5 Algebra of Henselian Fields

5.1 Extensions of Henselian Valuations

Our first goal is to give two alternative characterizations of being henselian. The first is that for any algebraic extension there is a unique extension of the valuation. The second, under some additional assumptions, is that there are no proper immediate algebraic extensions.

We begin with a useful lemma.

Lemma 5.1 *Suppose $\mathcal{O}_1, \ldots, \mathcal{O}_m$ are valuation rings of K with maximal ideals $\mathfrak{m}_i$, $A = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_m$ and $\mathfrak{n}_i = A \cap \mathfrak{m}_i$. Then $\mathcal{O}_i = A_{\mathfrak{n}_i}$ for each i.*

Proof Let $\boldsymbol{k}_i$ denote the residue field of $\mathcal{O}_i$. Let $x \in \mathcal{O}_1$. We may assume $x \neq 1$. Let $I = \{i : x \in \mathcal{O}_i\}$.

Choose M so that:

- $M \neq 0 (\mathrm{mod}\ \mathfrak{m}_i)$ for all i;
- for $i \in I$ either $x = 1(\mathrm{mod}\ \mathfrak{m}_i)$ or x is not a M^{th} root of unity in $\boldsymbol{k}_i$;
- for $i \notin I$ either $x = 1(\mathrm{mod}\ \mathfrak{m}_i)$ or $1/x$ is not a M^{th} root of unity in $\boldsymbol{k}_i$.

The next exercise is to show this is always possible. Let $y = 1 + x + \cdots + x^{M-1}$. Then y is a unit in $\mathcal{O}_i$ [if $x = 1(\mathrm{mod}\ \mathfrak{m}_j)$, then $y = M \neq 0(\mathrm{mod}\ \mathfrak{m}_j)$, while if $x \neq 1(\mathrm{mod}\ \mathfrak{m}_j)$, then $y = \frac{1-x^M}{1-x} \neq 0(\mathrm{mod}\ \mathfrak{m}_i)$]. In particular $xy^{-1} \in \mathcal{O}_i$ for $i \in I$.

Similarly, we can also assume that $z = 1 + x^{-1} + \cdots + x^{1-M}$ is a unit in $\mathcal{O}_j$ for $j \notin I$. But then $y^{-1} = x^{1-M} z^{-1} \in \mathcal{O}_j$ and $xy^{-1} = x^{2-M} z^{-1} \in \mathcal{O}_j$ for $j \notin I$. Thus $xy^{-1}, y^{-1} \in A$ and $y^{-1} \notin \mathfrak{n}_1$. Thus $x = (xy^{-1}/y^{-1}) \in A_{\mathfrak{n}_1}$. $\square$

Exercise 5.2 Show that it is always possible to choose M as in the above proof.

Lemma 5.3 *Let K be a field and let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be valuation rings of K such that $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ for $i \neq j$, let $A = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_m$ and let $\mathfrak{n}_i = \mathfrak{m}_i \cap A$. Then*

i) $\mathfrak{n}_i \not\subseteq \mathfrak{n}_j$ for $i \neq j$;

ii) $\mathfrak{n}_1, \ldots, \mathfrak{n}_m$ are maximal ideals of A and every maximal ideal of A is one of the $\mathfrak{n}_i$;

iii) for $(a_1, \ldots, a_m) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_m$, there is $a \in A$ with $\overline{a} = \overline{a}_i$ in $\boldsymbol{k}_i$.

Proof i) If $\mathfrak{n}_i \subseteq \mathfrak{n}_j$, then $\mathcal{O}_j = A_{\mathfrak{n}_j} \subseteq A_{\mathfrak{n}_i} = \mathcal{O}_i$.

ii) Suppose $I \subset A$ is a proper ideal. We will show that $I \subset \mathfrak{n}_i$ for some i. Suppose not. For each i choose $a_i \in I \setminus \mathfrak{n}_i$. Also for $i \neq j$ choose $b_{i,j} \in \mathfrak{n}_i \setminus \mathfrak{n}_j$. Then

$$c_j = \prod_{i \neq j} b_{i,j} \in \mathfrak{n}_i \setminus \mathfrak{n}_j \text{ for all } i \neq j.$$

Thus $a_jc_j \in_i \setminus \mathfrak{n}_j$ for all $i \neq j$ and

$$d = \sum a_j c_j \in I \setminus \mathfrak{n}_i \text{ for all } i.$$

Thus $1/d \in \mathcal{O}_i$ for all i, so $1/d \in A$. But then $1 \in I$, a contradiction.

iii) We know that $\mathcal{O}_i = A_{\mathfrak{n}_i}$ and $\mathfrak{m}_i = \mathfrak{n}_i A_{\mathfrak{n}_i}$. Thus $\boldsymbol{k}_i = A_{\mathfrak{n}_i}/\mathfrak{n}_i A_{\mathfrak{n}_i} = A/\mathfrak{n}_i$. Now we can apply the Chinese Remainder Theorem. □

Lemma 5.4 *Suppose $(K, \mathcal{O})$ is a valued field and L/K is algebraic. If $\mathcal{O}_1 \subseteq \mathcal{O}_2$ are valuation rings of L with $\mathcal{O}_i \cap K = \mathcal{O}$, then $\mathcal{O}_1 = \mathcal{O}_2$.*

Proof Then $\overline{\mathcal{O}}_1 = \mathcal{O}_1/\mathfrak{m}_2$ in $\mathcal{O}_2/\mathfrak{m}_2$ is a valuation ring in $\boldsymbol{k}_2$ and $\boldsymbol{k} \subset \overline{O}_1$. But $\boldsymbol{k}_2/\boldsymbol{k}$ is algebraic, thus $\overline{\mathcal{O}}_1$ is a field. Since it's a valuation ring its fraction field must be all of $\boldsymbol{k}_2$. Thus $\overline{O}_1 = \boldsymbol{k}_2$. Since $\mathfrak{m}_2 \subseteq \mathfrak{m}_1$, we must have $\mathcal{O}_1 = \mathcal{O}_2$. □

The following analysis will be the key to several of our main results in this section. Let $(K, \mathcal{O})$ be a valued field. Suppose F/K be a finite Galois extension and $\mathcal{O}_1, \ldots, \mathcal{O}_m$ are distinct extensions of $\mathcal{O}$ to F. Let $G = \{\sigma \in \mathrm{Gal}(F/K) : \sigma(\mathcal{O}_1) = \mathcal{O}_1\}$ and let $L \subseteq F$ be the fixed field of G. We will make two observations.

