Therefore $\rho^{-1}\lambda \in Z(\mathcal{O}')$ and therewith $\lambda|_{K_Z} = \rho|_{K_Z}$. Q.E.D.

The next theorem will give some equivalent conditions for a valued field $(K, \mathcal{O})$ to be Henselian. All equivalent conditions will talk about (zeros of) polynomials $f \in \mathcal{O}[X]$ in one variable. There are, of course, many such equivalents known. Here we concentrate on those used in the course of this book. Observing that (5) $\Rightarrow$ (1) uses only a separable polynomial, it is easy to see that in the conditions (3) to (6) it suffices to consider only separable polynomials from $\mathcal{O}[X]$ (where separable means without multiple zeros).

Here it is convenient to mention and to use an elementary result that is proved in Section A.6 in more generality:

Suppose v is the valuation corresponding to $\mathcal{O}$. Then the definition

$$w(a_nX^n + \cdots + a_0) := \min_{0\le i\le n} v(a_i)$$

(for $a_i \in K$), and $w(f/g) = w(f) - w(g)$ (for $f, g \in K[X] \setminus \{0\}$) yields a valuation w on $K(X)$, by (A.6.3). This extension of v to $K(X)$ is called the *Gauss extension*. The property $w(fg) = w(f) + w(g)$ will be used from now on in the following way. Let us call a polynomial $f \in \mathcal{O}[X]$ *primitive* if $w(f) = 0$, i.e., if at least one coefficient of f is a unit in $\mathcal{O}$. Now clearly the product of primitive polynomials from $\mathcal{O}[X]$ is again primitive, and if a primitive polynomial $f \in \mathcal{O}[X]$ has a factorization $f = gh$ in $K[X]$, then it also has a factorization $f = g_1h_1$ in $\mathcal{O}[X]$ with g_1 and h_1 both primitive, and being constant multiples of f and g, respectively.

Theorem A.3.13 ("Hensel's Lemma"): *For a valued field $(K, \mathcal{O})$ with residue field $\overline{K}$ and residue homomorphism $a \mapsto \overline{a}$, the following are equivalent:*

(1) $(K, \mathcal{O})$ is Henselian.

(2) Let $f, g, h \in \mathcal{O}[X]$, where f has only separable irreducible factors, $\overline{f} = \overline{g}\overline{h} \neq 0$, and $(\overline{g}, \overline{h}) = 1$. Then there exist $g_1, h_1 \in \mathcal{O}[X]$ with $f = g_1h_1$, $\overline{g_1} = \overline{g}$, $\overline{h_1} = \overline{h}$, and $\deg g_1 = \deg \overline{g}$.

(3) For each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $\overline{f}(\overline{a}) = 0$ and $\overline{f}'(\overline{a}) \neq 0$, there exists an $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $\overline{\alpha} = \overline{a}$.

(4) For each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $v(f(a)) > 2v(f'(a))$, there exists an $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $v(a - \alpha) > v(f'(a))$.

(5) Every polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}[X]$ with $a_{n-1} \notin \mathfrak{m}$ and $a_{n-2}, \dots, a_0 \in \mathfrak{m}$ has a zero in K.

(6) Every polynomial $X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$ with $a_{n-2}, \dots, a_0 \in \mathfrak{m}$ has a zero in K.

Proof: Let L be the splitting field of f over K.

(1) $\Rightarrow$ (2): Let $\mathcal{O}'$ be the unique extension of $\mathcal{O}$ to L (using (1), (A.3.8), and (A.1.13)). Let $f := a_nX^n + \cdots + a_0 \in \mathcal{O}[X]$. Since $\overline{f} \neq 0$, f is primitive. In L we have

$$f = \prod_{i=1}^{n}(\beta_iX - \alpha_i), \quad \beta_i, \alpha_i \in \mathcal{O}',\ \beta_i \neq 0,$$

with $\min\{v(\beta_i), v(\alpha_i)\} = 0$, i.e., $(\beta_i, \alpha_i) = 1$. We may suppose that

$$\overline{g} = \overline{\epsilon}\prod_{i=1}^{m}(\overline{\beta_i}X - \overline{\alpha_i}), \quad \epsilon, \beta_i \in (\mathcal{O}')^\times$$

