

## Hensel's Lemma

We return to the class of relatively Henselian valued fields defined in §15.3, and characterize it by means of several equivalent Diophantine conditions. Historically, these equivalent formulations were among the main origins of valuation theory. We use these conditions to give several major examples of Henselian field, such as the  $p$ -adic fields, quotient fields of rings of Witt vectors, generalized formal power series field, and Puiseux series fields.

### 18.1 The main variants

We will need the following form of the Taylor expansion formula.

LEMMA 18.1.1. *Let  $(F, v)$  be a valued field and let  $f(X) \in O_v[X]$ . For every  $a \in O_v$  and for every non-negative integer  $k$  one has:*

$$f(a + X) - \sum_{i=0}^k \frac{f^{(i)}(a)}{i!} X^i \in X^{k+1} O_v[X],$$

where  $f^{(i)}(X)$  denotes the formal derivative of  $f(X)$  of order  $i$ .

PROOF. Let  $g(X) = f(a + X)$  and expand  $g(X) = \sum_{i=0}^n c_i X^i$  with  $c_i \in O_v$ . Then

$$f^{(i)}(a) = g^{(i)}(0) = \begin{cases} i!c_i & \text{if } 0 \leq i \leq n, \\ 0 & \text{if } n < i. \end{cases}$$

For  $k' = \min\{k, n\}$  we therefore obtain

$$f(a + X) - \sum_{i=0}^k \frac{f^{(i)}(a)}{i!} X^i = g(X) - \sum_{i=0}^{k'} c_i X^i = \sum_{k' < i \leq n} c_i X^i.$$

The assertion follows. □

As before, given a valued field  $(F, v)$  and a polynomial  $f(X) \in O_v[X]$ , we denote the residue polynomial of  $f(X)$  in  $\bar{F}_v[X]$  by  $\bar{f}(X)$ .

THEOREM 18.1.2. *Let  $E/F$  be a normal extension and let  $v$  be a valuation on  $F$ . The following conditions are equivalent:*

- (a)  $v$  is Henselian relative to  $E$ ;
- (b)  $v$  is Henselian relative to every finite Galois extension  $E_1$  of  $F$  which is contained in  $E$ ;
- (c) if  $f(X)$  is an irreducible monic polynomial in  $O_v[X]$  which splits in  $E$ , then  $\bar{f}(X)$  is a power of an irreducible monic polynomial in  $\bar{F}_v[X]$ ;
- (d) **Hensel's Lemma:** if  $f(X)$  is a monic polynomial in  $O_v[X]$  which splits in  $E$  and if  $\bar{f}(X) = \tilde{g}(X)\tilde{h}(X)$  for some relatively prime polynomials

$\tilde{g}(X), \tilde{h}(X)$  in  $\bar{F}_v[X]$ , then there exist polynomials  $g(X), h(X) \in O_v[X]$  such that

$$f(X) = g(X)h(X), \quad \bar{g}(X) = \tilde{g}(X), \quad \bar{h}(X) = \tilde{h}(X);$$

- (e) for every monic polynomial  $f(X) \in O_v[X]$  which splits in  $E$  and for every simple zero  $\bar{a} \in \bar{F}_v$  of  $\bar{f}(X)$  there is a zero  $a \in O_v$  of  $f(X)$  with residue  $\bar{a}$  in  $\bar{F}_v$ ;
- (f) **The Hensel–Rychlik condition:** if  $g(X) \in O_v[X]$  splits in  $E$  and  $a \in O_v$  satisfies  $v(g(a)) > 2v(g'(a))$ , then there exists a zero  $c$  of  $g(X)$  such that

$$v(a - c) = v(g(a)/g'(a)).$$

PROOF. (a) $\Leftrightarrow$ (b): The reduction from the case of normal extensions to the case of Galois extensions is by Proposition 14.2.5(a). The additional reduction from the Galois case to the finite Galois case (as in (b)) is immediate.

(a) $\Rightarrow$ (c) By (a),  $v$  has a unique extension  $u$  to  $E$  (up to equivalence). Let  $a \in E$  be a zero of  $f(X)$ . By assumption,  $f(X)$  splits in  $E$  as

$$f(X) = \prod_{i=1}^n (X - \sigma_i(a))$$

for some  $\sigma_1, \dots, \sigma_n \in \text{Aut}(E/F) = Z(u/v)$ . Since  $O_u$  is integrally closed (Proposition 3.1.3),  $\sigma_i(a) \in O_u$ ,  $i = 1, \dots, n$ . We may therefore take residues in  $\bar{E}_u$  to obtain

$$\bar{f}(X) = \prod_{i=1}^n (X - \overline{\sigma_i(a)}) = \prod_{i=1}^n (X - \bar{\sigma}_i(\bar{a})),$$

where  $\bar{\sigma}_i$  is the image of  $\sigma_i$  under the epimorphism  $\Phi: \text{Aut}(E/F) \rightarrow \text{Aut}(\bar{E}_u/\bar{F}_v)$  of Theorem 16.1.1. Thus  $\bar{f}(X) \in \bar{F}_v[X]$  splits in  $\bar{E}_u[X]$  and its zeros are all conjugate to  $\bar{a}$  over  $\bar{F}_v$ . Since  $\bar{F}_v[X]$  is a unique factorization domain, this implies that  $\bar{f}(X)$  is a power of  $\text{irr}(\bar{a}, \bar{F}_v)$ .

