)-(a+b)) \geq \min\{v(x-a), v(y-b)\} > \min\{v(a), v(b)\} = v(a+b)$$

and therefore $v((x+y)-(a+b)) = v(x+y)$. As $a+b > 0$, the defition of $<'$ gives that $x+y >' 0$, as desired.

Also, use the identity $xy - ab = x(y-b) + (x-a)b$ to compute:

$$\begin{aligned} v(xy-ab) &\geq \min\{v(x)+v(y-b),\ v(x-a)+v(b)\} \\ &> \min\{v(x)+v(y),\ v(x)+v(y)\} = v(xy). \end{aligned}$$

Conclude that $xy >' 0$, as desired. ∎

LEMMA 16.2: *Let $<$ be a nonarchimedean ordering of a field K. Then K has a valuation v which is coarser than $<$ and $(K,<)$ has a real closure $\overline{K}$ which contains K_v^h.*

Proof: Let

$$O = \{x \in K |\ \exists n \in \mathbb{N}\colon |x| \leq n\}$$

$$M = \{x \in K |\ \forall m \in \mathbb{N}\colon |mx| < 1\}, \text{ and}$$

$$U = \{x \in K |\ \exists n \in \mathbb{N}\colon n^{-1} < |x| < n\}.$$

Then O is a nontrivial valuation ring of K, M is its maximal ideal, and U is the group of units of O. The valuation of K that corresponds to O satisfies (1) and is therefore finer than v. By Lemma 16.1, $<$ extends to an ordering $<$ of K_v^h. Any real closure $\overline{K}$ of $(K_v^h, <)$ is a real closure of $(K,<)$. ∎

REMARK 16.3: *Comparing topologies.* If a valuation v is coarser than an ordering $<$ of a field K, then the the v-topology of K coincides with the $<$-topology of K. Indeed, for each $a \in K^\times$, $v(x) > v(a)$ implies $|x| < |a|$. Conversely, let $b \in K^\times$ such that $v(b) > 0$. Then $|x| < |ab|$ implies $v(x) > v(a)$. Otherwise, $v(x) \leq v(a)$, hence

$v(x) < v(ab)$, and therefore $|x| > |ab|$, a contradiction. Conclude that both topologies have the same neighborhoods of zero and therefore they coincide. The following lemma implies that, unlike with valuations, also the converse is true. We therefore say that a valuation v and an an ordering $<$ of a field K are **independent** if there exists $x \in K$ such that $v(x) > 0$ and $x \geq 1$. ∎

Lemma 16.1 says that an archimedean ordering can never depend on a valuation. Lemma 16.2, on the other hand, says that each nonarchimedean ordering depends on some valuation.

LEMMA 16.4: *Every nonprincipal ultrapower $(K^*, <^*)$ of an ordered field (K, v) is nonarchimedean.*

Proof: Apply Lemma 10.2 on the field K, considered as an ordered group to get an element $x \in K^*$ which is greator than each $n \in \mathbb{N}$. In particular $<^*$ is a nonarchimedean ordering of K^*. ∎

For a polynomial $f = \sum_{i=0}^{n} a_i X^i$ we set $|f| = \max_{0 \leq i \leq n} |a_i|$.

PROPOSITION 16.5 (CONTINUITY OF ROOTS): *Let $f \in \mathbb{C}[X]$ be a monic polynomial of degree n with roots $x_1, \ldots, x_n$. Then, for each $\varepsilon > 0$, there exists $\delta \in \mathbb{R}$, $\delta > 0$, such that the following holds: If $g \in \mathbb{C}[X]$ is a monic polynomial of degree n such that $|g - f| < \delta$, then the roots of g can be neumerated as $y_1, \ldots, y_n$ such that $|y_i - x_i| < \varepsilon$, $i = 1, \ldots, n$.*

Proof: Consider a nonprincipal ultrapower $C = \mathbb{C}^N/\mathcal{D}$. It is an algebraically closed field with absolute value $|\ |$. As in Lemma 16.2, $O = \{x \in \mathbb{C} |\ \exists n \in \mathbb{N}\colon |x| \leq n\}$ is a nontrivial valuation ring of C. Let v be the corresponding valuation. As in Remark 16.3, v and $|\ |$ induce the same topology on C.

Since C is algebraically closed, the proposition follows for C from the continuity of roots of polynomials over algebraically closed fields with respect to valuations (Proposition 12.2). Since the statement of the proposition is elementary, it also holds for $\mathbb{C}$. ∎

REMARK 16.6: *A topological proof.* One may replace the use of logic in the proof of

Proposition 16.5 by the use of topology. Indeed, the symmetric group S_n acts on the space $\mathbb{C}^n$ by permuting the coordinates and the quotient space $X = \mathbb{C}^n/S_n$ is locally compact and Hausdorff. The map $(x_1, \ldots, x_n) \mapsto (a_1, \ldots, a_n)$ of $\mathbb{C}^n$ onto $\mathbb{C}^n$, where $a_k = (-1)^k p_k(x_1, \ldots, x_n)$ and p_k is the fundamental symmetric polynomial of degree k, induces a continuous bijection $\varphi\colon X \to \mathbb{C}^n$. One proves that if $(a_1, \ldots, a_n)$ ranges over a bounded set of $\mathbb{C}^n$, so does $(x_1, \ldots, x_n)$. It follows that $\varphi^{-1}(C)$ is compact for each compact subset of $\mathbb{C}^n$. Since $\mathbb{C}^n$ is a Hausdorff locally compact space, this implies that φ is a **proper map** [Bou, Proposition I.10.3.7, p. 104]. It follows that for each closed subset C of X its image $\varphi(C)$ is also closed [Bou, Proposition I.10.1.1, p. 98]. Hence, φ^{-1} is continuous. One therefore concludes the topological proof of Proposition 16.5 from the relation $\prod_{i=1}^{n}(X - x_i) = X^n + a_1 X^{n-1} + \cdots + a_n$. ∎

PROPOSITION 16.7: *Let R be a real closed field and let $f \in R[X]$ be a monic separable polynomial of degree n. Then there exists $\delta \in R$, $\delta > 0$, such that if a monic polynomial $g \in R[X]$ of degree n satisfies $|g - f| < \delta$, then f and g factor in $R[X]$ in the same way.*

Proof: Since R is elementary equivalent to $\mathbb{R}$ [P, Corollary 5.3], we may assume that $R = \mathbb{R}$. Let $x_1, \ldots, x_r$ be the real roots of f and let $z_1, \bar{z}, \ldots, z_s, \bar{z}_s$ be the nonreal roots of f. Thus, $n = r + 2s$. Choose $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ such that $\varepsilon < \frac{1}{2}|x - x'|$ for each pair (x, x') of distinct roots of f and $\varepsilon < |\mathrm{Im}(z)|$ for every nonreal roots z of f. Let δ be given as in Proposition 16.5.

Suppose that $g \in \mathbb{R}[X]$ is a monic polynomial of degree n such that $|g - f| < \delta$. Then, for each root x of f the polynomial g has a root y with $|y - x| < \varepsilon$. By the choice of ε, g has a least $2s$ nonreal roots. Also, for each $1 \leq i \leq r$, g has a root y_i such that $|y_i - x_i| < \varepsilon$. By the choice of ε, $y_1, \ldots, y_r$ are distinct. If for some i, y_i were nonreal, then $\bar{y}_i$ would be an additional root of g. This wold mean that g has more that n roots. Conclude from this contradiction that $y_1, \ldots, y_r$ are real. Hence, g has exactly $2s$ nonreal roots. So, f and g factor over $\mathbb{R}$ in the same way. ∎

17. Weak approximation theorems for valuations and orderings.

The main result of this work uses only approximation of zero. This puts no resriction on the valuations and orderings involved.