Lemma 5.5 *Under the assumptions above with $m > 1$:*
i) $(K, \mathcal{O})$ is not henselian;
ii) $(L, \mathcal{O}_1 \cap L)$ is a proper immediate extension of $(K, \mathcal{O})$

Proof Let $\mathcal{O}'_i = \mathcal{O}_i \cap L$ for $i = 1, \ldots, m$.

claim If $i > 1$, then $\mathcal{O}'_i \neq \mathcal{O}'_1$.

If $\mathcal{O}'_i = \mathcal{O}'_1$, then $\mathcal{O}_1$ and $\mathcal{O}_i$ are extensions of $\mathcal{O}'_1$ from L to F. But then by Theorem 3.24, there is $\sigma \in \mathrm{Gal}(F/L) = G$ with $\sigma(\mathcal{O}_1) = \mathcal{O}_i$, contradicting the definition of G.

Let $A = \mathcal{O}'_1 \cap \cdots \cap \mathcal{O}'_m$. Let $\mathfrak{n}_i = \mathcal{O}_i \cap A$.

claim If $i \geq 2$, then $\mathfrak{n}_i \neq \mathfrak{n}_1$.

By Lemma 5.1, if $\mathfrak{n}_i = \mathfrak{n}_1$, then $\mathcal{O}'_1 = A_{\mathfrak{n}_1} = A_{\mathfrak{n}_i} = \mathcal{O}'_i$, a contradiction.

By Lemma 3.21 we can find $a \in A$ such that $a = 1 (\mathrm{mod}\ \mathfrak{m}_1)$ and $a \in \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_m$, where $\mathfrak{m}_i$ is the maximal ideal of $\mathcal{O}_i$.

As $\mathfrak{m}_i \cap K = \mathfrak{m}_K$ we must have $a \notin K$. Let

$$f(X) = X^n + b_{n-1}X^{n-1} + \ldots b_0 = (X - a)(X - \alpha_2) \cdots (X - \alpha_n)$$

be the minimal polynomial for a over K, where $b_0, \ldots, b_{n-1} \in K$ and $\alpha_2, \ldots, \alpha_n \in F$.

claim $\alpha_2, \ldots, \alpha_n \in \mathfrak{m}_1$.

Let $i \geq 2$. There is $\sigma \in G(F/K)$ such that $\sigma(a) = \alpha_i$. We know that $a \in A \subset L$ and any $\sigma \in G$ fixes L pointwise. Thus $\sigma \notin G$ and $\sigma^{-1}(\mathcal{O}_1) = \mathcal{O}_j$ for some $j \neq 1$. But $a \in \mathfrak{m}_j$. Thus $\alpha_i = \sigma(a) \in \mathfrak{m}_1$.

It follows that $b_{n-1} = -a - \alpha_2 - \cdots - \alpha_n = -1 (\mathrm{mod}\ \mathfrak{m}_1)$ and $b_0, \ldots, b_{n-2} \in \mathfrak{m}_1$.

claim $(K, \mathcal{O})$ is not henselian.

Clearly $f(1) \in \mathfrak{m}_{\mathcal{O}}$. Let $g(X) = (X - \alpha_2) \cdots (X - \alpha_n)$. Then $f'(X) = (X - a)g'(X) + g(X)$. Thus

$$f'(1)(\mathrm{mod}\ \mathfrak{m}_1) = (1 - a)g'(1) + g(1)(\mathrm{mod}\ m_1) = 1(\mathrm{mod}\ \mathfrak{m}_1).$$

Thus $f'(1) \neq 0(\mathrm{mod}\ \mathfrak{m}_{\mathcal{O}})$. If K were henselian, f would not be irreducible. Thus K is not henselian.

To show that $(L, \mathcal{O}'_1)$ is an immediate extension we make some minor modifications to the proof above. Suppose c is a unit in $\mathcal{O}'_1$ we can find $a \in A$ such that $a = c(\mathrm{mod}\ \mathfrak{m}_1)$ but $a \in \mathfrak{m}_i$ for $i > 1$. Let f be the minimal polynomial for a over K. Arguing as above

$$f(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0 = (X - a)(X - \alpha_2) \cdots (X - \alpha_d)$$

where $b_{d-1} = -c(\mathrm{mod}\ \mathfrak{m}_1)$ and $b_0, \ldots, b_{d-2} \in \mathfrak{m}_1$. But $-(c + \alpha_2 + \cdots + \alpha_d) = b_{d-1} \in K$ and $\overline{c} = \overline{b}_{d-1}$. Thus the residue field does not extend.

We need to show the value group does not extend. We let v denoted the valuation on L. Let $x \in L$. We must find $y \in K$ with $v(x) = v(y)$. We can find $a \in A$ such that $a - 1 \in \mathfrak{m}_1$ and $a \in \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_m$. Then $v(a) = 0$ and $v(\sigma(a)) = 0$ for all $\sigma \in G$. Since $a \in \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_m$, as above, $v(\sigma(a)) > 0$ for all $\sigma \in \mathrm{Gal}(F/K) \setminus G$. We claim that we can choose N large enough we can ensure that

$$v(a^N x) \neq v(\sigma(a^N x)) \text{ for all } \sigma \in \mathrm{Gal}(F/K) \setminus G.$$

For any particular $\sigma \in \mathrm{Gal}(F/K) \setminus G$, $v(a^r x) = v(x)$ and $v(\sigma(a^r x)) = rv(\sigma(a)) + v(\sigma(x))$. Since $v(\sigma(a)) > 0$, for all but one value of r these are unequal. Thus, since $\mathrm{Gal}(F/K)$ is finite, we can choose N as desired.

