ABSOLUTE VALUES III: THE FUNDAMENTAL IN/EQUALITY, HENSEL AND KRASNER

PETE L. CLARK

Contents

3. Residual degree and ramification index

Let (K, v) be a valued field, with valuation ring R and maximal ideal $\mathfrak{m}$. As with any maximal ideal, the quotient ring $R/\mathfrak{m}$ is a field, called the **residue field** of K and denoted k. (Note that we have switched from k to K for our normed/valued field so as to allow the introduction of the residue field.) We have a canonical surjective map $R \to k$ called the **reduction map**.

Example: Suppose K is any field and v is the trivial (i.e., identically zero) valuation. Then $R = K$, $\mathfrak{m} = 0$, so $k = K$ and the reduction map is an isomorphism. Conversely, if the reduction map is injective, the valuation is trivial.

Example: Let ord_p be the p-adic norm on $\mathbb{Q}$. Then the valuation ring is the local ring R of all rational numbers of the form $\frac{a}{b}$ with b not divisible by p. This is of course the localization of $\mathbb{Z}$ at the maximal ideal (p). It follows that $R/\mathfrak{m} \cong \mathbb{Z}/(p) \cong \mathbb{F}_p$.

Example: Let k be a field and $R = k[[t]]$ and $K = k((t))$. Then the maximal ideal consists of all formal power series with 0 constant term, and it is easily seen that $R/\mathfrak{m} \cong k$ in such a way that the composite map $k \hookrightarrow R \to R/\mathfrak{m} \cong k$ is the identity. Thus in this case the residue field is also realized as a subfield of K.

Example: let k be a field, $R = k[t]$, $K = k(t)$. Let ord_t be the valuation corresponding to the prime element (t). Then again the residue field is isomorphic to $R/(t) \cong k$. More generally:

Date: June 6, 2010.

Proposition 1. *Let R be a Dedekind domain with fraction field K. Let $\mathfrak{p}$ be a nonzero prime ideal of R, and let $v = \mathrm{ord}_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic valuation. Then the residue field is naturally isomorphic to $R/\mathfrak{p}$.*

Exercise 3.1: Prove Proposition 1.

Now let $(L,w)/(K,v)$ be an extension of valued fields. Recall that this means that we have a field homomorphism $\iota : K \hookrightarrow L$ such that $w \circ \iota = v$. In such a situation, ι induces an embedding of valuation rings $R \hookrightarrow S$ and of maximal ideals $\mathfrak{m}_R \hookrightarrow \mathfrak{m}_S$. We may therefore pass to the quotient and get a homomorphism

$$\bar{\iota} : k = R/\mathfrak{m}_R \hookrightarrow S/\mathfrak{m}_S = l,$$

called the **residual extension**. The degree $[l : k]$ is called the **residual degree** and is also denoted $f(L/K)$.

Exercise 3.2: Suppose that L/K is algebraic. Show that l/k is algebraic.

Again let $(K,v) \hookrightarrow (L,w)$ be a homomorphism of valued fields. Then we have $v(K) \subset w(L)$. We define the **ramification index** $e(L/K)$ to be $[w(L) : v(K)]$. In terms of the associated norms, we have $e(L/K) = \frac{|L^\times|}{|K^\times|}$.

Exercise 3.3: Suppose L/K is algebraic. Show $w(L)/v(K)$ is a torsion group.

Example: Consider $L = \mathbb{Q}_p(p^{\frac{1}{n}})$ with the unique valuation w extending the p-adic valuation v on $\mathbb{Q}_p$. Of course $v(\mathbb{Q}_p) = \mathbb{Z}$ with uniformizing element p: $v(p) = 1$. Thus

$$1 = w(p) = w((p^{\frac{1}{n}})^n) = nw(p^{\frac{1}{n}}),$$

so that $w(p^{\frac{1}{n}}) = \frac{1}{n}$. It follows that $e(L/\mathbb{Q}_p) \geq n$. In fact we have $e(L/\mathbb{Q}_p) = n$, a consequence of the following:

Theorem 2. *(Degree Inequality (Preliminary Version)) Let $(K,|\ |) \hookrightarrow (L,|\ |)$ be an extension of non-Archimedean normed fields, with $[L : K] = n$. Then*

$$e(L/K)f(L/K) \leq n.$$

Proof. As usual, we let $(R,\mathfrak{m}_R)$ be the valuation ring of $(K,|\ |)$ and $(S,\mathfrak{m}_S)$ the valuation ring of $(L,|\ |)$. Let $u_1,\ldots,u_{f_1}$ be elements of S whose reductions modulo $\mathfrak{m}_S$ are linearly independent over $k = R/\mathfrak{m}_R$. (In particular, we have $u_i \in S^\times$ for all i.) Thus given elements $a_1,\ldots,a_{f_i} \in R$ such that $\sum_i a_i u_i \in \mathfrak{m}_S$, we have $a_i \in \mathfrak{m}_S$ for all i. Let $b_1,\ldots,b_{e_1}$ be elements of $L^\times$ whose images in $|L^\times|/|K^\times|$ are distinct. It suffices to show that the $e_1 f_1$ elements $u_i b_j$ of L are linearly independent over K. Scaling by elements of $K^\times$ does not disturb this conclusion, so we may assume WLOG that $b_j \in \mathfrak{m}_S$ for all j.
Step 1: Suppose that $a_i \in K$. Then $|\sum_i a_i u_i| \in |K|$.

Proof: Indeed, if $\sum_i a_i u_i \neq 0$, then some $a_i \neq 0$; by reordering we may assume that $0 = |a_1| \geq |a_i$ for all i. Then

$$|\sum_i a_i u_i| = |a_1||\sum_i a_1^{-1} a_i u_i|.$$

Moreover $|\sum_i a_i^{-1} a_i u_i| \leq 1$. If we had $|\sum_i a_i^{-1} a_i u_i| < 1$, then $\sum_i a_i^{-1} a_i u_i \in \mathfrak{m}_S$, and since $|a_1^{-1} a_i| \leq 1$, $a_1^{-1} a_i \in R$ for all i. The relation $\sum_i a_1^{-1} a_i u_i \in \mathfrak{m}_S$ contradicts

the definition of the u_i. Hence $|\sum_i a_1^{-1} a_i u_i| = 1$, so $|\sum_i a_i u_1| = |a_1| \in |K|$.

Step 2: Now suppose that there exist $a_{ij} \in K$ such that $\sum_{i,j} a_{ij} u_i b_j = 0$. If there exists j such that $\sum_i a_{ij} u_i \neq 0$, then $\sum_{i,j} a_{ij} u_i b_j = 0$ implies the existence of distinct j, say $j = 1$ and $j = 2$, such that $|\sum_i a_{i1} u_i b_1| = |\sum_i a_{i2} u_i b_2| \neq 0$. Then $\sum_i a_{i1} u_i \neq 0$ and $\sum_i a_{i2} u_i \neq 0$, so $|\sum_i a_{i1} u_i|, |\sum_i a_{i2} u_i| \in |K^\times|$. Then $|b_1||K^\times| = |b_2||K^\times|$, contrary to the choice of the b_j's. Thus the relation $\sum a_{ij} u_i b_j = 0$ implies $\sum_i a_{ij} u_i = 0$ for all j. Scaling by a suitable nonzero element of F, we get relations of the form $\sum_i a'_{ij} u_i = 0$ with $a'_{ij} \in R$, and unless all a_{ij}'s are 0, we may assume that one of them does not lie in $\mathfrak{m}_S$, contradicting the definition of the u_i's. Therefore the $e_1 f_1$ elements $u_i b_j$ are linearly independent over K, qed. □

Must we have equality in Theorem 2? Of course not! Consider the familiar case in which R is a Dedekind domain, K is its fraction field, L/K is a finite separable field extension of degree n, S is the integral closure of R in L, and $v = \mathrm{ord}_{\mathfrak{p}}$ is the valuation associated to a nonzero prime ideal $\mathfrak{p}$ of R. Then if $\mathfrak{p}S = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_g}$, we have $\sum_{i=1}^g e_i f_i = n$. On the other hand, for any $1 \leq i \leq g$, if we take w_i to be the $\mathcal{P}_\rangle$-adic valuation (renormalized so as to extend $\mathrm{ord}_{\mathfrak{p}}$), then we have $e(L/K) f(L/K) = e_i f_i$. So we cannot have equality when there is more than one prime of S lying over $\mathfrak{p}$.