(c) $\Rightarrow$ (d): We may assume that  $\tilde{g}(X), \tilde{h}(X)$  are monic. Let  $u$  be an extension of  $v$  to  $E$ . Write

$$f(X) = f_1(X) \cdots f_k(X),$$

with  $f_i(X) \in F[X]$  monic and irreducible. Again, since  $f(X)$  splits in  $E$  and  $O_u$  is integrally closed, the zeros of  $f(X)$  are in  $O_u$ . Hence, so are the zeros of each  $f_i(X)$ . It follows that

$$f_i(X) \in (O_u \cap F)[X] = O_v[X], \quad i = 1, \dots, k.$$

By (c),  $\bar{f}_i(X) = \bar{r}_i(X)^{m_i}$  for some irreducible monic polynomial  $\bar{r}_i(X) \in \bar{F}_v[X]$  and some positive integer  $m_i$ . Then

$$\tilde{g}(X)\tilde{h}(X) = \bar{f}(X) = \bar{r}_1(X)^{m_1} \cdots \bar{r}_k(X)^{m_k}$$

in  $\bar{F}_v[X]$ . Since  $\bar{F}_v[X]$  is a unique factorization domain and  $\tilde{g}(X)$  and  $\tilde{h}(X)$  are relatively prime, we get after renumbering:

$$\tilde{g}(X) = \prod_{i=1}^l \bar{r}_i(X)^{m_i} = \prod_{i=1}^l \bar{f}_i(X), \quad \tilde{h}(X) = \prod_{i=l+1}^k \bar{r}_i(X)^{m_i} = \prod_{i=l+1}^k \bar{f}_i(X).$$

Now let

$$g(X) = \prod_{i=1}^l f_i(X), \quad h(X) = \prod_{i=l+1}^k f_i(X).$$

Then  $g(X)$  and  $h(X)$  are polynomials in  $O_v[X]$  with residues  $\tilde{g}(X), \tilde{h}(X)$ , respectively, and  $f(X) = g(X)h(X)$ .

(d) $\Rightarrow$ (e): By assumption,  $\bar{f}(X) = (X - \bar{a})\tilde{h}(X)$  for some  $\tilde{h}(X) \in \bar{F}_v[X]$  with  $\tilde{h}(\bar{a}) \neq 0$ . From (d) we obtain polynomials  $g(X), h(X) \in O_v[X]$  such that

$$f(X) = g(X)h(X), \quad \bar{g}(X) = X - \bar{a}, \quad \bar{h}(X) = \tilde{h}(X).$$

Since  $f(X)$  is monic, so are  $\bar{f}(X)$  and  $\bar{h}(X)$ . We obtain:

$$\deg(g) = \deg(f) - \deg(h) = \deg(\bar{f}) - \deg(\bar{h}) = \deg(\bar{g}) = 1.$$

The leading coefficient of  $g(X)$  is in  $G_v$ , so we may assume without loss of generality that  $g(X)$  is in fact monic; thus  $g(X) = X - a$  for some  $a \in O_v$ . Then  $f(a) = 0$  and the residue of  $a$  in  $\bar{F}_v$  is  $\bar{a}$ .

(e) $\Rightarrow$ (b): We may assume for simplicity that  $E/F$  is already a finite Galois extension.

Let  $u$  be an extension of  $v$  to  $E$ . As before, let  $E_Z$  be the decomposition field of  $(E, u)/(F, v)$ . Lemma 15.2.1 yields  $a \in O_{u_Z}$  such that  $u(1 - a) > 0$  and  $(u \circ \sigma)(a) > 0$  whenever  $\sigma \in \text{Gal}(E/F) \setminus Z(u/v)$ . In particular,  $u(a) = 0$ .

Let  $\sigma_1(a), \dots, \sigma_k(a)$  be the distinct  $F$ -conjugates of  $a$ , where  $\sigma_1, \dots, \sigma_k \in \text{Aut}(E/F)$  and  $\sigma_1 = \text{Id}$ . For  $2 \leq i \leq k$  the restriction of  $\sigma_i$  to  $E_Z$  is non-trivial (e.g., on  $a$ ). Hence  $\sigma_i \notin Z(u/v)$ , so  $(u \circ \sigma_i)(a) > 0$ . For the residues in  $\bar{E}_u$  we thus have  $\bar{\sigma}_1(a) = \bar{a} = \bar{1}$  and  $\bar{\sigma}_i(a) = 0$  for  $2 \leq i \leq k$ .

Now let  $f(X) = \text{irr}(a, F)$ . Write

$$f(X) = \prod_{i=1}^k (X - \sigma_i(a)) = X^k + c_1 X^{k-1} + \dots + c_{k-1} X + c_k.$$

Expressing the  $c_j$  as symmetric polynomials in  $\sigma_1(a), \dots, \sigma_k(a)$ , we see that

$$c_1, \dots, c_k \in O_v, \quad \bar{c}_1 = -\bar{1}, \quad \bar{c}_2 = \dots = \bar{c}_k = 0.$$

Hence

$$\bar{f}(X) = X^k - X^{k-1} = X^{k-1}(X - \bar{1}),$$

so  $\bar{1}$  is a simple root of  $\bar{f}(X)$ . By (e), it lifts to a root of  $f(X)$  in  $O_v$ . But  $f(X)$  is irreducible in  $F[X]$ , so necessarily  $\deg(f) = 1$ , i.e.,  $a \in F$ . By the choice of  $a$ , this means that  $\text{Gal}(E/F) = Z(u/v)$ , as desired.

(f) $\Rightarrow$ (e): Let  $f(x)$  and  $\bar{a}$  be as in (e). Take in (f)  $g(X) = f(X)$ , and choose an arbitrary  $a \in O_v$  with residue  $\bar{a}$ . Then  $v(g(a)) > 0$  and  $v(g'(a)) = 0$ . We obtain a zero  $c$  of  $f(X)$  such that  $v(a - c) = v(f(a)) > 0$ , so  $\bar{a} = \bar{c}$ .

(e) $\Rightarrow$ (f): If  $g(a) = 0$ , then we take  $c = a$ . So suppose that  $g(a) \neq 0$ . The assumption then implies that  $g'(a) \neq 0$  as well. By the Taylor expansion formula (Lemma 18.1.1),

$$g(a + X) = g(a) + g'(a)X + X^2 h(X),$$

with  $h(X) \in O_v[X]$ . Substitute  $X = -(g(a)/g'(a))Y$  to obtain that

$$g\left(a - \frac{g(a)}{g'(a)}Y\right) = g(a) \left[ 1 - Y + \frac{g(a)}{g'(a)^2} h_1(Y) Y^2 \right],$$

where

$$h_1(Y) = h\left(-\frac{g(a)}{g'(a)}Y\right) \in O_v[Y].$$

Let

$$f(Y) = 1 - Y + \frac{g(a)}{g'(a)^2} h_1(Y) Y^2.$$

The assumption that  $v(g(a)) > 2v(g'(a))$  implies that  $v(f(1)) > 0$ , while  $v(f'(1)) = 0$ . Thus 1 is a simple root of  $\bar{f}(Y)$  in  $\bar{F}_v$ . Since  $g(X)$  splits in  $E$ , so does  $f(Y)$ . Condition (e) therefore gives rise to a zero  $b \in G_v$  of  $f(Y)$ . Then

$$c = a - \frac{g(a)}{g'(a)} b$$

is zero of  $g(X)$ . Moreover,  $v(a - c) = v(g(a)/g'(a))$ . □

Another important equivalent condition, the *Krasner-Ostrowski lemma*, will be discussed in §18.5. For other equivalent conditions (in the more classical case, where  $E$  is the algebraic closure of  $F$ ) see [Ri2]. The fact that the equivalence of the main classical forms of Henselity can also be formulated in this relative setting was noted by Bröcker [Br1].