Let $a^N x = \alpha_1, \ldots, \alpha_n$ be the distinct conjugates of $a^N x$ over K. Let

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_n) = X^n + b_{n-1}X^{n-1} + \cdots + b_0.$$

For $1 < i \leq n$, $\alpha_i = \sigma(a^N x)$ for some $\sigma \in \mathrm{Gal}(F/K) \setminus G$ [note that any $\tau \in G$ fixes $a^N x \in L$]. Thus $v(\alpha_i) \neq v(\alpha_1)$ for $i > 1$.

First suppose $v(\alpha_i) > v(\alpha_1)$ for all $i > 1$. Then $b_{n-1} = -\sum \alpha_i$, $v(x) = v(a^N x) = v(b_{n-1}) \in v(K)$, as desired. In general suppose that $v(\alpha_i) < v(\alpha_1)$ for $1 < i \leq k$ and $v(\alpha_i) > v(\alpha_1)$ for $k < i$. Note that

$$b_{n-j} = (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \alpha_{i_1} \cdots \alpha_{i_n}.$$

Thus

$$v(b_{n-k}) = v(\alpha_2 \cdots \alpha_k) \text{ and } v(b_{n-k-1}) = v(\alpha_1 \cdots \alpha_k).$$

Thus $v(x) = v(\alpha_1) = v(b_{n-k-1}/b_{n-k}) \in v(K)$.

Thus L is an immediate extension of K. $\square$

Theorem 5.6 *Let $(K, \mathcal{O})$ be a valued field. The following are equivalent:*

i) $(K, \mathcal{O})$ is henselian;

ii) For any separable algebraic extension L/K there is a unique extension of $\mathcal{O}$ to a valuation ring of L;

iii) For any algebraic extension L/K there is a unique extension of $\mathcal{O}$ to a valuation ring of L

iv) If $f(X) \in \mathcal{O}[X]$ is monic irreducible and $\overline{f}(X)$ is non-constant, then there is and irreducible $\overline{g}(X) \in \boldsymbol{k}[X]$ and $n \geq 1$ such that $\overline{f}(X) = \overline{g}(X)^n$.

v) If $f, g, h \in \mathcal{O}[X]$ is monic and $\overline{f} = \overline{g}\overline{h}$ where $\overline{g}$ and $\overline{h}$ are relatively prime, then there are $g_1, h_1 \in \mathcal{O}[X]$ such that $\overline{g}_1 = \overline{g}$, $\overline{h}_1 = \overline{h}$ and g_1 and $\overline{g}$ have the same degree.

Proof i) $\Rightarrow$ ii) Suppose not. Then we can find F/K a finite Galois extension such that $\mathcal{O}$ has multiple extensions $\mathcal{O}_1, \ldots, \mathcal{O}_m$ each of which are conjugate under $\mathrm{Gal}(F/K)$. Now we can apply Lemma 5.5 to show that $(K, \mathcal{O})$ is not henselian.

ii) $\Rightarrow$ iii) Let $K \subseteq F \subseteq L$ be the separable closure of K in L. By ii) there is a unique extension of the valuation to F. Since L/F is purely inseparable and there is a unique extension of the valuation to L.

iii) $\Rightarrow$ iv) In K^{alg} we can factor

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i).$$

Let $\mathcal{O}^*$ and $\mathfrak{m}^*$ denote the valuation ring and maximal ideal of an extension to K^{alg}.

Since $f \in \mathcal{O}[X]$, $\prod \alpha_i \in \mathcal{O}$, thus we can not have $v(\alpha_i) < 0$ for all i. Since any two roots are conjugate and there is a unique extension of the valuation ring to K^{alg} we must have all of the $\alpha_i \in \mathcal{O}$ or all of the $\alpha_i \notin \mathcal{O}$, but the latter option is not possible.

Thus, $\overline{f}(X) = \prod (X - \overline{\alpha}_i)$. To show that $\overline{f}$ is a power of an irreducible polynomial in $k[X]$ it is enough to show that we can not fact $\overline{f} = \overline{g}\overline{h}$ where $\overline{g}$ and $\overline{h}$ are relatively prime and monic. Suppose we can. If $\overline{g}(\overline{\alpha_i}) = 0$, then $g(\alpha_i) \in \mathfrak{m}^*$ and for any $\sigma \in \mathrm{Gal}(K^{\mathrm{alg}}/K)$, $g(\sigma(\alpha_i)) \in \sigma(\mathfrak{m}^*) = \mathfrak{m}^*$. But all of the roots of f are conjugate. Thus they are all roots of $\overline{g}$, a contradiction.

iv) $\Rightarrow$ v) Let $f = q_1 \cdot q_m$ be an irreducible factorization of f in $\mathcal{O}[X]$. into monic factors. For each i, there is a monic $p_i \in \mathcal{O}[X]$ such that $\overline{q}_i = \overline{p}_i^{n_i}$. We can find $J \subseteq \{1, \ldots, d\}$ such that $\overline{g} = \prod_{i \in J} \overline{p}_i^{n_i}$. Let

$$\overline{h} = \prod_{i \notin J} \overline{p}_i^{n_i}.$$

Let

$$g_1 = \prod_{i \in J} p_i^{n_i} \text{ and } h_1 = \prod_{i \notin J} p_i^{n_i}.$$

Then $\overline{f} = \overline{g}_1\overline{h}_1$ and $\overline{g}$ and g_1 have the same degree.

v) $\Rightarrow$ i) Suppose $f(X) \in \mathcal{O}[X]$ and $f(X) = X^d + X^{d-1} + \sum a_i X^i$ where $a_i \in \mathfrak{m}_i$. In $\boldsymbol{k}[X]$ we can factor $\overline{f}(X) = \overline{h}(X)(X+1)$, Since $\overline{f}'(-1) = \pm 1$, $\overline{h}(-1) \neq 0$. Thus $\overline{h}(X)$ and $(X+1)$ are relatively prime. By iv) there is $a \in K$ with $\overline{a} = -1$ such that $(X-a)$ is an irreducible factor of f. □

Exercise 5.7 Show that it $(K, \mathcal{O})$ is henselian and $(L, \mathcal{O}_L)$ is an algebraic extension, then $(L, \mathcal{O}_L)$ is henselian.