PROPOSITION 17.1: *Let $S = \{v_1, \dots, v_m, <_1 \dots, <_n\}$ be a set of valuations and orderings of a field K. Consider $\alpha_i \in \Gamma_{v_i}$, $i = 1, \dots, m$, $a \in K$, and $c_j \in K$ such that $c_j >_j 0$, $j = 1, \dots, n$. Then*

(a) *there exists $x \in K$, $x \neq a$, such that $v_i(x-a) \geq \alpha_i$, $i = 1, \dots, m$, and $|x-a| <_j c_j$, $j = 1, \dots, n$, and*

(b) *there exists $y \in K^\times$ such that $y < \alpha_i$, $i = 1, \dots, m$ and $y >_j c_j$, $j = 1, \dots, n$.*

Proof: If x saisfies (a), then $y = (x-a)^{-1}$ satisfies (b). If $z \in K^\times$ satisfies

$$v_i(z) > \alpha_i,\ i = 1, \dots, m, \qquad |z| <_j c_j,\ j = 1, \dots, n, \tag{1}$$

then $x = z + a$ satisfies (a). We prove the existence of z in two parts. Assume without loss that $\alpha_i > 0$, $i = 1, \dots, m$.

PART A: *$v_1, \dots, v_m$ are independent and $<_1, \dots, <_n$ are archimedean.* By the weak approximation theorem (Lemma 4.3), there exists $b \in K$ such that $v_i(b) < -\alpha_i$, $i = 1, \dots, m$. Then $v_i(\frac{1}{1+b^2}) > 2\alpha_i$, $i = 1, \dots, m$, and $|\frac{1}{1+b^2}| <_j 1$. As $<_j$ is archimedean, there exists k such that $|(\frac{1}{1+b^2})^k| <_j c_j$. So, $z = (1+b^2)^{-k}$ satisfies (1).

PART B: *Reduction step.* Suppose that a valuation w of K is comparable with some v_i (resp., $<_j$). By Lemma 3.2 (resp., the remark that proceeds Lemma 15.2), for each $\alpha \in \Gamma_w$ there exists $\beta \in \Gamma_{v_i}$ (resp., $c \in K$, $c >_j 0$) such that $w(z) > \beta$ implies $v_i(z) > \alpha$ (resp., $|z| <_j c$). Also, for each $\beta \in \Gamma_{v_i}$ (resp., $c \in K$, $c >_j 0$) there exists $\alpha \in \Gamma_w$ such that $v_i(z) > \alpha$ (resp., $|z| <_j c$) implies $w(z) > 0$. We may therefore replace v_i (resp., $<_j$) by w.

Replace first each nonarchimedean ordering $<_j$ by a coarser valuation, if necessary, to assume that S contains only archimedean orderings. If v_i and v_j are dependent, then they are finer than a common valuation w. Replace v_i, v_j and any other valuation in S that is finer than w by w. Repeat this step finitely many times to finally assume

that each pair of valuations of S either coincide or they are independent. Reenumerate $v_1, \dots, v_m$ such that $v_1, \dots, v_k$ are independent and for each $j < k$ there exists $i \leq k$ such that $v_i = v_j$.

By Part A, there exists $x \in K$, $x \neq a$ such that $v_i(x-a) \geq \alpha_i$, $i = 1, \dots, k$, and $|x-a| <_j c_j$. This x also satisfies (a). ∎

For the sake of completeness, we also prove in this section the weak approximation theorem for independent valuations and orderings. Here we refer to a set S of valuations and orderings of a field K as **independent** if each pair of objects in S induce distinct topologies on K. The theorem was proved by Artin and Whaples [AW, Thm. 1] for the case where each valuations in S has rank 1 and each ordering in S is archimedean. We follow Prestel and Ziegler [PZ, Thm. 4.5] and use ultraprodcuts to reduce the theorem to the case where each object in S is a valuation which is finer than no valuation of rank 1.

PROPOSITION 17.4 (Weak approximation theorem for independent valuations and orderings): *Let $v_1, \dots, v_m, <_1, \dots, <_n$ be an independent set of valuations and orderings of a field K. Let $a_1, \dots, a_m, b_1, \dots, b_n, c_1, \dots, c_n \in K$ such that $c_j >_j 0$, $j = 1, \dots, n$, and let $\alpha_i \in \Gamma_{v_i}$, $i = 1, \dots, m$. Then there exists $x \in K$ such that*

$$v_i(x - a_i) \geq \alpha_i, \ i = 1, \dots, m, \ \text{and} \ |x - b| \leq_j c_j, \ j = 1, \dots, n. \tag{2}$$

Proof: We use the language of fields with m valuations and n orderings. Lemma 4.1 implies that the statement "v_i and v_j are independent" is elementary. Also, the definition of independence of a valuation and ordering is elementary. As the statement of the Proposition is also elementary, we may use Lemma 16.3 and replace $(K, v_1, \dots, v_m, <_1, \dots, <_n)$ by a nonprincipal ultrapower, if necessary, to assume that $<_1, \dots, <_n$ are nonarchimdedean.

Then each $<_j$ is finer than some valuation w_j which induces the same topology on K as $<_j$. So, replace $<_j$ by w_j and obtain a set $(v_1, \dots, v_m, w_1, \dots, w_n)$ of independent valuations of K. By Proposition 4.4, they satisfy the approximation theorem. Conclude that the original set of valuations and orderings satisfy the approximation condition (2).

∎

18. Examples.

Before we move closer to the goal of this work we stop to give some examples which shed light on the concepts which we have presented up to now. We start with a brief description of the completion of a valued field (K, v) of rank 1.

Recall that a sequence $\{a_n\}_{n=1}^{\infty}$ of elements of K is **Cauchy** if for each $\gamma \in \Gamma_v$ there exists n_0 such that for all $m, n \geq n_0$ we have $v(a_n - a_m) > \gamma$. The field (K, v) is **complete** if every Cauchy sequence of elements of K converges to an element of K.

PROPOSITION 18.1: *Every valued field (K, v) of rank 1 has an extension $(\widehat{K}, \hat{v})$ which is complete such that K is dense in $\widehat{K}$. This extensions unique up to a K-isomorphism. It is the* **completion** *of (K, v).*

Proof: Let R be the ring of all Cauchy sequences of K where addition and multiplication are defined componentswise. The ideal I of R which consists of all sequences that converge to 0 is maximal. Indeed, if $\{a_n\}_{n=1}^{\infty}$ belongs to $R - I$, then there exists $\gamma \in \Gamma_v$ and n_0 such that $v(a_n) \leq \gamma$ for all $n \geq n_0$. The sequence $\{a_n^{-1}\}_{n=n_0}^{\infty}$ is the inverse in R of $\{a_n\}_{n=1}^{\infty}$ modulo I. Also, there exists m such that $v(a_n - a_m) > \gamma$ for each $n \geq m$ and therefore $v(a_n) = v((a_n - a_m) + a_m) = v(a_m)$. The quotient ring $\widehat{K} = R/I$ is therefore a ring and, we define the value $\hat{v}(a)$ of the coset $a = \{a_n\}_{n=1}^{\infty} + I$ for the above sequence as the eventual value $v(a_m)$.

Embed K diagonally in $\widehat{K}$, i.e., map $a \in K$ onto the coset $\{a\}_{n=1}^{\infty} + I$. Then K is dense in $\widehat{K}$ and $\hat{v}$ extends v.