## 18.2 $n$ th powers

One important use of Henselity is to show that groups of  $n$ th powers in the field are open with respect to the valuation topology.

PROPOSITION 18.2.1. *Let  $n$  be a positive integer and let  $E/F$  be a normal extension such that  $E$  contains all  $n$ th roots of elements of  $F$ . Let  $v$  be a valuation on  $F$  which is Henselian relative to  $E$ . Then*

$$1 + n^2 \mathfrak{m}_v \leq (F^\times)^n.$$

*In particular, if  $\text{char } F \nmid n$ , then  $(F^\times)^n$  is open with respect to the topology  $\mathcal{T}_v$ .*

PROOF. Take  $d \in 1 + n^2 \mathfrak{m}_v$ . By assumption, the polynomial  $g(X) = X^n - d$  splits in  $E$ . Observe that  $v(g(1)) > 2v(n) = 2v(g'(1))$ . The Hensel-Rychlik condition (condition (f) of Theorem 18.1.2) therefore yields  $c \in F$  such that  $c^n = d$ .

The second assertion follows from the first. □

18.2.2 EXAMPLES. The assumptions of the first part of Proposition 18.2.1 are satisfied in the following situations:

- (1)  $n$  is arbitrary and  $E$  is the algebraic closure of  $F$  (so  $v$  is Henselian);
- (2)  $n$  is arbitrary and  $E$  is the solvable closure of  $F$  (so  $v$  is solvably Henselian);
- (3)  $n = p$  is prime,  $F$  contains a root of unity of order  $p$ , and  $E = F(p)$  is the maximal  $p$ -Galois extension of  $F$  (so  $v$  is  $p$ -Henselian).

REMARK 18.2.3. Let  $n$  be a positive integer. Consider a valuation  $v$  on  $F$  with residue field of characteristic not dividing  $n$ . Then  $v$  is  $(F^\times)^n$ -compatible (in the sense of §11.1) if and only if  $1 + n^2\mathfrak{m}_v \leq (F^\times)^n$ . In this sense, the compatibility relation is a weak form of Henselity.

The following result of Wadsworth [Wad, Prop. 1.2] shows that when the residue field contains a root of unity of order  $p$ , the converse of Example 18.2.2(3) also holds.

PROPOSITION 18.2.4. *Let  $p$  be a prime number and let  $v$  be a valuation on  $F$  such that  $\bar{F}_v$  contains a primitive  $p$ th root of unity. Then  $v$  is  $p$ -Henselian if and only if it is  $(F^\times)^p$ -compatible.*

PROOF. Note that the assumption implies in particular that  $\text{char } \bar{F}_v \neq p$ .

We have just seen the “only if” part.

For the “if” part, assume that  $v$  is  $(F^\times)^p$ -compatible, but that a  $p$ -Henselization  $(\hat{F}, \hat{v})$  of  $(F, v)$  is a proper extension of  $F$ . Let  $E$  be a minimal proper extension of  $F$  inside  $\hat{F}$ . Then the extension  $E/F$  is finite, and its Galois hull  $M$  is contained in  $F(p)$ . Thus  $\text{Gal}(M/E)$  is a maximal proper subgroup of the finite  $p$ -group  $\text{Gal}(M/F)$ . Hence it is normal of index  $p$ . Therefore  $E/F$  is a Galois extension of degree  $p$ . By Kummer’s theory,  $E = F(\sqrt[p]{a})$  for some  $a \in F^\times \setminus (F^\times)^p$ .

Let  $u_1, \dots, u_m$  be the distinct extensions of  $v$  to  $E$  (up to equivalence), say with  $\hat{v}$  extending  $u_1$ . By Remark 15.1.1(e),  $Z(u_1/v) = 1$ , so  $v$  is not Henselian relative to  $E$ , i.e.,  $m \geq 2$ . By the fundamental inequality (Theorem 17.1.5),

$$e(u_1/v)f(u_1/v) < [E : F] = p.$$

Now if  $v(a) \notin v(F^\times)$ , then  $p|e(u_1/v)$ , a contradiction. Therefore  $a \in O_v^\times (F^\times)^p$ . Without loss of generality, we may assume that  $a \in O_u^\times$ . The residue  $\bar{a}$  of  $a$  in  $\bar{F}_v$  is then a  $p$ th power in  $\bar{E}_{u_1}^\times$ . Since

$$[\bar{E}_{u_1} : \bar{F}_v] = f(u_1/v) < p$$

and since  $\bar{F}_v$  contains a primitive  $p$ th root of unity, Kummer’s theory again implies that in fact  $\bar{a} \in (\bar{F}_v^\times)^p$ . Therefore  $a \in G_v(F^\times)^p = (F^\times)^p$ , by the compatibility assumption. This gives the desired contradiction.  $\square$

We conclude with a positive characteristic analog of Proposition 18.2.1.

LEMMA 18.2.5. *Let  $p$  be a prime number and let  $\wp(x) = x^p - x$ . Let  $E/F$  be a normal extension of fields of characteristic  $p$  such that  $F \subseteq \wp(E)$ . Let  $v$  be a valuation on  $F$  which is Henselian relative to  $E$ . Then*

$$\mathfrak{m}_v \leq \wp(F).$$

*In particular, for  $v$  nontrivial,  $\wp(F)$  is open in  $\mathcal{T}_v$ .*

PROOF. Take  $d \in \mathfrak{m}_v$ . By assumption,  $g(X) = \wp(X) - d$  has a root in  $E$ , and therefore splits in  $E$ . Its reduction to  $\bar{F}_v[X]$  has  $p$  distinct roots in  $\bar{F}_v$ , namely the elements of  $\mathbb{F}_p$ . Condition (e) of Theorem 18.1.2 allows us to lift them to roots of  $g(X)$  in  $F$ .