By now it should be clear what to do: pass to the completions! For one thing, the invariants $e(L/K)$ and $f(L/K)$ are "local" in the sense that they are unchanged upon passage to the completion:

Proposition 3. *Let $(K, v) \hookrightarrow (L, w)$ be a finite degree extension of valued fields, with $[L : K] = n$. By functoriality of completion, we get a homomorphism $(\hat{K}, \hat{v}) \hookrightarrow (\hat{L}, \hat{w})$. Then:*
a) $[\hat{L} : \hat{K}] \leq n$.
b) $v(K) = \hat{v}(\hat{K})$ and $w(L) = \hat{w}(\hat{L})$ (completion does not change the value group).
c) The homomorphism of residue extensions $k \hookrightarrow \hat{k}$ induced by $K \hookrightarrow \hat{K}$ is an isomorphism.
d) We have $f(L/K) = f(\hat{L}/\hat{K})$ and $e(L/K) = e(\hat{L}/\hat{K})$.

Exercise 3.4: Prove Proposition 3.

Theorem 4. *(Fundamental Degree In/Equality) Let (K, v) be a nontrivial valued field and L/K a field extension of degree n. Let $w_1, \ldots, w_g$ be the valuations on L extending v on K. For each such i, we define $e_i(L/K) = e((L, w_i)/(K, v))$. Then:*
a) We have

$$\sum_{i=1}^g e(L_i/K) f(L_i/K) \leq [L : K]. \tag{1}$$

b) We have equality in (1) under the following hypotheses: v is discrete and S, the integral closure of R in L, is finitely generated as an R-module.
*c) In particular, if v is discrete and L/K is finite and **separable**, then equality holds in (1).*

Proof. a) Let $\hat{L}_i$ be the completion of L with respect to w_i, and let $n_i = [\hat{L}_i : \hat{K}]$. By Theorem 2 and Propostion 3 we have, for all $1 \leq i \leq g$, that $e_i f_i \leq n_i$. On the other hand, by Theorem 2.19 we have $\sum_i n_i = \dim_{\hat{K}} \prod_{i=1}^g \hat{L}_i \leq \dim_{\hat{K}} L \otimes_K \hat{K} = [L : K]$. Thus $\sum_{i=1}^g e(L_i/K) f(L_i/K) = \sum_{i=1}^g e(\hat{L}_i/\hat{K}) f(\hat{L}_i/\hat{K}) \leq \sum_{i=1}^g n_i \leq [L : K]$.

b) Suppose that S is a finitely generated R-module. Since R and S are both domains, certainly S is a torsionfree R-module. Then, since R is a DVR and hence a PID, it follows from the structure theory of finitely generated modules over a PID that $S \cong R^m$ for some $m \in \mathcal{N}$. Since $K^n \cong L = S \otimes_R K \cong K^m$, we must have $m = n = [L : K]$. Moreover S is a Dedekind domain [Clark-CA, §17]. Therefore we may take $\mathfrak{p}$, the unique nonzero prime ideal of R, and factor the pushforward into prime powers:

$$\mathfrak{p}S = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}.$$

Applying the Chinese Remainder Theorem, we get $(R/\mathfrak{p})$-module isomorphisms

$$(R/\mathfrak{p})^n \cong R^n/\mathfrak{p}R^n \cong S/\mathfrak{p}S = S/(\prod_{i=1}^{g} \mathcal{P}_i^{e_i}) \cong \prod_{i=1}^{g} S/\mathcal{P}_i^{e_i}.$$

Since $\mathfrak{p}$ is a maximal ideal of R, $R/\mathfrak{p}$ is a vector space, and we may equate $R/\mathfrak{p}$-dimensions of both sides. Clearly $\dim(R/\mathfrak{p})^n = n$. On the other hand, since each $\mathcal{P}_i$ is a principal ideal (if it weren't, no problem: since localization commutes with passage to the quotient, we could make it so by passing the localization), multiplication by the kth power of a uniformizer of $\mathcal{P}_i$ gives an $S/\mathcal{P}_i$-isomorphism from $S/\mathcal{P}_i$ to $\mathcal{P}_i^k/\mathcal{P}_i^{k+1}$. Therefore

$$\dim_{R/\mathfrak{p}} S/\mathcal{P}_i^{e_i} = e_i \dim_{R/\mathfrak{p}} S/\mathcal{P}_i = e_i f_i \dim_{S/\mathcal{P}_i} S/\mathcal{P}_i = e_i f_i,$$

and we conclude $n = \sum_{i=1}^{g} e_i f_i$.
c) This follows from the following important result of commutative algebra. □