Finally, if (K', v') is another complete extension of (K, v) in which K is dense, then (K', v') is K-isomorphic to $(\widehat{K}, \hat{v})$. Indeed, each Cauchy sequence $\{a_n\}_{n=1}^{\infty}$ in K converges to a unique element a' in K'. Conversely, for each $a' \in K'$ there is a Cauchy sequence $\{a_n\}_{n=1}^{\infty}$ in K which converges to a'. The correspondence between a' and $\{a_n\}_{n=1}^{\infty} + I$ is the desired isomorphism. ∎

REMARK 18.2: Completions of an arbitrary valued field (K, v) is achieved in the same way by replacing countable Cauchy sequences by "transfinite Cauchy sequences" [A2, p. 173]. ∎

The density of K in $\widehat{K}$ immediately implies:

LEMMA 18.3: *The completion* $(\widehat{K}, \hat{v})$ *of a valued field* (K, v) *of rank 1 is an immediate extension. In particular* $\operatorname{rank}(\hat{v}) = 1$.

PROPOSITION 18.4 (HENSEL): *Every complete valued field* (K, v) *of rank 1 is Henselian.*

Proof: Let $f \in O_v[X]$ be a monic polynomial and let a be an element of O_v such that $v(f(a)) > 0$ and $v(f'(a)) = 0$. We have to prove the existence of $x \in O_v$ such that

$$f(x) = 0 \text{ and } v(x - a) > 0. \tag{1}$$

To that end set $t = v(f(a))$ and inductively define a sequence $x_1, x_2, x_3, \ldots$ of elements of O_v such that

$$x_1 = a,\ v(x_{n+1} - x_n) \geq nv(t),\ \text{and}\ v(f(x_n)) \geq nv(t). \tag{2}$$

Indeed, suppose that x_n has already been defined. Then $v(x_n - a) \geq v(t)$ and therefore $v(f'(x_n) - f'(a)) \geq v(t)$. So, $v(f'(x_n)) = 0$ and therefore $v(f'(x_n) - f'(a)) \geq v(t)$. So, $v(f'(x_n)) = 0$ and therefore $f'(x_n)$ is a unit of O_v. Hence, there exists $b \in O_v$ such that $f(x_n) + f'(x_n)bt^n = 0$. Let $x_{n+1} = x_n + bt^n$. Expand $f(x_{n+1}) = f(x_n + bt^n)$ around x_n to find that $f(x_{n+1}) = ct^{n+1}$ with $c \in O_v$. This completes the induction.

As a Cauchy sequence, $\{x_n\}_{n=1}^{\infty}$ converges to an element x which satisfies (1). ∎

REMARK 18.5: *Henselization.* Let (K, v) be a valued field of rank 1. Its completion, $(\widehat{K}, \hat{v})$ is Henselian (Proposition 18.4). Hence, so is $K_0 = K_s \cap \widehat{K}$ with respect to the restriction v_0 of $\hat{v}$ to K_0 (Corollary 11.2). It follows that (K_0, v_0) extends (K_v^h, v^h). In particular K is v-dense in K_v^h.

To prove that $K_0 = K_v^h$ consider $x \in K_0$. Let $f \in O_{v^h}[X]$ be an irreducible polynomial such that $f(x) = 0$. As x is separable over K_v^h, $f'(x) \neq 0$. Choose $a \in K_v^h$ such that $\hat{v}(x - a) > 2\hat{v}(f'(x))$. Then $\hat{v}(f'(x) - f'(a)) \geq \hat{v}(x - a) > 2\hat{v}(f'(x))$ and therefore $\hat{v}(f'(a)) = \hat{v}(f'(x))$. So $\hat{v}(f(a)) = \hat{v}(f(x) - f(a)) \geq \hat{v}(x - a) > 2\hat{v}(f'(a))$. As K_v^h is Henselian, there exists $y \in K$ such that $f(y) = 0$ (Proposition 11.1(e)). Hence $\deg(f) = 1$ and $x \in K_v^h$. ∎

EXAMPLE 18.6: *The field of p-adic numbers.* The completion of $\mathbb{Q}$ with respect to v_p (Example 2.1) is the **field $\mathbb{Q}_p$ of p-adic numbers**. Its valuation ring $\mathbb{Z}_p$ is the **ring of p-adic integers** and its residue field is the field $\mathbb{F}_p$ with p elements. By completeness, each element of $\mathbb{Z}_p$ can be represented as a convergent power series $\sum_{n=0}^{\infty} a_n p^n$, with integers $0 \leq a_n < p$. It follows that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. ∎

EXAMPLE 18.7: *The field of formal power series.* Consider the field $K = K_0((t))$ of formal power series in t with coefficients in a field K_0.

CLAIM: (K, w) is complete. Indeed, let $\{f_k\}_{k=1}^{\infty}$ be a Cauchy sequence, with $f_k = \sum_{n=m_k}^{\infty} a_{kn} t^n$. Then, for each r there exists $k_0 = k_0(r)$ such that if $k \geq k_0$, then $v(f_{k+1} - f_k) > r$. This means that $a_{kn} = a_{k_0 n}$ for each $n \leq r$ and each $k \geq k_0$. It follows that f_k converges to $f = \sum a_{k_0(r),r} t^r$.

Thus (K, w) is complete. Moreover (K, w) is the completion of $K_0(t)$ with respect to the restriction of w to this field. By Proposition 18.4, (K, w) is Henselian. ∎

EXAMPLE 18.8: *Illustrations for Propositions 12.4, 12.5 and 13.5.* Let $\bar{v}$ and $\bar{v}'$ be valuations of $\tilde{\mathbb{Q}}$ with residue fields of distinct characteristics p and p'. Their residue fields are $\widetilde{\mathbb{F}}_p$ and $\widetilde{\mathbb{F}}_{p'}$, respectively. Both $(\tilde{\mathbb{Q}}, \bar{v})$ and $(\tilde{\mathbb{Q}}, \bar{v}')$ are Henselian (Corollary 11.3).

Consider now the canonical valuation w of $K = \tilde{\mathbb{Q}}((t))$ (Example 18.7). Let $\pi_w \colon K \to \tilde{\mathbb{Q}} \cup \{\infty\}$ be the place associated with w. In particular $\pi_w(\sum_{i=0}^{\infty} a_i t^i) = a_0$. Then $O_v = \pi_w^{-1}(O_{\bar{v}}) = \{\sum_{i=0}^{\infty} a_i t^i |\ v(a_0) \geq 0\}$ are valuation rings of K contained in O_w. The rank of the corresponding valuations v and v' of K is 2. Since $\bar{v}$ and $\bar{v}'$ are independent, v and v' are incomparable. By Proposition 12.1, both (K, v) and (K, v') are Henselian. This illustrate Proposition 13.4.

The field $\tilde{\mathbb{Q}}((t))$ is a Galois extension of $\mathbb{Q}((t))$. The latter field is Henselian with respect to the restriction of w to $\mathbb{Q}((t))$, as indeed should follow from Remark 13.6. However, since $\mathbb{Q}$ is not Henselian with respect to the p-adic valuation, Proposition 13.1 implies that $\mathbb{Q}((t))$ is not Henselian with respect to the restriction of v to $\mathbb{Q}((t))$. Thus, the conditions of Proposition 13.5 are essential.