The second assertion follows from the first and from the fact that  $\wp(F)$  is an additive subgroup of  $F$ .  $\square$

### 18.3 Example: complete valued fields

It was the discovery of Kurt Hensel [He] that  $p$ -adic fields satisfy condition (d) of Theorem 18.1.2 when  $E$  is the algebraic closure (whence the names “Hensel’s lemma” and “Henselity”). In fact, his argument applies to any field which is complete with respect to a valuation of rank 1. We prove a somewhat sharper version of the equivalent condition (e) of the theorem for such fields.

**THEOREM 18.3.1.** *Let  $v$  be a complete rank 1 valuation on the field  $F$ . Let  $f(X) \in O_v[X]$  and  $a \in O_v$  satisfy  $v(f(a)) > 0$  and  $v(f'(a)) = 0$ . Then there exists  $b \in F$  such that  $f(b) = 0$  and  $v(b - a) \geq v(f(a))$ . Moreover,  $b$  is the unique zero of  $f(X)$  satisfying  $v(b - a) > 0$ .*

**PROOF.** For the existence of  $b$  set  $\alpha = v(f(a))$ . Thus  $\alpha > 0$ . We define inductively a sequence  $a_1, a_2, \dots$  in  $F$  such that  $a_1 = a$  and for every  $n \geq 1$ :

- (1)  $v(a_n - a_{n+1}) \geq n\alpha$ ;
- (2)  $v(f(a_n)) \geq n\alpha$ ;
- (3)  $v(f'(a_n)) = 0$ .

Suppose that  $a_n$  has already been defined. By (3),  $f'(a_n) \neq 0$ . Let  $h = f(a_n)/f'(a_n)$  and let  $a_{n+1} = a_n - h$ . By (2) and (3),  $v(a_n - a_{n+1}) = v(h) \geq n\alpha$ . The Taylor expansion formula (Lemma 18.1.1) gives:

$$f(a_{n+1}) \in f(a_n) - hf'(a_n) + h^2O_v = h^2O_v.$$

Hence

$$v(f(a_{n+1})) \geq 2v(h) \geq 2n\alpha \geq (n+1)\alpha.$$

Furthermore,  $v(a_n - a_{n+1}) \geq n\alpha$  implies that

$$v(f'(a_n) - f'(a_{n+1})) \geq n\alpha > 0.$$

Since  $v(f'(a_n)) = 0$  (by (3)) also  $v(f'(a_{n+1})) = 0$ , completing the inductive construction.

It now follows from (1) and the ultrametric inequality that  $v(a_n - a_m) \geq n\alpha$  for  $n \leq m$ . In particular,  $\{a_n\}_{n=1}^\infty$  is a Cauchy sequence with respect to the metric  $d_v$  of §9.1. By the completeness, it converges to a limit  $b \in F$ . Since  $\mathcal{T}_v$  is a ring topology (Proposition 8.1.1),  $f(X)$  is  $\mathcal{T}_v$ -continuous. It therefore follows from (2) that  $f(b) = 0$ . Also,

$$v(a_n - a) = v(a_n - a_1) \geq \alpha$$

for all  $n$ , so  $v(b - a) \geq \alpha$ . In particular,  $v(b) \geq 0$ .

For the uniqueness, suppose that  $c$  is a zero of  $f(X)$  with  $v(c - a) > 0$ . Then  $c \in O_v$ . Write  $f(X) = (X - b)g(X)$ , with  $g(X) \in F[X]$ . Let  $\bar{v}$  be the restricted Gauss valuation on  $F(X)$  extending  $v$  (see Example 4.3.2). Then

$$\bar{v}(X - b) = \min\{v(1), v(-b)\} = 0.$$

Hence  $0 \leq \bar{v}(f) = \bar{v}(g)$ , so  $g(X) \in O_v[X]$ . As

$$f'(X) = g(X) + (X - b)g'(X),$$

we have

$$(18.3.1) \quad f'(c) = g(c) + (c - b)g'(c).$$

Since  $v(f'(a)) = 0$  and  $v(c - a) > 0$  we also have  $v(f'(c)) = 0$ . In addition,

$$v(c - b) \geq \min\{v(c - a), v(a - b)\} > 0$$

and  $v(g'(c)) \geq 0$ . It now follows from (18.3.1) that  $g(c) \neq 0$ . From  $0 = f(c) = (c - b)g(c)$  we deduce that  $c = b$ .  $\square$

**COROLLARY 18.3.2.** *Let  $v$  be a complete rank 1 valuation on the field  $F$  and let  $E$  be a normal extension of  $F$ . Then  $(F, v)$  is Henselian relative to  $E$ .*

**PROOF.** Theorem 18.3.1 gives the assertion for the algebraic closure of  $F$ . By Corollary 15.3.2, it holds for every normal extension of  $F$ .  $\square$

**COROLLARY 18.3.3.** *Let  $v$  be a rank 1 valuation on the field  $F$  and let  $(\hat{F}, \hat{v})$  be the completion of  $(F, v)$ .*

- (a) *Any Henselization of  $(F, v)$  embeds over  $(F, v)$  in  $(\hat{F}, \hat{v})$ .*
- (b) *If  $\text{char } \bar{F}_v = 0$  or  $v$  is discrete, then the relative algebraic closure of  $F$  in  $\hat{F}$  is a Henselization of  $(F, v)$ .*

**PROOF.** (a) This follows from Corollary 18.3.2 and the universal property of Henselizations (Theorem 15.3.5).

(b) Let  $F'$  be the relative algebraic closure of  $F$  in  $\hat{F}$ , and let  $v'$  be the restriction to it of  $\hat{v}$ . Since  $(\hat{F}, \hat{v})$  is Henselian, so is  $(F', v')$ , by Proposition 15.3.3. Hence it is an algebraic extension of some Henselization of  $(F, v)$ . The assumptions imply that this extension is defectless (by Proposition 17.3.2 and Theorem 17.4.3). Moreover, this extension is immediate since  $(\hat{F}, \hat{v})/(F, v)$  is immediate. By Ostrowski's formula (Theorem 17.2.1), the extension is trivial, i.e.,  $(F', v')$  is a Henselization of  $(F, v)$ .  $\square$

When combined with Examples 9.2.1 and 9.2.2, Corollary 18.3.2 above gives some fundamental examples of Henselian valued fields.