Exercise 5.8 Suppose $(K, \mathcal{O})$ is henselian, $F \subseteq K$ and F is separably closed in K. Prove that $(F, \mathcal{O} \cap F)$ is henselian.

5.2 Algebraically Maximal Fields

Definition 5.9 We say that a valued field $(K, \mathcal{O})$ is *algebraically maximal* if it has no proper separable algebraic immediate extensions.

Corollary 5.10 *An algebraically maximal valued field $(K, \mathcal{O})$ is henselian.*

Proof If $(K, \mathcal{O})$ is not henselian we can find F/K a finite Galois extension with multiple extensions of $\mathcal{O}$ to F. By Lemma 5.5, we can find an intermediate field $K \subset L \subseteq F$ with L/K immediate. □

The converse is true under some additional assumptions which will apply in many of our settings.

Definition 5.11 We say that $(K, \mathcal{O})$ has *equicharacteristic zero* if K and the residue field $\boldsymbol{k}$ have characteristic zero.

We say that $(K, \mathcal{O})$ is *finitely ramified* if $\boldsymbol{k}$ has characteristic $p > 0$ and $\{v(x) : 0 < v(x) < v(p) : x \in K^\times\}$ is finite.

Note that the later condition is true for the p-adics.

Exercise 5.12 Prove that if $(K, \mathcal{O}_K)$ is a finite algebraic extension of $(\mathbb{Q}_p, \mathbb{Z}_p)$, then $(K, \mathcal{O}_K)$ is finitely ramified.

Exercise 5.13 Suppose L/K is finitely ramified. Show that the set $\{v(x) : 0 < v(x) < v(n)\}$ is finite for all $n \in \mathbb{Z}$.

Theorem 5.14 *If $(K, \mathcal{O})$ is henselian and equicharacteristic zero or finitely ramified, then $(K, \mathcal{O})$ is algebraically maximal.*

Proof Suppose F is an algebraic immediate extension and $x \in F \setminus K$. Without loss of generality F/K is finite. There is $L \supseteq K$ such that L/K is Galois. There is a unique extension $\mathcal{O}_L$ of $\mathcal{O}$. Let v be the valuation associated with $\mathcal{O}_L$. For and $a \in K$, we have $v(x-a) = v(b)$ for some $b \in K$, but then $v(\sigma(x) - a) = v(b)$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Let $d = [L:K]$ Let

$$a = \frac{1}{d} \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in K.$$

Since F/K is immediate, there is $b \in K$ such that $v((x-a)/b) = 0$ and $c \in K$ such $v(\frac{x-a}{b} - c) > 0$. Then

$$v(x - (a + bc)) > v(b) = v(x - a).$$

Since $(K, \mathcal{O})$ is equicharacteristic zero or finitely ramified, repeating this argument finitely many times in the case where the residue field has characteristic p we can find $\widehat{a} \in K$ such that

$$v(x - \widehat{a}) > v(x - a) + v(n)$$

(if the residue field has characteristic zero $v(n) = 0$ so we need only do this once). Then

$$\begin{aligned} v(n) + v(a - \widehat{a}) &= v(n(a - \widehat{a})) \\ &= v\left(\sum_{\sigma \in \mathrm{Gal}(L/K)} (\sigma(x) - \widehat{a}) \right) \\ &\geq \min(v(\sigma(x) - \widehat{a})) \\ &\geq v(x - \widehat{a}) \text{ since } v(w) = v(\sigma(w)) \text{ for all } w \in L \\ &> v(x - a) + v(n) \\ &= v(a - \widehat{a}) + v(n) \end{aligned}$$

a contradiction. The last line holds since $v(a - \widehat{a}) = v((a - x) + (x - \widehat{a}))$ and $v(x - \widehat{a}) > v(x - a)$. □

Corollary 5.15 *If $(K, \mathcal{O})$ is henselian with divisible value group and algebraically closed residue field of characteristic zero, then K is algebraically closed.*

Proof If L/K is a proper algebraic extension, then we can extend the valuation to L and, by Lemma 3.16 it must be an immediate extension, contradicting Theorem 5.14. □

Corollary 5.16 *If k is an algebraically closed field of characteristic zero, then the Puiseux series field $k\langle T \rangle$ is algebraically closed.*

This doesn't work in characteristic $p > 0$. The series solution to $f(X) = X^p - X = T^{-1}$ should be of the form

$$a + T^{-1/p} + T^{-1/p^2} + \cdots + T^{-1/p^n} + \ldots$$

where $a \in \mathbb{F}_p$, which is not a Puiseux series. This series is in the immediate extension $\mathbb{F}_p(((\mathbb{Q})))$ and thus in the separable closure of the Puiseux series in the Hahn series. This shows that henselianity alone is not enough to conclude algebraically maximal. Kedlaya in [18] gives a characterization of the algebraic closure of $\mathbb{F}_p^{\mathrm{alg}}((T))$.

If k is real closed and Γ is divisible, $k^{\mathrm{alg}}\langle T\rangle$ is a degree 2 extension of $k\langle T\rangle$. Thus $\boldsymbol{k}\langle T\rangle$ is real closed. This is true in much more generality.