(possibly after re-numbering the factors). Set

$$g_1 := c\prod_{i=1}^{m}\Big(X - \frac{\alpha_i}{\beta_i}\Big) \quad \text{with} \quad \overline{c} = \overline{\epsilon\prod_{i=1}^{m}\beta_i}, \quad c \in \mathcal{O}^\times.$$

Such a c exists because $\overline{\epsilon\prod_{i=1}^{m}\beta_i}$ is the leading coefficient of $\overline{g} \in \overline{K}[X]$. Then $\overline{g_1} = \overline{g}$ and $\deg g_1 = \deg \overline{g} = m$. Now set $h_1 = f/g_1$. Then

$$\overline{h_1} = \overline{\epsilon}^{-1}\prod_{i=m+1}^{n}(\overline{\beta_i}X - \overline{\alpha_i}) = \overline{h}.$$

We shall show that (each coefficient of) g_1 is invariant under all $\sigma \in \mathrm{Gal}(L/K)$; it will then follow that $g_1, h_1 \in \mathcal{O}[X]$. From $\sigma(\mathcal{O}') = \mathcal{O}'$ follows $\sigma(\mathfrak{m}') = \mathfrak{m}'$. Thus σ defines a mapping $\overline{\sigma} : \overline{L} \to \overline{L}$ by $\overline{a} \mapsto \overline{\sigma(a)}$, which is an automorphism of $\overline{L}/\overline{K}$. From $(\overline{g}, \overline{h}) = 1$ it follows that for each $i \in \{1, \dots, m\}$ there exists $j \in \{1, \dots, m\}$ such that

$$\sigma\Big(\frac{\alpha_i}{\beta_i}\Big) = \frac{\alpha_j}{\beta_j}.$$

Thus σ permutes the zeros of g_1, whence the coefficients of g_1 lie in K, and therewith $g_1 \in \mathcal{O}[X]$.

(2) $\Rightarrow$ (3): First suppose f is separable. Set $g(X) = X - a$ and $\overline{h} = \overline{f}/\overline{g} \in \overline{K}[X]$. Then $\overline{f} = \overline{g}\overline{h}$ and $(\overline{g}, \overline{h}) = 1$, since $\overline{f}'(\overline{a}) \neq 0$. There exist $g_1, h_1 \in \mathcal{O}[X]$ with $f = g_1h_1$, $\overline{g_1} = \overline{g} = X - \overline{a}$, and $\deg g_1 = 1 = \deg \overline{g}$, by (2). It then follows that $g_1 = e(X - b)$ with $e \in \mathcal{O}^\times$ and $b \in \mathcal{O}$. Then $\overline{e} = 1$, $f(b) = 0$, and $\overline{b} = \overline{a}$.

Now let f be inseparable, and write $f = f_1f_2$, with $f_1, f_2 \in \mathcal{O}[X]$, where $\overline{f_1}$ is the product of the separable irreducible factors of $\overline{f}$, and $\overline{f_2}$ is the product of the inseparable irreducible factors of $\overline{f}$. Then $\overline{f_2}(X) = \overline{f_3}(X^p)$, for some $f_3 \in \mathcal{O}[X]$, where $p = \mathrm{char}\,\overline{K} = \mathrm{char}\,\mathcal{O}/\mathfrak{m} > 0$. From $\overline{f}(\overline{a}) = 0$ and $\overline{f}'(\overline{a}) \neq 0$ follows $\overline{f_1}(\overline{a}) = 0$ and $\overline{f_1}'(\overline{a}) \neq 0$ (since $p > 1$). Then the previous paragraph implies that f_1 has a zero $\alpha \in K$ with $\overline{\alpha} = \overline{a}$, so f has one, too.