#### 18.3.4 EXAMPLES.

- (1) (Hensel) The canonical  $p$ -adic valuation  $v_p$  on the field  $\mathbb{Q}_p$  of  $p$ -adic numbers is Henselian. Thus it has a unique extension to any algebraic extension  $F$  of  $\mathbb{Q}_p$ , and this valuation is also Henselian, by Corollary 15.3.2.
- (2) By (1) and by Proposition 15.3.3, the relative algebraic closure  $\mathbb{Q}_{p,\text{alg}}$  of  $\mathbb{Q}$  in  $\mathbb{Q}_p$  is Henselian.
- (3) Let  $\bar{F}$  be a perfect field of characteristic  $p > 0$  and let  $F$  be the quotient field of its ring  $W(\bar{F})$  of Witt vectors (see §12.4). By Theorem 12.4.1,  $F$  is equipped with a canonical discrete complete valuation with residue field  $\bar{F}$ . By Corollary 18.3.2, it is Henselian.

From Example 18.3.4(1) one can deduce that on a  $p$ -adic field, the  $p$ -adic valuation is the only “interesting” valuation, in the following sense.

**EXAMPLE 18.3.5.** Let  $F = \mathbb{Q}_p$  for some prime number  $p$  and let  $v_p$  be its  $p$ -adic valuation. We show that every valuation  $v$  on  $F$  which is not equivalent to  $v_p$  has a divisible value group. This is clear for the trivial valuation. So suppose that  $v$  is non-trivial and let  $n$  be a positive integer. As we have seen in Example 10.1.2,  $v_p$  and  $v$  are necessarily independent. Now  $v_p$  is Henselian (Example 18.3.4(1)),

so by Proposition 18.2.1,  $(F^\times)^n$  is  $\mathcal{T}_{v_p}$ -open. It follows from Proposition 10.3.1(a) that  $F^\times = (F^\times)^n O_v^\times$ , i.e.,  $v(F^\times) = nv(F^\times)$ .

As an application we obtain:

**COROLLARY 18.3.6.** *Let  $p, q$  be prime numbers and let  $\sigma: \mathbb{Q}_p \rightarrow \mathbb{Q}_q$  be a field embedding. Then  $p = q$  and  $\sigma$  is the identity map.*

**PROOF.** Denote again the canonical valuations on  $\mathbb{Q}_p, \mathbb{Q}_q$  by  $v_p, v_q$ , respectively. Then  $v_p$  and  $v_q \circ \sigma$  are discrete valuations on  $\mathbb{Q}_p$ . By what we have just seen, this can happen only if they are equivalent. Since  $\sigma$  is the identity on  $\mathbb{Q}$ , one has  $(v_q \circ \sigma)(q) > 0$ . Hence also  $v_p(q) > 0$ , so  $p = q$ . It follows that  $\sigma$  is an isometry of the metric space  $(\mathbb{Q}_p, d_{v_p})$  with itself (see §9.1), and in particular, is continuous in the induced topology  $\mathcal{T}_{v_p}$ . But  $\mathbb{Q}$  is  $\mathcal{T}_{v_p}$ -dense in  $\mathbb{Q}_p$ . We conclude that  $\sigma$  is the identity on  $\mathbb{Q}_p$ .  $\square$

Finally, we record the following topological fact which sometimes serves as a partial converse of Proposition 18.2.1.

**PROPOSITION 18.3.7.** *Let  $v$  be a discrete valuation on a field  $F$  and let  $n$  be a positive integer. Every  $\mathcal{T}_v$ -open subgroup of  $F^\times$  containing  $(F^\times)^n$  must contain  $(F^\times)^n(1 + n^2\mathfrak{m}_v)$ .*

**PROOF.** Let  $(E, u)$  be the completion of  $(F, v)$ . It is Henselian (Corollary 18.3.2). By Theorem 9.3.2(f),  $(E, u)/(F, v)$  is an immediate extension. Hence  $\mathfrak{m}_v^i = F \cap \mathfrak{m}_u^i$  for  $i \geq 1$ .

Now let  $S$  be a  $\mathcal{T}_v$ -open subgroup of  $F^\times$  containing  $(F^\times)^n$ . The subgroups  $1 + \mathfrak{m}_v^i$ ,  $i = 1, 2, \dots$ , form a local basis of  $\mathcal{T}_v$  at 1. Therefore  $1 + \mathfrak{m}_v^i \leq S$  for some  $i \geq 1$ . By Proposition 3.4.5,  $E^\times = F^\times(1 + \mathfrak{m}_u^i)$ . Hence  $(E^\times)^n \leq (F^\times)^n(1 + \mathfrak{m}_u^i)$ . By Proposition 18.2.1,  $1 + n^2\mathfrak{m}_u \leq (E^\times)^n$ . We conclude that

$$(F^\times)^n(1 + n^2\mathfrak{m}_v) \leq F \cap (E^\times)^n \leq (F^\times)^n(1 + \mathfrak{m}_v^i) \leq S. \quad \square$$

#### 18.4 Example: power series fields

The Henselity of complete valued fields of rank 1 established in the previous section implies in particular that whenever  $\Gamma$  is an ordered abelian group of rank 1, the field  $K((\Gamma))$  of generalized formal power series over  $K$  is Henselian with respect to its canonical valuation  $v(f) = \min(\text{Supp}(f))$  (see Example 4.2.1). However, this turns out to be valid for ordered abelian groups of arbitrary ranks, as we now show.

**THEOREM 18.4.1 (Krull [Kru2]).** *Let  $K$  be a field and  $\Gamma$  an ordered abelian group. Let  $F = K((\Gamma))$ , and let  $v: F^\times \rightarrow \Gamma$  be its canonical valuation. Then  $(F, v)$  has no proper immediate extensions.*

**PROOF.** Assume that  $(E, u)/(F, v)$  is an immediate extension, and let  $a \in E^\times$ . We need to show that  $a \in F$ .