Corollary 5.17 *Let $(K,<)$ is an ordered field and let $\mathcal{O}$ be the convex hull of a subring. Suppose $(K,\mathcal{O})$ is henselian with real closed residue field $\boldsymbol{k}$ and divisible value group Γ. Then K is real closed.*

Proof Let L be the real closure of $(K,<)$ and let $\mathcal{O}^*$ be the convex hull of $\mathcal{O}$ in K. Then, since the orderings agree, $(K,\mathcal{O})\subseteq(L,\mathcal{O}^*)$. The residue field $\boldsymbol{k}_L$ is real closed and algebraic over $\boldsymbol{k}$, so it must equal $\boldsymbol{k}$. Similarly, the value group of L is contained in the divisible hull of $v(K)$ and hence equals $v(K)$. Thus L/K is an immediate extension and, since $(K,\mathcal{O})$ is henselian and equicharacteristic zero, $L=K$. □

5.3 Henselizations

Infinite Galois Theory

We quickly review some facts we need about the Galois Theory of infinite algebraic extensions. The reader should consult [16] §8.6 or [14] §1.

Let K be a field. The *separable closure* of K is K^s the maximal separable algebraic extension of K. When we apply these results we will be working almost exclusively in the setting where K has characteristic zero so there would be no harm in working with K^{alg} the algebraic closure of K. We let $\mathrm{Gal}(K^s/K)$ be the Galois group of all automorphisms of K^s that are the identity on K.

Suppose L/K is a finite Galois extension. If $\sigma\in\mathrm{Gal}(K^s/K)$, then $\sigma|L\in\mathrm{Gal}(L/K)$. Moreover if $\tau\in\mathrm{Gal}(L/K)$, there is $\widehat{\tau}\in\mathrm{Gal}(K^s/K)$ extending τ. Thus

$$\mathrm{Gal}(K^s/K)=\varprojlim_{L/K\text{ finite Galois}}\mathrm{Gal}(L/K)$$

is a profinite group. We topologize $\mathrm{Gal}(K^s/K)$ by taking the weakest topology such that for all finite Galois extensions L/K and $\sigma\in\mathrm{Gal}(L/K)$, $U_\sigma=\{\tau\in\mathrm{Gal}(K^s/K):\sigma\subseteq\tau\}$ is open.

If H is a subgroup of $\mathrm{Gal}(K^s/K)$, let $\mathrm{Fix}(H)=\{x\in K^s:\sigma(x)=x$ for all $\sigma\in H\}$ be the fixed field of H.

Theorem 5.18 (Fundamental Theorem of Infinite Galois Theory) *The maps $L\mapsto\mathrm{Gal}(K^s/L)$ and $H\mapsto\mathrm{Fix}(H)$ are inclusion-reversing bijections between the collection of intermediate fields $K\subseteq L\subseteq K^s$ and closed subgroups of $\mathrm{Gal}(K^s/K)$.*

Henselizations

Let $(K, \mathcal{O})$ be a valued field, let K^s be the separable closure of K and let $\mathcal{O}^s$ be an extension of $\mathcal{O}$ to K. Let $G(\mathcal{O}^s) = \{\sigma \in \mathrm{Gal}(K^s/K) : \sigma(\mathcal{O}^s) = \mathcal{O}^s\}$. We call $G(\mathcal{O}^s)$ the *decomposition group.*

Lemma 5.19 *$G(\mathcal{O}^s)$ is a closed subgroup of* $\mathrm{Gal}(K^s/K)$.

Proof Suppose $\sigma \notin G(\mathcal{O}^s)$. There is $x \in \mathcal{O}^s$ with $\sigma(x) \notin \mathcal{O}^s$. Let L/K be finite Galois with $x \in L$ and let $\tau = \sigma|L$. Then $\sigma \in U_\tau$ and $U_\tau \cap G(\mathcal{O}^s)$ is empty. $\square$

Definition 5.20 Let $K^h(\mathcal{O}^s)$ be the fixed field of $G(\mathcal{O}^s)$ and let $\mathcal{O}^h(\mathcal{O}^s) = \mathcal{O}^s \cap K^h$. We call $(K^h(\mathcal{O}^s), \mathcal{O}^h(\mathcal{O}^s))$ a *henselization* of $(K, \mathcal{O})$.

When no confusion arises we will suppress $\mathcal{O}^s$ and write $(K^h, \mathcal{O}^h)$.

Lemma 5.21 *i) $\mathcal{O}^s$ is the unique extension of $\mathcal{O}^h$ to K^s. Thus $(K^h, \mathcal{O}^h)$ is henselian.*

ii) $(K^h, \mathcal{O}^h)$ is an immediate extension of K.

Proof i) Suppose $\mathcal{O}_1^s$ is an extension of $\mathcal{O}^h$ to K^s. By Theorem 3.24, $\mathcal{O}^s$ and $\mathcal{O}_1^s$ are conjugate under $\mathrm{Gal}(K^s/K)$. But $G(\mathcal{O}^s)$ is the Galois group of K^s/K^h, so any element of $\mathrm{Gal}(K^s/K)$ fixes $\mathcal{O}^s$. Hence $\mathcal{O}^s = \mathcal{O}_1^s$

ii) follows from Lemma 5.5. $\square$

Lemma 5.22 *If $(K_1, \mathcal{O}_1)$ is a henselian extension of $(K, \mathcal{O})$ then there is a unique embedding $j : (K^h, \mathcal{O}^h) \to (K_1, \mathcal{O}_1)$ fixing K pointwise.*

Proof Without loss of generality, by Exercise 5.8, we may assume that $K_1 \subseteq K^s$. Since K_1 is henselian, there is a unique extension $\mathcal{O}_1^s$ of $\mathcal{O}_1$ to K^s. Then $\mathrm{Gal}(K^s/K_1) \subseteq G(\mathcal{O}_1^s)$. Thus $K_1 \supseteq K^h(\mathcal{O}_1^s)$. By Theorem 3.24 there is $\sigma \in \mathrm{Gal}(K^s/K)$ with $\sigma(\mathcal{O}^s) = \mathcal{O}_1^s$, but then $\sigma(K^h) = K^h(\mathcal{O}_1^s) \subseteq K_1$ and $\sigma|K^h$ is the desired embedding of $(K^h, \mathcal{O}^h)$ into $(K_1, \mathcal{O}_1)$.