Theorem 5. *(First Normalization Theorem) Let R be an integrally closed domain with fraction field K, let L/K be a finite separable field extension, and let S be the integral closure of R in S. Then S is finitely generated as an R-module.*

Proof. (Serre) Let $T : L \times L \to K$ be the **trace form**, i.e., $T : (a, b) \in L^2 \mapsto \mathrm{Tr}_{L/K}(ab)$. This is a symmetric K-bilinear form on L. It is a basic field-theoretic fact the trace form is nondegenerate iff L/K is separable (e.g. [Clark-FT, §8]).
Step 1: We have $\mathrm{Tr}(B) \subset A$. Indeed, let $x \in B$. Then $\mathrm{Tr}_{L/K}(x)$ is the sum of conjugates of x – i.e., other roots of the minimal polynomial of x over K – hence is a sum of integral elements and thus integral. Thus $\mathrm{Tr}_{L/K}(x)$ is integral over R and lies in K; since R is integrally closed, the conclusion follows.
Step 2: Let $e_1, \ldots, e_n$ be a K-basis for L. By clearing denominators, we may assume that each e_i lies in S. Let $V = \langle e_1, \ldots, e_n \rangle_R$, a free, rank n R-module. Using the trace form, we define for each R-submodule M of L a "dual" submodule M^*:

$$M^* = \{x \in L \mid \forall m \in M, \mathrm{Tr}_{L/K}(xm) \in R\}.$$

Then we have a chain of R-module inclusions

$$V \subset B \subset B^* \subset V^*.$$

Let $(e^1, \ldots, e^n)$ be the dual basis to $(e_1, \ldots, e_n)$ under trace form, i.e., such that $T(e_i, e^j) = \delta_{i,j}$ (Kronecker delta). By the nondegeneracy of T, $(e^1, \ldots, e^n)$ exists uniquely and is a K-basis of L. Let $W = \langle e^1, \ldots, e^n \rangle_R$. We claim that $W = V^*$. First, for any $1 \leq i \leq n$ and $m_1, \ldots, m_n \in R$, we have $T(e^i(m_1 e_1 + \ldots + m_n e_n)) = \sum_{j=1}^{n} m_j T(e^i e_j) \subset R$, so $e^i \in V^*$ and thus $W \subset V^*$. Conversely, since $(e^1, \ldots, e^n)$ is a K-basis for L, an element of V^* may be written uniquely as $v = a_1 e^1 + \ldots + a^n e^n$

with $a_i \in K$. But then for all i, $a_i = \mathrm{Tr}_{L/K}(ve_i) \in R$, so $v \in W$. It follows that V^* is a finitely generated R-module. Since R is Noetherian, its submodule B is also finitely generated. □

We will not need them, but here are two further sufficient conditions for equality in Theorem 4:

Theorem 6. *Maintain the same setup as in Theorem 3.4. Suppose that* either *K is complete and discretely valued* or *the residue field of K has characteristic 0. Then equality holds in (1).*

Proof. See O. Endler's *Valuation Theory.* □

3.1. **Hensel's Lemma.** We have already seen two incarnations of Hensel's Lemma in our proof of the existence of the extended norm in a finite dimensional extension of a complete non-Archimedean field. In fact, our first proof of this result remains incomplete (so to speak!) until we establish this form of Hensel's Lemma.

In fact there are many, many results which go by the name Hensel's Lemma, both in valuation theory and in commutative algebra. In commutative algebra one has the concept of a **Henselian local ring**, which is especially important in the field of étale cohomology. We have no need of this concept here, so we will stick to valuation-theoretic formulations of Hensel's Lemma. From a valuation theoretic framework, the most natural and intrinsic version of Hensel's Lemma is indeed that for any finite dimensional field extension L/K, the valuation v extends uniquely to a valuation on L. Recall that we call this condition **Henselian** and then the existence result referred to above can be succinctly restated as: complete valued fields are Henselian.

The following is a rather detailed and careful formulation of various valuation theoretic forms of Hensel's Lemma. It will be sufficient for our purposes for the rest of the course (and, I hope, beyond).