Finally, let E be a proper subfield of $\tilde{\mathbb{Q}}$ such that, with $\bar{v}_E$ the restriction of $\bar{v}$ to E,

$(\tilde{\mathbb{Q}}, \bar{v})$ is the Henselization of $(E, \bar{v}_E)$. One may choose E to be the field of real algebraic numbers ar any PAC proper subfield of $\tilde{\mathbb{Q}}$ [FJ, Thm. 10.4]. Let v_E be the restriction of E to $E((t))$. By Proposition 13.1, $(\tilde{\mathbb{Q}}((t)), v)$ is the Henselization of $(E((t)), v_E)$. Since E is algebraically closed in $E((t))$, we have $G(E) \cong \mathcal{G}(\tilde{\mathbb{Q}}((t))/E((t)))$. In particular, $\tilde{\mathbb{Q}}((t))$ has nontrivial automorphisms over $E((t))$. Note that the residue field $\widetilde{\mathbb{F}}_p$ of v is algebraically closed, but $\tilde{\mathbb{Q}}((t))$ is not separably closed. Thus the conditions of Proposition 14.5 are essential. ∎

EXAMPLE 18.9: *Nonarchimedean orderings.* Let $(K, <)$ be an ordered field. Extend $<$ to an ordering $<^+$ of $K((t))$: for $f = \sum_{n=m}^{\infty} a_n t^n$ with $a_m \neq 0$ set

$$f > 0 \qquad \text{if and only if} \qquad a_m > 0.$$

In particular $0 <^+ t <^+ a$ for each $a \in K$, $a > 0$. Thus t is **infinitesimal** with respect to K. In particular $<^+$ is a nonarchimedean ordering of K. By Lemma 16.2, $K((t))$ has a valuation v which is coarser than $<^+$. We can identify such a valuation explicitly as the canonical valuation v of $K((t))$, which is defined by $v(f) = m$. If $m > 0$, then $f = t^m(a_m + a_{m+1}t + a_{m+2}t^2 + \cdots)$ with $a_m \neq 0$. Hence $a_{m+1}t + a_{m+2}t^2 + \cdots < 1$ and therefore $|f| < |t^m||a_m + 1| < 1$.

By the discussion that proceeds Lemma 15.2, $<^+$ and v induce the same valuation on $K((t))$.

Now define another ordering $<^-$ on $K((t))$ by

$$\begin{aligned} f > 0 \quad \text{if and only if} \quad & m \text{ is even and } a_m > 0, \text{ or} \\ & m \text{ is odd and } a_m < 0. \end{aligned}$$

In this case $-a < t < 0$ for each $a \in K$, $a > 0$. Again, t is infinitesimal with respect to K and v is coarser than $<^-$. It follows that $<^+$-topology of $K((t))$ coincides with the $<^-$-topology, although the orderings are distinct. It is therefore no wonder that the weak approximation theorem does not hold for $<^+$ and $<^-$. For example, there is no $f \in K((t))$ such that

$$|f - 1| <^+ 1 \quad \text{and} \quad |f - 4| <^- 1. \tag{3}$$

Indeed, if $v(f) > 0$, then $v(2f) > 0$ (Observe that since K admits an ordering, $\mathrm{char}(K) = 0$.) and therefore $|f| <^+ \frac{1}{2}$ and $|f| <^- \frac{1}{2}$, so (3) does not hold. If $v(f) < 0$, then $v(5/f) > 0$ and therefore $|f| >^+ 5$ and $|f| >^- 5$. Again, (3) is false. Finally, if $v(f) = 0$, then $f = a_0 + a_1 t + a_2 t^2 + \cdots$ with $a_0 \neq 0$. Then $f - 1 <^+ 1$ would imply $a_0 \leq 2$ and $f - 4 >^- -1$ would imply that $a_0 \geq 3$. Conclude that (3) is false also in this case. ∎

19. Density of Hilbert sets.

Geyer [G, Lemma 3.4] proves that if $v_1, \ldots, v_m, <_1, \ldots, <_n$ is a set of valuations of rank 1 and archimedean orderings of a separably Hilbertian field K, then the diagonal map $\mathbf{x} \mapsto (\mathbf{x}, \ldots, \mathbf{x})$ maps each separable Hilbertian subset H of K^r into a dense subset of $(K^d)^{m+n}$. Here, the ith copy of K^d is equipped with the v_i-topology, $i = 1, \ldots, m$, while the jth copy of K^d is equipped with the $<_j$th topology. Geyer's proof, which depends on the weak approximation theorem works also for an independent set of valuations and orderings. The goal of this section is to modify Geyer's proof and to prove an approxiamtion of zero theorem for Hilbert sets and for an arbitrary set of valuations and orderings. Throughout we use the notation of Section 0.

It notaionally convenient to work with Hilbert sets which are defined by only one polynomial.

LEMMA 19.1: *Let $f_1, \ldots, f_m \in K[T_1, \ldots, T_r, X]$ be irreducible polynomials which are separable in X and let $0 \neq g \in K[T_1, \ldots, T_r]$. Then there exists an irreducible polynomial which is separable and monic in X such that $H_K(f) \subseteq H_K(f_1, \ldots, f_m; g)$.*

Proof: : Just replace T in the proof of [FJ, Lemma 11.2] by $T_1, \ldots, T_r$. ∎

LEMMA 19.2: *Let K be a separably Hilbertian field. Let $f \in K[T_1, \ldots, T_r, X]$ be an absolutely irreducible polynomial which is separable in X. Then, there exist $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \ldots \in K^r$ and $c_1, c_2, c_3, \ldots \in K_s^r$ such that $f(\mathbf{a}_i, c_i) = 0$ and $K(c_1), K(c_2), K(c_3), \ldots$ is linearly disjoint sequence of separable extensions of K of degree $n = \deg_X f$.*

Proof: Assume inductively that $\mathbf{a}_i, c_i$ have been found for $i = 1, \ldots, m$. Then $L = K(c_1, \ldots, c_m)$ is a finite separable extension of K. As $f(\mathbf{T}, X)$ is irreducible over L,

Lemma 0.3 gives $\mathbf{a}_{m+1} \in K^r$ such that $f(\mathbf{a}, X)$ is irreducible over L and of degree n. Choose a root c_{m+1} of $f(\mathbf{a}, X) = 0$. Then $K(c_{m+1})$ is a separable extension of K of degree n which is linearly disjoint from L over K. Conclude that $K(c_1), \ldots, K(c_{m+1})$ are linearly disjoint over K. ∎

LEMMA 19.3: *let $F_1, F_2, F_3, \ldots$ be a linearly disjoint sequence of extensions of a field K. Let L be a finite separable extension of K, and let $f \in K[X]$ be an irreducible separable polynomial. Then there exists k such that*

(a) *f is irreducible over F_i, $i = k, k+1, k+2, \ldots$, and*

(b) *the sequence $LF_k, LF_{k+1}, LF_{k+2}, \ldots$ is linearly disjoint over L.*

Proof: of (a): Let N be the splitting field of f over K. Then N has only finitely many subfields which contain K. If $N \cap F_i$ were a proper extension of K for infinitely many i's, then there would exist $i < j$ such that $N \cap F_i = N \cap F_j$ is a proper extension of K. This would however contradict $F_i \cap F_j = K$. Hence, there exists k such that for each $i \geq k$, $N \cap F_i = K$. Conclude from the tower lemma [FJ, Lemma 9.3] that f_i is irreducible over F_i.

Proof of (b): Replace L, if necessary, by its Galois closure over K to assume that L is Galois over K. Assume that the sequence $L, F_k, F_{k+1}, F_{k+2}, \ldots$ is linearly disjoint over K for no k. Then, for each k there exists an integer $f(k) \geq k$ such that $L \cap (F_k \cdots F_{f(k)})$ is a proper extension of K. Again, as L has only finitely many subfields that contain K, there exists a proper extension K' of K such that $L \cap (F_k \cdots F_{f(k)}) = K'$ for infinitely many k's. Fix one of those k's and take $l > f(k)$ such that $L \cap (F_l \cdots F_{f(l)}) = K'$. Hence $K' \subseteq (F_k \cdots F_{f(k)}) \cap (F_l \cdots F_{f(l)})$. This contradiction to the linear disjointness of $F_1, F_2, F_3, \ldots$ over K proves the existence of k such that $L, F_k, F_{k+1}, \ldots$ is linearly disjoint over K. Conclude that $LF_k, LF_{k+1}, LF_{k+2}, \ldots$ are also linearly disjoint. ∎

LEMMA 19.4: *Let $f \in K[X_1, \ldots, X_r, Y]$ be an irreducible polynomial over K. Let n be a positive integer which is not a multiple of* $\mathrm{char}(K)$. *Consider a subset*

$$\{c_{ij} |\ i = 1, 2, 3 \ldots;\ j = 1, \ldots, r\}$$

of K such that

$$\{K(\sqrt[n]{c_{ij}}) |\ i = 1, 2, 3, \ldots;\ j = 1, \ldots, r\}$$

is a linearly disjoint set of extensions of K of degree n. Then for all but finitely many i's, the polynomial

$$f_i(X_1,\dots,X_r,Y) = f\left(\frac{1}{X_1^{n-1}-c_{i1}X_1^{-1}},\dots,\frac{1}{X_r^{n-1}-c_{ir}X_r^{-1}},Y\right) \tag{1}$$

is irreducible in the ring $K(X_1,\dots,X_r)[Y]$.