Suppose $j : (K^h, \mathcal{O}^h) \to (K_1, \mathcal{O}_1)$ is another embedding. We can extend j to $\tau \in \mathrm{Gal}(K^s/K)$. Then $\tau(\mathcal{O}^s) \cap \tau(K^h) = \mathcal{O}_1^s \cap \tau(K^h)$. But $(\tau(K^h), \tau(O^h))$ is henselian, so $\mathcal{O}_1^s$ is the unique extension of $\tau(\mathcal{O}^s)$ to K^s and $\tau(\mathcal{O}_s) = \mathcal{O}_1^s$. Thus $\tau^{-1}\sigma(\mathcal{O}^s) = \mathcal{O}^s$ and $\tau^{-1}\sigma \in G(\mathcal{O}^s)$. Since K^h is the fixed field of $G(\mathcal{O}_s)$, σ and τ agree on K^h. Thus $j = \sigma|K^h$. $\square$

Exercise 5.23 In particular if $\mathcal{O}^s$ and $\mathcal{O}_1^s$ are distinct extensions of $\mathcal{O}$, then there is a unique isomorphism between $(K^h(\mathcal{O}^s), \mathcal{O}^s)$ and $(K^h(\mathcal{O}_1^s), \mathcal{O}(\mathcal{O}_1^s))$ fixing K.

Summarizing we have proved:

Theorem 5.24 *Let $(K, \mathcal{O})$ be a valued field. There is a henselization $(K^h, \mathcal{O}^h)$, i.e. a henselian immediate separable algebraic extension of $(K, \mathcal{O})$ such that if $(K_1, \mathcal{O}_1)$ is a henselian extension of $(K, \mathcal{O})$ then there is a unique embedding $j : (K^h, \mathcal{O}^h) \to (K_1, \mathcal{O}_1)$ with $j|K$ the identity.*

Corollary 5.25 *a) Let (K, v) be an algebraically closed valued field of characteristic 0 and let $A \subset K$. Show that* $\mathrm{dcl}(A)$*, the definable closure of A, is exactly the henselization of the fraction field of A.*

Proof Let F be the fraction field of A. Then F^{alg} is an elementary submodel of (K, v). The valued field automorphisms of F^{alg} that fixes A are exactly the elements of the decomposition group $G(\mathcal{O}_{\mathbb{F}^{\mathrm{alg}}})$, when has fixed field F^h. It follows that $F^h = \mathrm{dcl}(A)$. $\square$

Exercise 5.26 Let (K, v) be an algebraically closed field of characteristic $p > 0$. Prove that $A = \mathrm{dcl}(A)$ if and only if A is perfect and henselian.

5.4 Pseudolimits

Let K be a valued field with valuation v. We will consider sequences $(a_\alpha : \alpha < \delta)$ where δ is a limit ordinal and $a_\alpha \in K$ for $\alpha < \delta$. Frequently, we will simplify notation by just writing (a_α).

Definition 5.27 We say that a is a *pseudolimit* of $(a_\alpha : \alpha < \delta)$ if the sequence $(v(a - a_\alpha) : \alpha < \delta)$ is eventually strictly increasing. We write $(a_\alpha) \rightsquigarrow a$. We let $\gamma_\alpha = v(a - a_\alpha)$.

Exercise 5.28 Suppose $(a_\alpha) \rightsquigarrow a$ and $b \in K$.
a) Show $(a_\alpha + b) \rightsquigarrow a + b$.
b) Show $(ba_\alpha) \rightsquigarrow ba$

Lemma 5.29 *Suppose $(a_\alpha) \rightsquigarrow a$. Then either:*
i) $(v(a_\alpha))$ is eventually constant and equal to $v(a)$;
ii) $(v(a_\alpha))$ is eventually strictly increasing and $v(a_\alpha) < v(a)$ for sufficiently large α.

Proof Suppose γ_α is increasing for $\alpha \geq \alpha_0$ and $v(a) \leq v(a_{\alpha_0})$. Then $v(a - a_{\alpha_0}) \geq v(a)$ and $\alpha > \alpha_0$, $v(a_\alpha) = v(a)$, since

$$v(a - \alpha) > v(a - a_{\alpha_0}) \geq v(a).$$

Thus we are in case i).

If this never happens then $v(a_\alpha) < v(a)$ for all sufficiently large α and for $\beta > \alpha$ Then $\gamma_\alpha = v(a_\alpha)$ and $v(a_\alpha) < v(a_\beta)$ for sufficiently large $\alpha < \beta$ and case ii) holds. $\square$

Lemma 5.30 *Suppose $(K, v) \subseteq (L, v)$ is an immediate extension and $x \in L \setminus K$. There is a sequence (a_α) in K such that $(a_\alpha) \rightsquigarrow x$ and (a_α) has no pseudolimit in K.*

Proof Let $a_0 = 0$. Suppose we have a_α. Since $v(K) = v(L)$ we can find $b \in K$ such that $v(b) = v(x - a_\alpha)$. Since $\boldsymbol{k}_K = \boldsymbol{k}_L$, there is $c \in K$ such that $0 \neq \bar{c} = \mathrm{res}(\frac{x - a_\alpha}{b})$. Thus

$$v(x - (a_\alpha + bc)) > v(b) = v(x - a_\alpha).$$

Let $a_{\alpha+1} = a_\alpha + cb$. Then $v(x - a_{\alpha+1}) > v(x - a_\alpha)$.