To this end let  $S$  be the set of all  $f \in F$  such that  $u(a - f)$  (as an element of  $\Gamma \cup \{\infty\}$ ) is strictly larger than every element of the support  $\text{Supp}(f)$  of  $f$ . In particular,  $0 \in S$ . We partially order  $S$  by the relation  $\preceq$  defined in §2.7. We recall that  $f \preceq f'$  means that  $f(\delta) = f'(\delta)$  for every  $\delta \in \Gamma$  for which there exists  $\gamma \in \text{Supp}(f)$  with  $\delta \leq \gamma$ .

Assume that  $C$  is a non-empty chain in  $(S, \preceq)$ . By Lemma 2.7.6, it has a least upper bound  $f^* \in F$  satisfying  $\text{Supp}(f^*) = \bigcup_{f \in C} \text{Supp}(f)$ . We claim that  $f^* \in S$ . Indeed, consider  $\gamma \in \text{Supp}(f^*)$ . Then  $\gamma \in \text{Supp}(f)$  for some  $f \in C$ . As  $f \preceq f^*$  this implies that  $\gamma < v(f - f^*)$ . Also,  $f \in C \subseteq S$  gives  $\gamma < u(a - f)$ . By the ultrametric inequality,  $\gamma < u(a - f^*)$ , as claimed.

Consequently Zorn's lemma yields a maximal element  $f$  in  $(S, \preceq)$ . Suppose that  $a \neq f$ . Then  $\gamma = u(a - f) \in \Gamma$ . By Lemma 3.2.5,  $E^\times = F^\times G_u$ . Therefore there exists  $g \in F^\times$  with  $a - f \in gG_u$ . Thus  $u(g) = \gamma$ . In fact, we may choose  $g = bt^\gamma$  for some  $b \in K^\times$ . Let  $f' = f + g$ . Since  $\gamma$  is strictly larger than every element of  $\text{Supp}(f)$  we have  $f \prec f'$ . Furthermore,

$$u(a - f') = u(a - f - g) > u(g) = \gamma = \max(\text{Supp}(f')).$$

Hence  $f' \in S$ . This contradiction to the maximality of  $f$  in  $(S, \preceq)$  shows that  $a = f \in F$ , as desired.  $\square$

Krull's original proof of Theorem 18.4.1 uses a transfinite construction, which is replaced in the above argument by the application of Zorn's lemma. A proof of an analytic flavor is given in [Ri1].

Valued fields having no proper immediate extensions are called **maximally complete**. We refer to [Kap1] for an analytic characterization of these fields. Since Henselizations are always immediate extensions (by Proposition 15.3.7), maximally complete fields are necessarily Henselian. In particular, we deduce from Theorem 18.4.1:

**COROLLARY 18.4.2.** *Let  $K$  be a field and let  $\Gamma$  be an ordered abelian group. Then  $K((\Gamma))$  is Henselian with respect to its canonical valuation.*

**EXAMPLE 18.4.3** (MacLane [Mac2]). Let  $K$  be an algebraically closed field and  $\Gamma$  a divisible ordered abelian group. By Corollary 14.2.3, every algebraic extension of  $K((\Gamma))$  must be immediate with respect to the canonical valuation. In view of Theorem 18.4.1, this extension must be trivial. We conclude that  $K((\Gamma))$  is algebraically closed. Of course, when  $\text{char } K = 0$  this is also a special case of Corollary 17.3.3.

**EXAMPLE 18.4.4:**  $\Gamma$ -Puisseux series.

Let  $K$  be an arbitrary field,  $\Gamma$  an ordered abelian group, and

$$K_{\text{Puis}}((\Gamma)) = \varinjlim K((\Gamma'))$$

the field of  $\Gamma$ -Puisseux series over  $K$ , where  $\Gamma'$  ranges over all subgroups of  $\Gamma_{\text{div}}$  which contain  $\Gamma$  as a subgroup of finite index (§2.8). Let  $v$  be the canonical valuation on  $K_{\text{Puis}}((\Gamma))$  with respect to the trivial valuation on  $K$ , as in Example 4.2.3. Thus the value group of  $v$  is  $\Gamma_{\text{div}}$  and its residue field is  $K$ . It extends the canonical valuation on  $F = K((\Gamma))$ , which is Henselian by Corollary 18.4.2. As we have observed in §2.8,  $K_{\text{Puis}}((\Gamma))$  is algebraic over  $K((\Gamma))$ . We conclude from Corollary 15.3.2 that  $v$  is also Henselian.

**PROPOSITION 18.4.5.** *Assume that  $\text{char } K = 0$  and let  $\Gamma$  be an ordered abelian group.*

- (a)  $K_{\text{Puis}}((\Gamma))$  is the relative algebraic closure of  $K((\Gamma))$  in  $K((\Gamma_{\text{div}}))$ .
- (b) If  $K$  is algebraically closed, then  $K_{\text{Puis}}((\Gamma))$  is the algebraic closure of  $K((\Gamma))$ .

PROOF. (a) The canonical valuation on  $K((\Gamma))$  is Henselian and its residue field  $K$  has characteristic 0. Hence it is defectless relative to the algebraic closure (Proposition 17.3.2). By the tower property for the defect (17.2.1), so is its extension  $v$  to  $K_{\text{Puis}}((\Gamma))$ . Furthermore, the extension  $K((\Gamma_{\text{div}}))/K_{\text{Puis}}((\Gamma))$  is immediate with respect to the canonical valuations. Therefore the relative algebraic closure of  $K_{\text{Puis}}((\Gamma))$  in  $K((\Gamma_{\text{div}}))$  is also an immediate extension of  $K_{\text{Puis}}((\Gamma))$ . Being algebraic, defectless and immediate, this extension is necessarily trivial, i.e.,  $K_{\text{Puis}}((\Gamma))$  is algebraically closed in  $K((\Gamma_{\text{div}}))$ , as required.