Theorem 7. *(Omnibus Hensel's Lemma) Let (K, v) be a valued field with valuation ring R and maximal ideal $\mathfrak{m}$.*
a) The following conditions are equivalent:
*(i) (Henselian): For every finite extension L/K, v extends **uniquely** to L.*
(ii) (Hensel-Kurschak): A monic irreducible polynomial $P(t) \in K[t]$ with constant coefficient lying in R ring has all its coefficients lying in R.
(iii) (Newton's Method) Let $f \in R[t]$ be a polynomial. Suppose that there exists $\alpha \in R$ such that $v(f(\alpha)) > 2v(f'(\alpha))$. Then there exists $\beta \in R$ such that $f(\beta) = 0$ and $v(\alpha - \beta) > v(f'(\alpha))$.
(iv) (Lifting of factorizations) Suppose $f \in R[t]$ is a primitive polynomial such that $f \equiv \overline{g}\overline{h} \pmod{}m$ with $\gcd(\overline{g}, \overline{h}) = 1$. Then $\overline{g}$ and $\overline{h}$ lift to polynomials $g, h \in R[t]$ such that $f = gh$ and $\deg(g) = \deg(\overline{g})$.
(v) (Lifting of smooth points on varieties) Let $k \leq n$ be positive integers, and let $f_1, \ldots, f_k \in R[t] = R[t_1, \ldots, t_n]$ be polynomials. Suppose there exists $\overline{x} = (\overline{x_1}, \ldots, \overline{x_n}) \in R/\mathfrak{m}$ such that $f_1(\overline{x}) = \ldots = f_k(\overline{x}) = 0$ and the derivative matrix $(\frac{\partial f_i}{\partial \overline{x}_j})$ evluated at $\overline{x}$ has rank k. Then $\overline{x}$ lifts to a point $x \in R^n$ such that $f_1(x) = \ldots = f_k(x) = 0$.
b) Each of the equivalent conditions of part a) holds when (K, v) is complete.

Proof. ... □

3.2. **Squares in local fields.**

Proposition 8. *Let (K, v) be a discretely valued field. Then a choice of uniformizing element $\pi \in K$ gives rise to an isomorphism of groups $(K^\times, \cdot) \cong (R^\times, \cdot) \times (\mathbb{Z}, +)$.*

Proof. We have the short exact sequence

$$1 \to R^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0.$$

Because $\mathbb{Z}$ is a free – hence projective! – $\mathbb{Z}$-module, the sequence splits. To choose a splitting it is necessary and sufficient to lift the generator $1 \in \mathbb{Z}$ to an element in $K^\times$. This is precisely the choice of a uniformizing element. □

Thus for instance the group-theoretic study of $K^\times$ is reduced to that of $R^\times$. In these kind of considerations, it is traditional to change notation and terminology: put $U := R^\times$ and call U the **unit group** of K. (This is, strictly speaking, an abuse of terminology, since the unit group of K should just be $K^\times$. However, it is traditional and not very confusing. Anyway, by the previous result, the two groups are very closely related!)

Proposition 9. *Let p be an odd prime number, and let $u \in \mathbb{Z}$ be a quadratic nonresidue modulo p. Then $[\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times 2}] = 4$, and a set of coset representatives is $1, p, u, pu$.*

Exercise 3.5: Prove Proposition 9.

Proposition 10. *We have $[\mathbb{Q}_2^\times : \mathbb{Q}_2^{\times 2}] = 8$. A set of coset representatives is $\pm 1, \pm 2, \pm 5, \pm 10$.*

Exercise 3.6: Prove Proposition 10.

Proposition 11. *Let q be an odd prime power and let $K = \mathbb{F}_q((t))$. Then $[K^\times : K^{\times 2}] = 4$. A set of coset representatives is $1, u, t, ut$, where $u \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^\times$.*

Exercise 3.7: Prove Proposition 11.

Note that for for any field K, $K^\times / K^{\times 2}$ is an elementary abelian 2-group, called the group of **square classes** of K. In particular, it is a $\mathbb{Z}/2\mathbb{Z}$-vector space. Thus, instead of listing all of its elements, it would be equivalent but more efficient to give a basis. In the case of $\mathbb{Q}_p$ with p odd, a basis is given by p, u. In the case of $\mathbb{Q}_2$, a basis is given by $-1, 2, 5$.