Suppose δ is a limit ordinal and we have constructed $(a_\alpha : \alpha < \delta)$ with $v(x - a_\alpha) < v(x - a_\beta)$ for $\alpha < \beta < \delta$. If there is $b \in K$ such that $v(x - b) > v(x - a_\alpha)$ for all $\alpha < \delta$ let $a_\delta = b$ and continue. If no such b exists (a_α) is our desired sequence. $\square$

A sequence (a_α) in K might not have a pseudolimit in K, but we can tell if it could have pseudolimit in an extension.

Definition 5.31 We say that (a_α) is *pseudocauchy* if there is α_0 such that $v(a_\delta - a_\beta) > v(a_\beta - a_\alpha)$ for $\delta > \beta > \alpha > \alpha_0$.

Lemma 5.32 *i) If $(a_\alpha) \rightsquigarrow a$, then (a_α) is pseudocauchy.*

ii) If (a_α) is pseudocauchy, there is an elementary extension $(K, v) \prec (L, v)$ such that (a_α) has a pseudolimit in L.

Proof i) If $\delta > \beta > \alpha$ are suitably large, then $a_\delta - a_\beta = (a - a_\beta) - (a - a_\delta)$. Thus $v(a_\delta - a_\beta) = v(a - a_\beta)$. Similarly, $v(a_\beta - a_\alpha) = v(a - a_\alpha)$ and, thus, $v(a_\delta - a_\beta) > v(a_\beta - a_\alpha)$ and the sequence is pseudocauchy.

ii) Consider the type $t(v) = \{v(x - a_\beta) > v(x - a_\alpha) : \text{for } \alpha_0 < \alpha < \beta\}$. Let $\Delta \subset t(v)$ be finite. Choose $\delta > \alpha$ for all a_α occurring in Δ. Then $v(a_\delta - a_\beta) > v(a_\beta - a_\alpha) = v(a_\delta - a_\beta)$ for $\delta > \beta > \alpha > \alpha_0$. Thus $t(v)$ is finitely satisfiable and thus realized in some elementary extension of K. $\square$

Corollary 5.33 *If (a_α) is pseudocauchy, then $(v(a_\alpha))$ is either eventually constant or eventually strictly increasing.*

Exercise 5.34 Prove that in a Hahn field $\boldsymbol{k}(((\Gamma)))$ every pseudocauchy sequence has a pseudolimit and conclude that Hahn fields have no proper immediate extensions. (This is essentially the same proof we gave in §1.)

The next lemma is important but not surprising and rather routine. We omit the proof and refer the reader to [9] Proposition 4.7 for the proof.

Lemma 5.35 *Suppose $(a_\alpha) \rightsquigarrow a$ and $f(X) \in K[X]$. Then $(f(a_\alpha)) \rightsquigarrow f(a)$.*

Thus if (a_α) is pseudocauchy, so is $(f(a_\alpha))$.

There is an important dichotomy among pseduocauchy sequences.

Definition 5.36 Let (a_α) be a pseudocauchy sequence in K. We say that (a_α) is of *algebraic type* if there is a nonconstant polynomial $f(X) \in K[X]$ such that $(v(f(a_\alpha)))$ is eventually strictly increasing. Otherwise we say (a_α) is of *transcendental type*.

If (a_α) is of transcendental type, then $(v(f(a_\alpha)))$ is eventually constant for all $f \in K[X]$.

Lemma 5.37 *If (a_α) is a pseudocauchy sequence over K of transcendental type, then (a_α) has no pseudolimit in K and there is an extension of v to the field of rational functions $K(X)$ with $v(f) =$ eventual value of $v(f(a_\alpha))$. Then $(K(X), v)$ is an immediate extension of K where $(a_\alpha) \rightsquigarrow X$.*

If L/K is a valued field extension of K and $(a_\alpha) \rightsquigarrow a$ in L, then sending X to a we get a valued field isomorphism between $K(X)$ and $K(a)$ fixing K.

Proof If $(a_\alpha) \rightsquigarrow a$, let $f(X) = X - a$, then $(v(f(a_\alpha)))$ is eventually strictly increasing and the sequence is of algebraic type, a contradiction. Thus (a_α) has no pseudolimit in K.

Let v be defined as above. Then, for α sufficiently large

$$v(fg) = v(f(a_\alpha)) + v(g(a_\alpha)) = v(f) + v(g)$$

and

$$v(f+g) = v(f(a_\alpha) + g(a_\alpha)) \geq \min(v(f(a_\alpha))v(g(a_\alpha))) = \min(v(f), v(g)).$$

Thus v is a valuation on $K(X)$ extending the valuation on K. Clearly, the value group of $K(X)$ is equal to the value group of K. Let $f \in K(X) \setminus K$ with $v(f) = 0$. Then $0 = v(f) = v(f(a_\alpha))$ for sufficiently large α. If $\beta > \alpha$, then $v(f - f(a_\beta)) > v(f - f(a_\alpha)) > v(f(a_\alpha)) = 0$ and $\mathrm{res}(f) = \mathrm{res}(a_\beta)$. Thus $K(X)$ is an immediate extension of K.

Suppose (L, v) is a valued field extension of K and $a \in L$ is a pseudolimit of (a_α). For nonconstant $f \in K[X]$ we have $(f(a_\alpha)) \rightsquigarrow f(a)$. Thus $v(f(a)) = v(f(a_\alpha)) = v(f)$ for sufficiently large α. In particular $f(a) \neq 0$, thus a is transcendental over K and the field isomorphism of $K(X)$ to $K(a)$ obtained by sending X to a preserves the valuation. $\square$

Definition 5.38 If (a_α) is of algebraic type, a *minimal polynomial* of (a_α) is a polynomial g of minimal degree such $(v(g(a_\alpha))$ is eventually increasing.