Proof: Choose r algebraically independent elements $t_1,\dots,t_r$ over K. For each i and j choose $x_{ij}\in K(t)_s$ such that

$$x_{ij}^n - t_j x_{ij} - c_{ij} = 0. \tag{2}$$

Then

$$t_j = x_{ij}^{n-1} - c_{ij}x_{ij}^{-1}, \qquad j=1,\dots,r.$$

Hence, with $\mathbf{x}_i=(x_{i1},\dots,x_{ir})$, $K(\mathbf{x}_i)$ is an algebraic extension of $K(\mathbf{t})$, of degree at most n^r, and therefore $x_{i1},\dots,x_{ir}$ are algebraically independent over K.

CLAIM: For each m, $[K(\mathbf{x}_1,\dots,\mathbf{x}_m) : K(\mathbf{t})] = n^{rm}$. Indeed, the specialization $t_j\to 0$, $j=1,\dots,r$, extends to a homomorphism φ: $K[\mathbf{x}_1,\dots,\mathbf{x}_m]\to K[\sqrt[n]{c_{ij}}\mid i=1,\dots,m;\ j=1,\dots,r]$. By assumption, the latter ring (which is actually a field) has, as a vector space over K, dimension n^{rm}. Hence, the dimension of $K(\mathbf{x}_1,\dots,\mathbf{x}_m)$ as a $K(\mathbf{t})$-vector space is at least n^{rm}. As $[K(\mathbf{x}_1,\dots,\mathbf{x}_m):K(\mathbf{t})]\le n^{rm}$ (by (2)), equality must hold.

By the claim, $K(\mathbf{x}_1),K(\mathbf{x}_2),K(\mathbf{x}_3),\dots$ is a linearly disjoint sequence of extensions of $K(\mathbf{t})$ of degree n^r. By assumption, $f(t_1,\dots,t_r,Y)$ is irreducible over $K(\mathbf{t})$. So, Lemma 19.2 provides a k such that for each $i\ge k$

$$f(t_1,\dots,t_r,Y) = f_i\left(\frac{1}{x_{i1}^{n-1}-c_{i1}x_{i1}^{-1}},\dots,\frac{1}{x_{ir}^{n-1}-c_{ir}x_{ir}^{-1}},Y\right)$$

is irreducible over $K(\mathbf{x}_i)$. As $x_{i1},\dots,x_{ir}$ are algebraically independent over r, this means that the polynomial (1) is irreducible over $K(\mathbf{X})$. ∎

LEMMA 19.5: *Let K be a separably Hilbertian field with valuations and orderings $v_1,\dots,v_m,<_{m+1},\dots,<_n$. Then, for each irreducible polynomial $f\in K[X_1,\dots,X_r,Y]$ which is separable in Y there exists $\mathbf{a}\in K^r$ such that $f(\mathbf{a},Y)$ is irreducible over K,*

$$v_i(\mathbf{a})\ge 0,\ i=1,\dots,m, \text{ and } |\mathbf{a}|\le_j 1,\ j=m+1,\dots,n. \tag{3}$$

Proof: Let $p = 2$ if $\mathrm{char}(K) \neq 2$ and $p = 3$ if $\mathrm{char}(K) = 2$. As the polynomial $Y^p - X$ is absolutely irreducible and separable in Y and K is separably Hilbertian, Lemma 19.1 gives a set $\{c_{kl} \in K^\times |\ k = 1, 2, 3, \ldots;\ l = 1, \ldots, r\}$ such that $\{K(\sqrt[p]{c_{kl}})|\ k = 1, 2, 3, \ldots;\ l = 1, \ldots, r\}$ is a linearly disjoint set of quadratic extensions of K.

For each nonnegative integer k there are unique $\varepsilon_{kij} \in \{0, 1\}$ such that

$$k \cong \sum_{l=1}^{r} \sum_{i=1}^{n} \varepsilon_{kil} 2^{i-1+(l-1)n} \bmod 2^{rn}.$$

Each c_{kl} can be multiplied by a p-power b_{kl}^p of $K^\times$ without changing $K(\sqrt[p]{c_{kl}})$. Use Proposition 17.1 to choose c_{kl} such that for $1 \leq i \leq n$ and $m + 1 \leq j \leq n$

$$(4a) \qquad \varepsilon_{kil} = 0 \text{ implies } v_i(c_{kl}) > 0 \text{ and } |c_{kl}| \leq_j 1$$

$$(4b) \qquad \varepsilon_{kil} = 1 \text{ implies } v_i(c_{kl}) \leq 0 \text{ and } |c_{kl}| \geq_j 6.$$

By Lemma 19.4, all but finitely many of the polynomials

$$f_k(X_1, \ldots, X_r, Y) = f\left(\frac{1}{X_1^{p-1} - c_{k1}X_1^{-1}}, \ldots, \frac{1}{X_r^{p-1} - c_{kr}X_r^{-1}}, Y\right)$$

are irreducible in $K(\mathbf{X})[Y]$. Omit the first $e \cdot 2^{rn}$ of them for e large enough, if necessary, to assume that each f_k is irreducible. Then choose $\mathbf{b} \in K^r$ such that $f_k(\mathbf{b}, Y)$ is irreducible for each $0 \leq k < 2^{nr}$.

For each $1 \leq i \leq m$, $m + 1 \leq j \leq n$, and $1 \leq l \leq r$ define ε_{il} and ε_{jl} in the following way:

$$(5a) \qquad v_i(b_l) \leq 0 \text{ implies } \varepsilon_{il} = 0; \quad |b_l| \geq_j 2 \text{ implies } \varepsilon_{jl} = 0$$

$$(5b) \qquad v_i(b_l) > 0 \text{ implies } \varepsilon_{il} = 1; \quad |b_l| <_j 2 \text{ implies } \varepsilon_{jl} = 1.$$

Let

$$k = \sum_{l=1}^{r} \left[\sum_{i=1}^{m} \varepsilon_{il} 2^{i-1+(l-1)n} + \sum_{j=m+1}^{n} \varepsilon_{jl} 2^{j-1+(l-1)n} \right]$$

and

$$a_l = \frac{1}{b_l^{p-1} - c_{kl} b_l^{-1}} \qquad l = 1, \ldots, r.$$

Then $f(\mathbf{a}, Y) = f_k(\mathbf{b}, Y)$ is irreducible. We prove that $\mathbf{a}$ satisfies (3).

If $1 \le i \le m$ and $v_i(b_l) \le 0$, then $\varepsilon_{il} = 0$ (by (5a)). Hence, by (4a), $v_i(c_{kl}) > 0$. Thus $v_i(c_{kl}b_l^{-1}) > v_i(b_l^{p-1})$. Conclude that $v_i(b_l^{p-1} - c_{kl}b_l^{-1}) = v_i(b_l^{p-1}) \le 0$ and $v_i(a_l) \ge 0$.