(3) $\Rightarrow$ (4): $f(a - X) = f(a) - f'(a)X + X^2g(X)$, for some $g \in \mathcal{O}[X]$. Writing $X = f'(a)Y$, and observing that $v(f'(a)) \neq \infty$ and hence $f'(a) \neq 0$, we get

$$\frac{f(a-f'(a)Y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - Y + Y^2h(Y) =: f_1(Y).$$

Then $f_1 \in \mathcal{O}[Y]$, since $v(f(a)) > v(f'(a)^2)$. Now $\overline{f_1} = Y\big(Y\overline{h}(Y)-1\big)$, which has the simple zero $\overline{0}$ in the residue field. Therefore f_1 has a zero $y \in \mathfrak{m}$, by (3). Then f has the zero $\alpha := a - f'(a)y \in \mathcal{O}$. Since $y \in \mathfrak{m}$, $v(\alpha - a) > v(f'(a))$.

(4) ⇒ (5): Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ as in (5). Then

$$\overline{f} = X^n + \overline{a_{n-1}}X^{n-1} = X^{n-1}(X + \overline{a_{n-1}}).$$

Then $-\overline{a_{n-1}}$ $(\neq \overline{0})$ is a simple zero of $\overline{f}$. In particular,

$$v(f(-a_{n-1})) > 0 = v(f'(-a_{n-1})).$$

Then f has a zero in $\mathcal{O}$, by (4).

(5) ⇒ (6): Trivial.

(6) ⇒ (5): Suppose $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $a_{n-1} \in \mathcal{O}^\times$ and $a_{n-2}, \ldots, a_0 \in \mathfrak{m}$. Replace X by $a_{n-1}Y$ and divide by a_{n-1}^n; we obtain

$$g(Y) = Y^n + Y^{n-1} + \frac{a_{n-2}}{a_{n-1}^2}Y^{n-2} + \cdots + \frac{a_0}{a_{n-1}^n}.$$

Apply (5) to $g(Y)$ to obtain a zero $y \in K$ of g. Then $x := a_{n-1}y$ is a zero of f.

(5) ⇒ (1): Suppose $(K, \mathcal{O})$ were not Henselian. Then there would be a finite Galois extension L/K in which $\mathcal{O}$ extends to $\mathcal{O}'$ and $\mathcal{O}''$, with $\mathcal{O}' \neq \mathcal{O}''$. It follows that $Z(\mathcal{O}') \neq \mathrm{Gal}(L/K)$, since by (A.2.8), $\mathcal{O}'$ and $\mathcal{O}''$ are conjugate over K. Hence $m \geq 2$ in (A.3.1.1). As in the proof of (A.3.3), and writing $\beta^{[i]} = \sigma_i(\beta)$, there exists $\beta \in R = \bigcap_{i=1}^m \mathcal{O}^{[i]}$ with $\beta^{[1]} - 1 \in \mathfrak{m}'$ and, for $i = 2, \ldots, m$, $\beta^{[i]} \in \mathfrak{m}'$. Then

$$f := \prod_{i=1}^m (X - \beta^{[i]}) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in \mathcal{O}[X],$$

$-a_{m-1} = \sum \beta^{[i]} \equiv 1 \bmod \mathfrak{m}$, $a_{m-2} \equiv \cdots \equiv a_0 \equiv 0 \bmod \mathfrak{m}$. Then f has a zero in K, by (5). Hence $\beta \in K$ and thus $\beta^{[i]} = \beta^{[j]}$ for all i, j. This contradicts $\beta^{[1]} \equiv 1 \bmod \mathfrak{m}$ and $\beta^{[2]} \equiv 0 \bmod \mathfrak{m}$. (Note: f is separable.) Q.E.D.

Corollary A.3.14: *Let $(K', \mathcal{O}')$ be Henselian, $K \subseteq K'$, and $\mathcal{O} = K \cap \mathcal{O}'$. If K is relatively separably closed in K', then $(K, \mathcal{O})$ is Henselian.*

Proof: We use (1) ⇒ (5) and (5) ⇒ (1) of (A.3.13): Let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}[X]$$

be separable, $a_{n-1} \notin \mathfrak{m}$, and $a_{n-2}, \ldots, a_0 \in \mathfrak{m}$. Then f has a zero in K', hence also in K. Q.E.D.