Lemma 5.39 *Let (a_α) be a pseudocauchy sequence of algebraic type with minimal polynomial $g(X)$ and no pseudolimit in K. Then $g(X)$ is irreducible of degree at least 2. Let a be a zero of g in an extension field of K. Then v extends to a valuation on $K(a)$ where $v(f(a)) =$ eventual value of $v(f(a_\alpha))$, where $f(X) \in K[X]$ of degree less than deg(g). Then $K(a)$ is an immediate extension of K where $(a_\alpha) \rightsquigarrow a$.*

If L/K is any valued field extension of K where $b \in K$ is a zero of g and $(a_\alpha) \rightsquigarrow b$, then the isomorphism $K(a)$ to $K(b)$ obtained by sending a to b, preserves the valuation.

Proof If $g(X) = X - a$ then $(v(g(a_\alpha))) = v(a_\alpha - a)$ is eventually strictly increasing and $(a_\alpha) \rightsquigarrow a$, a contradiction. Thus g has degree at least two. If $g = g_1 g_2$ is a nontrivial factorization of g, then, by minimality of the degree of g, $(v(g_i(a_\alpha)))$ is eventually constant for each i, but then $(v(g(a_\alpha))) = (v(g_1(a_\alpha) + g_2(a_\alpha)))$ is eventually constant, a contradiction. Thus g is irreducible of degree at least two.

Consider the extension $K(a)$ where $g(a) = 0$. Suppose $f_1, f_2 \in K[X]$ have degree less that $\deg(g)$. There are $h, r \in K[X]$ with degree less than $\deg(g)$ such that $f_1 f_2 = hg + r$. Then for α sufficiently large

$$v(f_1) = v(f_1(a_\alpha)), v(f_2) = v(f_2(a_\alpha)) \text{ and } v(f_1 f_2) = v(r) = v(r(a_\alpha)).$$

Then,

$$v(f_1) + v(f_2) = v(f_1(a_\alpha) f_2(a_\alpha)) = v(h(a_\alpha) g(a_\alpha) + r(a_\alpha)).$$

The sequence $(v(h(a_\alpha)g(a_\alpha) + r(a_\alpha))$ is eventually constant, while the sequence $(v(h(a_\alpha)g(a_\alpha))$ is eventually increasing. This is only possible if $v(h(a_\alpha)g(a_\alpha)) > v(r(a_\alpha))$ eventually. But then $v(h(a_\alpha)g(a_\alpha) + r(a_\alpha)) = v(r(a_\alpha))$ eventually and $v(f_1 f_2) = v(f_1) + v(f_2)$ as desired.

The rest of the proof closely follows the proof of Lemma 5.37. $\square$

Corollary 5.40 *Let (K, v) be a valued field. Then every pseudocauchy sequence in K has a pseudolimit in K if and only if K has no proper immediate extensions.*

Exercise 5.41 Prove that K has no proper immediate extensions if and only if K is spherically complete.

We can refine Lemma 5.30 for algebraic immediate extensions.

Lemma 5.42 *Suppose (L, v) is an immediate extension of K and $a \in L \setminus K$ is algebraic over K with minimal polynomial g. Let (a_α) be a pseudocauchy sequence over K with no pseudolimit in K such that $(a_\alpha) \rightsquigarrow a$. Then (a_α) is of algebraic type. In fact $(v(g(a_\alpha)))$ is increasing.*

Proof Let $g(X) = (X - a)h(X)$ where $h \in K(a)[X]$. Then $g(a_\alpha) = (a_\alpha - a)h(a_\alpha)$. The sequence $(v(a_\alpha - a))$ is eventually increasing and the sequence $(v(h(a_\alpha)))$ is either eventually increasing or eventually constant. Thus $v(g(a_\alpha))$ is either eventually increasing or eventually constant. $\square$

Corollary 5.43 *Let (K, v) be a valued field. If every pseudocauchy sequence (a_α) of algebraic type in K has a pseudolimit in K, then K is henselian. Moreover, the converse holds if, in addition (K, v) is either equicharacteristic zero or finitely ramified.*

Proof If every pseudocauchy sequence (a_α) of algebraic type has a pseudolimit in K, then by Lemma 5.42 (K, v) has no proper immediate algebraic extension and, by Theorem am hen, (K, v) is henselian. Note that this direction did not use the additional assumptions on (K, v).

If (K, v) is henselian and either equicharacteristic zero or finitely ramified, then by Theorem 5.10, (K, v) has no proper immediate algebraic extensions. Thus by Lemma 5.39, every pseudocauchy sequence of algebraic type in K has a pseudolimit in K. $\square$

Exercise 5.44 Suppose K is a valued field with value group Γ such that there is a lifting of the residue field $\boldsymbol{k}$ to K and there is $s : \Gamma \to K$ a section of the value group. Show there is a valuation preserving embedding of K into the Hahn field $\boldsymbol{k}(((\Gamma)))$. [Hint: View $\boldsymbol{k}$ as a subfield of K. First show that $\boldsymbol{k}(s(\Gamma))$ embeds into $\boldsymbol{k}(((\Gamma)))$. Then consider a maximal subfield $K_0 \subseteq K$ such that the embedding extends to a valuation preserving embedding of K_0 into $\boldsymbol{k}(((\Gamma)))$.]

Conclude that if K is a real closed field with valuation ring $\mathcal{O}$ a convex subring, residue field $\boldsymbol{k}$ and value group Γ, then there is a valuation preserving embedding of K into $\boldsymbol{k}(((\Gamma)))$.[8]

[8]Mourgess and Ressarye [23] proved the stronger result that we can embedding K into $k(((\Gamma)))$ such that if f is in the image so is any truncation (i.e. initial segment) of f. They used this to prove that every real closed field has an integral part (i.e. a discrete subring Z such that for all $x \in K$, $|[x, x+1) \cap Z| = 1$).