If $v_i(b_l) > 0$, then $\varepsilon_{il} = 1$ (by (5b)). Hence, by (4b), $v_i(c_{kl}) \le 0$. Thus $v_i(b_l^{p-1}) > v_i(c_{kl}) - v_i(b_l)$. Conclude that $v_i(b_l^{p-1} - c_{kl}b_l^{-1}) = v_i(c_{kl}) - v_i(b_l) < 0$ and $v_i(a_l) > 0$.

If $m+1 \le j \le n$ and $|b_l| \ge_j 2$, then $\varepsilon_{jl} = 0$ (by (5a)). Also, $p = 2$, because otherwise $\mathrm{char}(K) = 2$ and K has no orderings. Hence, by (4a), $|c_{kl}| \le_j 1$. Thus $|b_l - c_{kl}b_l^{-1}| \ge_j |b_l| - |c_{kl}||b_l^{-1}| >_j 1$ and therefore $|a_l| <_j 1$.

Finally, if $|b_l| <_j 2$, then $\varepsilon_{jl} = 1$ (by (5b)). Hence, by (4b), $|c_{kl}| \ge_j 6$. Thus $|b_l - c_{kl}b_l^{-1}| \ge_j |c_{kl}||b_l^{-1}| - |b_l| >_j 1$ and $|a_l| <_j 1$. Thus, (3) is satisfied in each case. ∎

PROPOSITION 19.7 (Approximation of zero theorem for separably Hilbert sets): *Let K be a separably Hilbertian field equipped with quasi independent valuations and orderings $v_1, \dots, v_m, <_1, \dots, <_n$. Denote the valuation ring of v_i by Γ_i. Let H be a separable Hilbert subset of K^r. Then, for each $\mathbf{a} \in K^r$, $\alpha_i \in \Gamma_{v_i}$, $i = 1, \dots, m$, and $c_j \in K$, $c_j >_j 0$, there exists $\mathbf{x} \in H$ such that*

$$v_i(\mathbf{x} - \mathbf{a}) \ge \alpha_i,\ i = 1, \dots, m, \quad \text{and} \quad |\mathbf{x} - \mathbf{a}| \le_j c_j,\ j = 1, \dots, n. \tag{6}$$

Proof: By Lemma 19.1 there exists an irreducible polynomial $g \in K[X_1, \dots, X_r, Y]$ which is separable in Y such that $H_K(g) \subseteq H$. Use Proposition 16.1 to find $d \in K^\times$ such that

$$v_i(d) \ge \alpha_i,\ i = 1, \dots, m, \text{ and } |d| \le_j \frac{1}{2}c_j,\ j = 1, \dots, n.$$

Apply Lemma 19.5 to the polynomial $f(\mathbf{T}, Y) = g(\mathbf{a} + d\mathbf{T}, Y)$ to find $\mathbf{t} \in K^r$ such that $g(\mathbf{a} + d\mathbf{t}, Y)$ is irreducible over K,

$$v_i(\mathbf{t}) \ge 0,\ i = 1, \dots, m, \text{ and } |\mathbf{t}| \le_j 1,\ j = 1, \dots, n.$$

Then $\mathbf{x} = \mathbf{a} + d\mathbf{t}$ belongs to H and satisfies (6). ∎

A combination of the weak approximation theorem for independent valuations and orderings (Proposition 17.4) and the approxiamtion of zero theorem for separably Hilbert sets (Proposition 19.7) immediately gives a density theorem. It will however not be used in the proof of the main result.

PROPOSITION 19.8 (Density theorem for separably Hilberts sets): *Let K be a separably Hilbertian field equipped with an independent set $v_1, \dots, v_m, <_1, \dots, <_n$ of valuations an dorderings. Let H be a separable Hilbert subset of K^r. Then, for all $\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{b}_1, \dots, \mathbf{b}_n \in K^r$, $\alpha_i \in \Gamma_{v_i}$, $i = 1, \dots, m$, $c_j \in K$, $c_j >_j 0$, $j = 1, \dots, n$, there exists $\mathbf{x} \in H$ such that*

$$v_i(\mathbf{x} - \mathbf{a}_i) > \alpha_i,\ i = 1, \dots, m; \quad \text{and} \quad |\mathbf{x} - \mathbf{b}_j| <_j c_j,\ j = 1, \dots, n.$$

The approximation of zero theorem makes it possible to strengthen Lemma 0.4:

LEMMA 19.9: *Let K be a separably Hilbertian field equipped with valuations $v_1, \dots, v_m$ and orderings $<_1, \dots, <_n$. Let $f \in K[X]$ be a monic polynomial of degree d. Let $\alpha_i \in \Gamma_{v_i}$, $i = 1, \dots, m$, and let $c_1, \dots, c_n \in K$. Then there exists a sequence $g_1, g_2, g_3, \dots$ of monic polynomials of degree d in $K[X]$ and a linearly disjoint sequence $L_1, L_2, L_3, \dots$ of Galois extensions of K such that for each k*

(a) *$v_i(g_k - f) \geq \alpha_i$, $i = 1, \dots, m$; $|g_k - f| \leq_j c_j$, $j = 1, \dots, n$, and*

(b) *L_k is the splitting field of g_k over K and $\mathcal{G}(L_k/K) \cong S_n$.*

Proof: Let $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Suppose by induction that $g_1, \dots, g_{k-1}$ and $L_1, \dots, L_{k-1}$ have been constructed. Then $L = L_1 \cdots L_{k-1}$ is a finite Galois extension of K. The Galois group of the general polynomial $h(\mathbf{T}, X) = X^d + T_{n-1}X^{d-1} + \cdots + T_0$ of degree d over $L(T_0, \dots, T_{n-1})$ is isomorphic to S_n. By a theorem of Hilbert [FJ, Lemma 12.12], L^d (resp., K^d) has a separable Hilbert subset H_L (resp., H_K) such that for each $\mathbf{b} \in H_L$ (resp., $\mathbf{b} \in H_K$) $\mathcal{G}(h(\mathbf{b}, X), L) \cong S_d$ (resp., $\mathcal{G}(h(\mathbf{b}, X), L) \cong S_d$). By Lemma 0.3, $H_K \cap H_L$ contains a separable Hilbert subset H of K^d. Now use the approximation of zero theorem (Proposition 19.7) to choose $\mathbf{b} \in H_K$ such that $v_i(\mathbf{b} - \mathbf{a}) \geq \alpha_i$ for $i = 1, \dots, m$ and $|\mathbf{b} - \mathbf{a}| \leq_j c_j$ for $j = 1, \dots, n$. Then $g_k(X) = h(\mathbf{b}, X)$ satisfies (7). ∎

20. The free product theorem.

We apply the information which which has been accumulated in this work so far to prove the main result of this work. We need however two more group theoretic lemmas:

LEMMA 20.1: *Let φ_i: $G_i \to A$ be a homomorphism of a profinite group G_i into a finite group A, $i = 1, \ldots, k$, and let m be a positive integer. Suppose that $\varphi_1, \ldots, \varphi_{k-1}$ are injective and that $G_k \cong \widehat{F}_e$, for some positive integer e. Then there exists a finite group B and homomorphisms α: $B \to A$ and ψ: $G_i \to B$, $i = 1, \ldots, k$ such that m divides $|B|$, $\alpha \circ \psi_i = \varphi_i$ for $i = 1, \ldots, k$, and $B = \langle \psi(G_1), \ldots, \psi(G_k) \rangle$. In particular, $\psi_1, \ldots, \psi_{k-1}$ are injective.*

Proof: Let $G = G_1 * \cdots * G_k$. Extend φ_i, $i = 1, \ldots, k$ into a homomorphism φ: $G \to A$. Choose an open normal subgroup N_k of G_k such that $m \mid (G_k : N_k)$. Let N be an open normal subgroup of $G = G_1 * \cdots * G_k$ such that $N \leq \mathrm{Ker}(\varphi)$ and $N \cap G_k \leq N_k$. Then $B = G/N$ is a finite group whose order is a multiple of m. Moreover, there are homomorphisms φ: $G \to B$ and α: $B \to A$ such that $\varphi = \alpha \circ \psi$. Let ψ_i be the restriction of ψ to G_i. Then $\alpha \circ \psi_i = \varphi_i$, $i = 1, \ldots, k$ and $B = \langle \psi(G_1), \ldots, \psi(G_k) \rangle$. ∎

A group G of permutations of a set X is said to act **regularly** on X if for each $\sigma \in G$ and $x \in X$, $x^\sigma = x$ implies $\sigma = 1$.