(b) By Example 18.4.3,  $K((\Gamma_{\text{div}}))$  is algebraically closed. By (a),  $K_{\text{Puis}}((\Gamma))$  is therefore also algebraically closed. Since it is algebraic over  $K((\Gamma))$ , it is its algebraic closure.  $\square$

The assumption that  $\text{char } K = 0$  in Proposition 18.4.5(b) (and hence also in Proposition 18.4.5(a)) cannot be omitted even when  $\Gamma = \mathbb{Z}$ , as the following example demonstrates.

EXAMPLE 18.4.6 (Abhyankar [Ab], Chevalley [Ch, p. 64]). Let  $K$  be a field of characteristic  $p > 0$ . As usual, let  $t$  stand for the map in  $K((\mathbb{Z}))$  which is 1 at 1 and 0 elsewhere. We claim that the polynomial equation

$$X^p - X - 1/t = 0$$

has no solutions in  $K_{\text{Puis}}((\mathbb{Z})) = \varinjlim K((\frac{1}{m}\mathbb{Z}))$ . In particular, the latter field is not algebraically closed.

To prove the claim, suppose that  $f \in K_{\text{Puis}}((\mathbb{Z}))$  satisfies  $f^p - f = 1/t$ . Then  $f \in K((\frac{1}{m}\mathbb{Z}))$  for some positive integer  $m$ . Let  $v_m$  be the canonical valuation on  $K((\frac{1}{m}\mathbb{Z}))$  with value group  $\frac{1}{m}\mathbb{Z}$ . Take  $i$  maximal with  $p^i | m$ , and let

$$g = f - t^{-1/p} - t^{-1/p^2} - \dots - t^{-1/p^i}$$

(when  $i = 0$  we take  $g = f$ ). Observe that  $g \in K((\frac{1}{m}\mathbb{Z}))$  and  $g^p - g = t^{-1/p^i}$ . We obtain that

$$v_m(g) = -1/p^{i+1} \notin \frac{1}{m}\mathbb{Z}$$

(Lemma 3.2.1(e)), a contradiction

Still in the case where  $K$  is algebraically closed of characteristic  $p > 0$ , Kedlaya [Ked], extending earlier works by Huang, Rayner [Ra2], and Ştefănescu [Ste], realizes the algebraic closure of  $K((\mathbb{Z}))$  explicitly as the “twist-recurrent” maps in the algebraically closed field  $K((\mathbb{Q}))$ . In particular, the support of such maps must be contained in a set of the form

$$\{1/mp^i \mid i = 0, 1, 2, \dots\}$$

for some positive integer  $m$ .

### 18.5 The Krasner–Ostrowski lemma

The following lemma gives another condition which is equivalent to relative Henselity. Its importance lies in the fact that it connects the arithmetic (or better said, analytic) properties of a valued field with its Galois theory. The implication (a) $\Rightarrow$ (b) is known in the folklore as “Krasner’s Lemma” (see [Kra]), however, as pointed out by Roquette in [Ro], the argument actually goes back to Ostrowski [O1].

LEMMA 18.5.1. *Let  $(E, u)/(F, v)$  be a normal extension of valued fields. The following conditions are equivalent:*

- (a)  *$v$  is Henselian relative to  $E$ ;*
- (b) *if  $a, b \in E$  and if  $u(b - \sigma(b)) < u(b - a)$  whenever  $\sigma \in \text{Aut}(E/F)$  and  $\sigma(b) \neq b$ , then the extension  $F(a, b)/F(a)$  is purely inseparable.*

PROOF. (a) $\Rightarrow$ (b): Suppose that  $\sigma \in \text{Aut}(E/F)$  fixes  $a$ . We need to show that it fixes  $b$  as well.

Since  $v$  is Henselian relative to  $E$ , one has  $u = u \circ \sigma$ . In particular,  $u(b - a) = u(\sigma(b) - \sigma(a))$ . From the ultrametric inequality we obtain that

$$u(b - \sigma(b)) = u((b - a) - (\sigma(b) - \sigma(a))) \geq u(b - a).$$

Our assumption now implies that  $\sigma(b) = b$ .

(b) $\Rightarrow$ (a): In light of condition (b) of Theorem 18.1.2, we may assume that  $E/F$  is a finite Galois extension. Lemma 15.2.1 yields  $b \in E_Z$  such that  $u(1 - b) > 0$  and  $(u \circ \sigma)(b) > 0$  whenever  $\sigma \in \text{Gal}(E/F) \setminus Z(u/v)$ . Then  $u(b) = 0$ .

Now suppose that  $\sigma \in \text{Gal}(E/F)$  satisfies  $\sigma(b) \neq b$ . Then  $\sigma \notin Z(u/v)$ , so  $(u \circ \sigma)(b) > 0$ , and therefore  $u(b - \sigma(b)) = 0$ . Since the extension  $(E_Z, u_Z)/(F, v)$  is immediate (Theorem 15.2.2), there exists  $a \in O_v$  with the same residue as  $b$ , i.e.,  $u(b - a) > 0$ . It follows from (b) that the extension  $F(b)/F$  is purely inseparable. But  $E/F$  is Galois, so necessarily  $b \in F$ . By the choice of  $b$ , this can happen only if  $\text{Gal}(E/F) = Z(u/v)$ . We conclude that  $v$  is Henselian relative to  $E$ .  $\square$

The main importance of Lemma 18.5.1 lies in the following consequence of it. It shows that in a relatively Henselian field, minor changes in the coefficients of a separable polynomial do not effect the splitting field.

For a valued field  $(F, v)$  we denote again the restricted classical Gauss valuation on  $F(X)$  by  $\bar{v}$ . Thus

$$\bar{v}(f) = \min\{v(c_0), \dots, v(c_n)\}$$

for  $f(X) = \sum_{i=0}^n c_i X^i$ .