Definition A.3.15: A valued field $(K, \mathcal{O})$ is called *algebraically maximal* if it admits no proper, algebraic, immediate extension $(K', \mathcal{O}')$.

Note that K with the trivial valuation is algebraically maximal.

Definition A.3.16: A valued field $(K, \mathcal{O})$ is called *finitely ramified* if either $\mathrm{char}\,\overline{K} = 0$, or $\mathrm{char}\,\overline{K} = p > 0$ and there are only finitely many values between 0 and $v(p)$.

Note that $(K, \mathcal{O})$ with $\mathcal{O} = K$ is finitely ramified, and that if $(K, \mathcal{O})$ is finitely ramified and $\mathcal{O}$ is nontrivial, then $\mathrm{char}\,K = 0$. In fact, if $\mathrm{char}\,K = p > 0$, then there are infinitely many elements between 0 and $v(p) = v(0) = \infty$ in the value group.

Examples A.3.17: (1) Let $\leq$ be an ordering of K, and let $\mathcal{O} = \mathcal{O}(\mathbb{Z}, \leq)$ (A.1.2)(b). Then $\overline{K}$ is ordered, whence $\mathrm{char}\,\overline{K} = 0$.

(2) If $\Gamma_{\mathcal{O}} \cong \mathbb{Z}$ and $\mathrm{char}\,K = 0$, then $(K, \mathcal{O})$ is finitely ramified.

Remark A.3.18: Suppose $(K, \mathcal{O})$ is finitely ramified. *Then for every $n \in \mathbb{Z} \setminus \{0\}$, there are only finitely many values between 0 and $v(n)$.* To see this, we consider the two cases, $\mathrm{char}\,\overline{K} = p$ and $\mathrm{char}\,\overline{K} = 0$. If $\mathrm{char}\,\overline{K} = p$, write $n = p^e s$ with $p \nmid s$; then $v(n) = ev(p)$, so that there are e times as many values between 0 and $v(n)$ as between 0 and $v(p)$ (approximately). Now suppose $\mathrm{char}\,\overline{K} = 0$. Since in this case $\mathrm{char}\,K = 0$, $\mathbb{Q} \subseteq K$, and $\mathfrak{m}_{\mathcal{O}} \cap \mathbb{Q} = (0) \subseteq \mathcal{O}$, so that for all $r \in \mathbb{Q}$, $\overline{r} = r$. Since $\mathrm{char}\,\overline{K} = 0$, for all $n \in \mathbb{Z} \setminus \{0\}$, $\overline{n} \neq 0$, whence $v(n) = 0$. Thus also in this case, there are only finitely many values between 0 and $v(n)$.

Theorem A.3.19: *Suppose $(K, \mathcal{O})$ is finitely ramified. Then $(K, \mathcal{O})$ is Henselian if and only if $(K, \mathcal{O})$ is algebraically maximal.*

Proof: (⇐) Let $(K, \mathcal{O})$ be algebraically maximal. Then $(K, \mathcal{O})$ is Henselian, since the Henselization is an algebraic, immediate extension.

(⇒) Let $(K', \mathcal{O}') \supseteq (K, \mathcal{O})$ be a proper, algebraic, immediate extension. Then clearly $\mathcal{O} \neq K$, and thus $\mathrm{char}\,K = 0$. Let $\alpha \in K' \setminus K$. Without loss of generality, suppose K'/K is finite, and let L be the normal closure of K'/K. Then $\mathcal{O}$ extends uniquely to L. In particular, this extension also extends $\mathcal{O}'$ from K' to L. Now

$$v(\beta) = v(\sigma(\beta)), \quad \text{for all } \beta \in L \text{ and } \sigma \in G := \mathrm{Gal}(L/K).^2 \qquad (A.3.19.1)$$

Let $\alpha^{[1]} = \alpha, \alpha^{[2]}, \ldots, \alpha^{[n]}$ be the conjugates of α. Then

[2] This follows from the fact that $\sigma|_K = \mathrm{id}$ or that the order of σ is finite (cf. Exercise A.7.4(iii)).