Note that if G acts regularly on X, then so does each subgroup of G. For example, if $f \in K[X]$ is a separable polynomial with roots $x_1, \ldots, x_n$ and $L = K(x_i)$ for each i, then L is a Galois extension of K and $\mathcal{G}(L/K)$ acts regularly on $\{x_1, \ldots, x_n\}$.

LEMMA 20.2: *Let G and G' be finite groups which act regularly on a finite set X. If f: $G \to G'$ is an isomorphism, then there exists a permutation π of X such that $f(\sigma) = \pi^{-1}\sigma\pi$ for each $\sigma \in G$. In particular $G^\pi = G'$.*

Proof: let X_0 (resp., X_0') be a system of representatives for the G- (resp., G'-) orbits of X. By regularity, $|X_0| = |X|/|G| = |X|/|G'| = |X_0'|$. Hence, there exists a bijection π_0: $X_0 \to X_0'$. Extend π_0 to a permutation π of X by the rule $(x_0^\sigma)^\pi = (x_0^{\pi_0})^{f(\sigma)}$, for $x_0 \in X_0$ and $\sigma \in G$. Then, each $x = x_0^\tau$ with $\tau \in G$, satisfies $x^{\sigma\pi} = x^{\pi f(\sigma)}$. This means that $\pi^{-1}\sigma\pi = f(\sigma)$. ∎

In the rest of this section we abuse notation and write a relation of the form

$$\langle G_1^{\sigma_1}, \dots, G_m^{\sigma_m}, \tau_1, \dots, \tau_e \rangle \cong \prod_{i=1}^{e}{}^{*} G_i * \widehat{F}_e \tag{1}$$

for closed subgroups $G_1, \dots, G_m$ of $G(K)$ and elements $\tau_1, \dots, \tau_e \in G(K)$ to mean that $\langle \tau_1, \dots, \tau_e \rangle \cong \widehat{F}^e$ and the closed subgroup on the left hand side of (1) is the free product of $G_1^{\sigma_1}, \dots, G_e^{\sigma_3}$ and $\langle \sigma_{e+1}, \dots, \sigma_m \rangle$. This implies in particular that the isomorphism (1) holds.

a **local algebraic** extension of a field K is an algebraic extension L of K which admits a Henselian valuation or is a real closure of K.

THEOREM 20.3 (Free product theorem): *Let K be a countable Hilbertian field. Let $E_1, \dots, E_m$ be local algebraic extensions of K, and let m be a positive integer. Then, for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G(K)^m \times G(K)^e$*

$$\langle G(E_1)^{\sigma_1}, \dots, G(E_m)^{\sigma_m}, \tau_1, \dots, \tau_e \rangle \cong G(E_1) * \cdots * G(E_m) * \widehat{F}_e. \tag{2}$$

Proof: If (2) holds for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G(K)^m \times G(K)^e$, then

$$\langle G(E_1)^{\sigma_1}, \dots, G(E_m)^{\sigma_m} \rangle \cong G(E_1) * \cdots * G(E_m)$$

for almost all $\boldsymbol{\sigma} \in G(K)^m$. So, assume without loss that $e \geq 1$.

We let i range over $1, \dots, m$. For each i, E_i is either Henselian with respect to a valuation v_i or it is a real closure of $(K, <_i)$ for some ordering $<_i$ of K. Denote the topology that v_i (resp., $<_i$) induces on K by $\mathcal{T}_i$.

Let F be a finite Galois extension of K. For each set $F_i = FE_i$. Let $B = \langle B_1, \dots, B_m, C \rangle$ be a finite group whose order is a multiple of $[F : K]$. For each i let $\rho_i \colon \mathcal{G}(F_i/E_i) \to B_i$ be an isomorphism, and let $\gamma \colon \langle \tau_1, \dots, \tau_e \rangle \to C$ be an epimorphism. It suffices to prove that for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau})$

(3) there exists a finite Galois extension L of K and B can be embedded in $\mathcal{G}(L/K)$ is such a way that for each i, $LE_i = F_i$, $\mathcal{G}(L/L \cap E_i^{\sigma_i}) = B_i$, and if $\bar{\sigma}_i$ is the restriction of σ_i to L and $\bar{\tau}_j$ is the restriction of τ_j to L, then the map $\bar{\sigma}_i \circ \mathrm{res}_L \colon \mathcal{G}(F_i/E_i) \to B_i$ coincides with ρ_i, $i = 1, \dots, m$, and $\bar{\tau}_j = \gamma(\tau_j)$ for $j = 1, \dots, e$.

The rest of the proof naturally breaks up into two parts.

PART A: *Proof of the reduction step.* Suppose that (3) is true for each system $\mathcal{F} = (F, B, \rho_1, \dots, \rho_m, \gamma)$ as above and for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau})$. As K is countable, there are only countably many systems $\mathcal{F}$. By the free generators theorem (Proposition 0.5) almost all $\boldsymbol{\tau} \in G(K)^e$ generate a group which is isomorphic to $\widehat{F}_e$. So, almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau})$ satisfy (3) for each system $\mathcal{F}$ and $\langle \boldsymbol{\tau} \rangle \cong \widehat{F}_e$. We claim that each such $(\boldsymbol{\sigma}, \boldsymbol{\tau})$ satisfies (2).

Indeed, let $\varphi_i \colon G(E_i)^{\sigma_i} \to A$, $i = 1, \dots, m$, and $\psi \colon \langle \tau_1, \dots, \tau_e \rangle \to A$ be homomorphisms into a finite group A. Let $F'_{i,0}$ be the fixed field in K_s of $\mathrm{Ker}(\varphi_i)$ and let $F_{i,0}$ be the unique finite Galois extension of E_i such that $F_{i,0}^{\sigma_i} = F'_{i,0}$. Choose a finite Galois extension F of K such that $F_i = FE_i$ contains $F_{i,0}$ for each i. Let $\bar{\varphi}_i \colon \mathcal{G}(F_i^{\sigma_i}/E_i^{\sigma_i}) \to A$ be the homomorphism induced by φ_i, let $\bar{\rho}_i = \bar{\varphi}_i \circ \sigma_i \colon \mathcal{G}(F_i/E_i) \to A$. By Lemma 20.2 there exists a finite group $B = \langle B_1, \dots, B_m, C \rangle$ whose order is a multiple of $[F : K]$, a homomorphism $\alpha \colon B \to A$, an isomorphism $\rho_i \colon \mathcal{G}(F_i/E_i) \to B_i$, $i = 1, \dots, m$, and an epimorphism $\gamma \colon \langle \tau_1, \dots, \tau_e \rangle \to C$ such that $\alpha \circ \rho_i = \bar{\rho}_i$, $i = 1, \dots, m$. In this set up our assumption says that (3) holds. Define $\varphi \colon G_{\sigma,\tau} \to A$ to be the restriction of $\alpha \circ \mathrm{res}_L$ to $G_{\sigma,\tau}$. Then

$$\alpha \circ \mathrm{res}_L \circ \sigma_i = \alpha \circ \bar{\sigma}_i \circ \mathrm{res}_L = \alpha \circ \rho_i = \bar{\rho}_i = \bar{\varphi}_i \circ \sigma_i \quad \text{on} \quad \mathcal{G}(F_i/E_i).$$