THEOREM 18.5.2. *Let  $E/F$  be a normal extension of fields and let  $v$  be a Henselian valuation on  $F$  relative to  $E$ . Let  $f(X) \in F[X]$  be a monic polynomial of degree  $n$  with  $n$  distinct roots  $a_1, \dots, a_n$  in  $E$ . Then there exists  $\alpha \in v(F^\times)$  such that any other monic polynomial  $g(X) \in F[X]$  of degree  $n$  which splits in  $E$  and with  $\bar{v}(f - g) > \alpha$  has  $n$  distinct roots  $b_1, \dots, b_n$  in  $E$  such that  $F(a_i) = F(b_i)$ ,  $i = 1, \dots, n$ . In particular,  $f$  and  $g$  have the same splitting field over  $F$ .*

PROOF. Let  $u$  be the unique extension of  $v$  to  $E$ . We may assume that it is non-trivial and that  $n \geq 2$ . Choose  $\gamma \in u(E^\times)$  with

$$\max\{u(a_i - a_j) \mid i \neq j\} < \gamma.$$

By the continuity of roots in the valuation topology  $\mathcal{T}_u$  (Theorem 8.2.3) there exists a positive  $\alpha \in u(E^\times)$  such that if  $b_1, \dots, b_n \in E$  and

$$g(X) = \prod_{i=1}^n (X - b_i) \in F[X]$$

satisfy  $\bar{u}(f - g) > \alpha$  then, after re-numbering,  $u(a_i - b_i) > \gamma$ ,  $i = 1, \dots, n$ . In light of the cofinality of  $v(F^\times)$  in  $u(E^\times)$  (Corollary 14.2.3(e)) we may assume that  $\alpha \in v(F^\times)$ . For  $b_1, \dots, b_n$  as above, the ultrametric inequality gives for  $i \neq j$ :

$$\min\{\gamma, u(b_i - b_j)\} \leq \min\{u(a_i - b_i), u(b_i - b_j), u(b_j - a_j)\} \leq u(a_i - a_j) < \gamma.$$

It follows that

$$\max\{u(b_i - b_j) \mid i \neq j\} < \gamma.$$

In particular,  $b_1, \dots, b_n$  are distinct.

Lemma 18.5.1 implies that the extensions  $F(a_i, b_i)/F(a_i)$  and  $F(a_i, b_i)/F(b_i)$  are purely inseparable. On the other hand, since  $a_1, \dots, a_n$  are the distinct zeros of  $f(X) \in F[X]$ , they are separable over  $F$ . Similarly,  $b_1, \dots, b_n$  are separable over  $F$ . Consequently,  $F(a_i) = F(a_i, b_i) = F(b_i)$ ,  $i = 1, \dots, n$ .  $\square$

**COROLLARY 18.5.3.** *Let  $(\hat{F}, \hat{v})/(F, v)$  be an extension of non-trivially valued fields such that  $F$  is  $\mathcal{T}_{\hat{v}}$ -dense in  $\hat{F}$  and  $(\hat{F}, \hat{v})$  is Henselian. Let  $\hat{F}_{\text{sep}}, F_{\text{sep}}$  be the separable closures of  $\hat{F}, F$ , respectively. Then  $\hat{F}_{\text{sep}}$  is the compositum  $F_{\text{sep}}\hat{F}$ .*

**PROOF.** Obviously,  $F_{\text{sep}}\hat{F} \subseteq \hat{F}_{\text{sep}}$ . Conversely, let  $a \in \hat{F}_{\text{sep}}$  and let  $f(X) = \text{irr}(a, \hat{F})$ . Using the density, we may choose a monic polynomial  $g(X) \in F[X]$  of the same degree as  $f(X)$  and whose coefficients are sufficiently close to those of  $f(X)$  with respect to  $\mathcal{T}_{\hat{v}}$ . It follows from Theorem 18.5.2 that the splitting fields of  $f(X)$  and  $g(X)$  over  $\hat{F}$  coincide. Moreover,  $g(X)$  is separable over  $F$ , hence it splits in  $F_{\text{sep}}$ . Therefore  $f(X)$  splits in  $F_{\text{sep}}\hat{F}$ . We conclude that  $a \in F_{\text{sep}}\hat{F}$ .  $\square$

#### 18.5.4 EXAMPLES.

- (1) The algebraic closure  $\tilde{\mathbb{Q}}_p$  of  $\mathbb{Q}_p$  is the compositum  $\tilde{\mathbb{Q}}\mathbb{Q}_p$ , where  $\tilde{\mathbb{Q}}$  is the field of algebraic numbers.
- (2) Given a field  $F$ , the separable closure of  $F((t))$  is  $F((t))_{\text{sep}}F((t))$ . The latter field should not be confused with the Laurent series field  $F_{\text{sep}}((t))$  over  $F_{\text{sep}}$ , which is usually much larger.
- (3) Let  $F$  be a separably closed field and let  $v$  be a valuation of rank 1 on  $F$ . Then the completion  $(\hat{F}, \hat{v})$  of  $(F, v)$  is also separably closed. Indeed,  $(\hat{F}, \hat{v})$  is Henselian by Corollary 18.3.2, and we apply Corollary 18.5.3.
- (4) (Kürschák [**Kür**]) Let  $v_0$  be a valuation of rank 1 on a field  $F_0$ . Construct inductively an increasing sequence of valued fields of rank 1

$$(F_0, v_0) \subseteq (F_1, v_1) \subseteq (F_2, v_2) \subseteq (F_3, v_3) \subseteq \dots$$

as follows:

- (i) Take  $(F_{2i+1}, v_{2i+1})$  to be the completion of  $(F_{2i}, v_{2i})$ . Since this is an immediate extension (Theorem 9.3.2(f)),  $v_{2i+1}$  indeed has rank 1.
- (ii) Take  $F_{2i+2}$  to be the separable closure of  $F_{2i+1}$ , and  $v_{2i+2}$  to be the extension of  $v_{2i+1}$  to it. Notice that this extension is unique by Corollary 18.3.2, and has rank 1 by Corollary 14.2.3(c).

Now since  $(F_2, v_2)$  is separably closed, Example (3) above implies that so is its completion  $(F_3, v_3)$ . Consequently, this sequence of extensions stabilizes from  $(F_3, v_3)$  and on.

- (5) In particular, start with  $F_0 = \mathbb{Q}$  and let  $v_0$  be its  $p$ -adic valuation for some prime number  $p$ . Then  $F_1 = \mathbb{Q}_p$  and  $F_2 = \tilde{\mathbb{Q}}_p = \tilde{\mathbb{Q}}\mathbb{Q}_p$ . The field  $F_3$  is often denoted by  $\mathbb{C}_p$ . It is both complete and algebraically closed. Hence it is a convenient “universal domain” for carrying computations of combined algebraic/ $p$ -adic analytic nature.