Hence $\alpha \circ \mathrm{res}_L = \bar{\varphi}_i$ on $\mathcal{G}(F_i^{\sigma_i}/E_i^{\sigma_i})$, and therefore φ coincides with φ_i on $G(E_i)^{\sigma_i}$. Likewise, the restriction of φ to $\langle \tau_1, \dots, \tau_e \rangle$ coincides with ψ.

$$\begin{array}{ccccc}
G(E_i) & \xrightarrow{\sigma_i} & G(E_i)^{\sigma_i} & & \\
\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\
\mathcal{G}(F_i/E_i) & \xrightarrow{\sigma_i} & \mathcal{G}(F_i^{\sigma_i}/E_i^{\sigma_i}) & & \\
\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \\
\mathcal{G}(L/L \cap E_i) & \xrightarrow{\bar{\sigma}_i} & \mathcal{G}(L/L \cap E_i^{\sigma_i}) = B_i & \xrightarrow{\alpha} & A
\end{array}$$

Conclude that (2) is true.

PART B: *Proof of (3) for almost all* $(\boldsymbol{\sigma}, \boldsymbol{\tau})$. Consider a system $(F, B, \rho_1, \dots, \rho_m, \gamma)$ as in the beginning of the proof. Let $d = [F : K]$ and $n = |B|$. Then $d|n$. Choose a

primitive element x for the extension F/K and let $x_1, \dots, x_d$ be its conjugates over K. Choose elements $a_1, \dots, a_{n/d}$ in K such that

$$x_s + a_t \neq x_{s'} + a_{t'} \quad \text{if} \quad (s,t) \neq (s',t').$$

Then

$$f(X) = \prod_{s=1}^{d} \prod_{t=1}^{n/d} (X - x_s - a_t)$$

is a monic polynomial of degree n with coefficients in K and with n distinct roots. As K is Hilbertian, Lemma 19.9 gives a sequence $g_1, g_2, g_3, \dots$ of monic polynomials of degree n in $K[X]$ and a linearly disjoint sequence $L_1, L_2, L_3, \dots$ of Galois extensions of K such that for each k

(4a) g_k is $\mathcal{T}_i$-close to f for $i \in I$, and

(4b) L_k is the splitting field of g_k over K and $\mathcal{G}(L_k/K) \cong S_n$.

For each i and each (s,t) we have $E_i(x_s - a_t) = E_i(x_s) = E_i \cdot K(x_s) = E_iF = F_i$. Hence, by (4a), Proposition 12.3, and Lemma 15.5, the set R_k of roots of g_k consists of n elements, each of them generates F_i over E_i. Thus, by (4b), $L_kE_i = F_i$ and $\mathcal{G}(L_k/L_k \cap E_i) \cong \mathcal{G}(F_i/E_i)$ acts regularly on R_k. The group B acts regularly on itself by multiplication from the right. So, since $|B| = n = |R_k|$ and $\mathcal{G}(L_k/K) \cong S_n$, we can view B as a subgroup of $\mathcal{G}(L_k/K)$ which acts regularly on R_k. Denote the image of B_i in $\mathcal{G}(L_k/K)$ under this identification by B_{ki}, and the image of C by C_k. By Lemma 20.2, for each i there exists $\sigma_{ki} \in \mathcal{G}(L_k/K)$ such that $\mathcal{G}(L_k/L_k \cap E_i)^{\sigma_{ki}} = B_{ki}$ and the map $\sigma_{ki} \circ \mathrm{res}_L$ from $\mathcal{G}(F_i/E_i)$ onto B_{ki} coincides with ρ_i. Also, $\tau_{kl} = \gamma(\tau_l)$, $l = 1, \dots, e$ generate $B_{k,m+1}$. So,

$$\left\langle \mathcal{G}(L_k/L_k \cap E_1^{\sigma_{k1}}), \dots, \mathcal{G}(L_k/L_k \cap E_m^{\sigma_{km}}), \tau_{k1}, \dots, \tau_{ke} \right\rangle = \langle B_{k1}, \dots, B_{km}, C_k \rangle = B.$$

By Lemma 0.2, for almost all $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G(K)^m \times G(K)^e$ there exists k such that $\mathrm{res}_L(\boldsymbol{\sigma}, \boldsymbol{\tau}) = (\boldsymbol{\sigma}_k, \boldsymbol{\tau}_k)$. Each of these $(\boldsymbol{\sigma}, \boldsymbol{\tau})$ satisfies (3). ∎

References

[AW] E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations,* Bulletin of AMS **51** (1945), 469–492.

[A1] J. Ax, *Solving diophantine problems modulo every prime,* Annals of Mathematics **85** (1967), 161–183.

[A2] J. Ax, *A mathematical approach to some problems in number theory,* AMS Proc. Symp. Pure Math. **XX** (1971), 161–190.

[BNW] E. Binz, J. Neukirch and G.H. Wenzel, *A subgroup theorem for free products of profinite groups,* Journal of Algebra **19** (1971), 104–109.

[Bou] N. Bourbaki, *General Topology, Chapters 1–4,* Springer, Berlin, 1989.

[E] A.J. Engler, *Fields with two incomparable Henselian valuation rings,* manuscripta mathematica **23** (1978), 373-385.

[Ef] I. Efrat, *The elementary theory of free pseudo p-adicallyy closed fields of finite corank* Journal of Symbolic Logic,

[EJ] I. Efrat and M. Jarden, *Free pseudo p-adically closed fields of finite corank,* Journal of Algebra,

[FJ] M.D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik III **11**, Springer, Heidelberg, 1986.

[G] W.-D. Geyer, *Galois groups of intersections of local fields,* Israel Journal of Mathematics **30** (1978), 382–396.

[HJ] D. Haran and M. Jarden, *The absolute Galois group of a pseudo p-adically closed field,* Journal für die reine und angewandte Mathematik **383** (1988), 147–206.

[J1] M. Jarden, *Algebraic extensions of finite corank of Hilbertian fields,* Israel Journal of Mathematics **18** (1974), 279-307.

[J2] M. Jarden, *The elementary theory of large e-fold ordered fields,* Acta mathematica **149** (1982), 239-260.

[JK] M. Jarden and U. Kiehne, *The elementary theory of algebraic fields of finite corank,* Inventiones Mathematicae **30** (1975), 275-294.

[K] A.G. Kurosh, *The Theory of Groups II,* Chelsea, New York, 1960.

[L] S. Lang, *Algebra,* Addison-Wesley, Reading, 1970.

[LS] R. C. Lyndon and P.E. Schupp, *Combinatorial Group Theory,* Ergebnisse der Mathematik und ihrer Grenzgebiete **89**, Springer, Berlin.

[PZ] A. Prestel and M. Ziegler, *Model theoretic methods in the theory of topological fields,* Journal für die reine und angewandte Mathematik **299/300** (1978), 318–341.

[R] P. Ribenboim, *Théorie des valuations,* Les Presses de l'Université de Montréal, Montréal, 1964.

[Ri] L. Ribes, *Introduction to profinite groups and Galois Cohomology,* Queen's papers in pure and applied Mathematics 24, Queen's University, Kingston, 1970.

[S] F.K. Schmidt, *Mehrfach perfeckte Körper*, Mathematische Annalen **108** (1933), 1–25.