Exercise 3.8: a) Let K be a Henselian discrete valuation field with residue field k of characteristic different from 2. Show that $\dim_{\mathbb{F}_2} K^\times / K^{\times 2} = \dim_{\mathbb{F}_2} k^\times / k^{\times 2} + 1$.
b) Suppose further that $K = k((t))$. Let $\{b_i\}_{i \in I}$ be an $\mathbb{F}_2$-basis for $k^\times / k^{\times 2}$. Show that an $\mathbb{F}_2$-basis for $k((t))^\times / k((t))^{\times 2}$ is $\{b_i\} \cup \{t\}$.

Exercise 3.9: What can you say about the set of square classes in $\mathbb{F}_2((t))$?

3.3. **Quadratic forms over local fields.**

We begin with a very brief review of the notion of a quadratic form over a field and some associated invariants. For more information, the reader may consult

[Clark-QF] or the classic texts of Cassels [Cas] or Lam [Lam].

Let K be a field of characteristic different from 2 but otherwise arbitrary.[1] A **quadratic form** q over K is a polynomial $q(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$, i.e., homogeneous of degree 2. (We say that n is the **dimension** of q.) We define the **Gram matrix** M_q whose (i,i) entry is $a_{i,i}$ and whose (i,j) entry, for $i \neq j$, is $\frac{a_{ij}}{2}$ (note that we are using $2 \in K^\times$ here!). Then if we let x denote the column vector $(x_1, \ldots, x_n)$, we have the identity

$$q(x_1, \ldots, x_n) = x^T M_q x.$$

We wish to regard two quadratic forms over K as "equivalent" if one can be obtained from the other by an invertible linear change of variables. More explicitly, for any $P \in$
$operatornameGL_n(K)$, we define $(P \bullet q)(x) = q(Px)$. Here is one slightly tricky point for beginners: for any vector $x \in K^n$, we have

$$(P \cdot q)(x) = x^T M_{P \cdot q} x = (Px)^T M_q P x = x^T P^T M_q P x,$$

and it follows that the matrix representative of $P \bullet q$ is $P^T M_q P$. In other words, the induced relation on symmetric matrices is not similarity but the above relation, classically called **congruence** of matrices.

Recall that any symmetric matrix M over the real numbers can be not only diagonalized but orthogonally diagonalized, i.e., there exists a matrix P with $PP^T = 1_n$ such that $P^{-1}MP$ is diagonal. By orthogonality of P, we have $P^{-1}MP = P^T MP$, so the result implies that any quadratic form over the real numbers can be **diagonalized**, i.e., after a linear change of variables is given in the diagonal form

$$\langle a_1, \ldots, a_n \rangle = a_1 x_1^2 + \ldots + a_n x_n^2.$$

One of the classical theorems of the subject is a generalization of this: over any field K of characteristic different from 2 is diagonalizable.

Exercise 3.9.5: A very special and important quadratic form is $q_{\mathbb{H}}(x_1, x_2) = x_1 x_2$, the so-called **hyperbolic plane**.
a) Let K be any field of characteristic different from 2. Give an explicit change of variables that diagonalizes $q_{\mathbb{H}}$.
b) Show by brute force that $q_{\mathbb{H}}$ cannot be diagonalized over $\mathbb{F}_2$.
c) Show that $q_{\mathbb{H}}$ cannot be diagonalized over any field of characteristic 2.

A quadratic form is said to be **nondegenerate** if any of its defining symmetric matrices are invertible, and otherwise degenerate. It can be shown that any nondegenerate quadratic form in n variables is $\mathrm{GL}_n(K)$-equivalent to a quadratic form in fewer variables. Applying this observation repeatedly, we may view any degenerate quadratic form simply as a strangely presented nondegenerate quadratic form in fewer (possibly 0) variables, so it is harmless to restrict attention to nondegenerate forms.

A quadratic form q is **anisotropic** if for all $a = (a_1, \ldots, a_n) \in K^n$, $q(a) = 0$

[1] The case of characteristic 2 comes up in at least one exercise, but only as an example of what can go wrong!

implies $a = (0, \ldots, 0)$. In other words, the quadratic hypersurface $q(x) = 0$ has no K-rational points. A nondegenerate quadratic form which is not anisotropic is called **isotropic**.

Let $n \in \mathbb{Z}^+$. A field K is said to have **u-invariant** n – written $u(K) = n$ – if every quadratic form over K in more than n variables is isotropic and there exists at least one n-dimensional anisotropic quadratic form over K. If no such positive integer exists, we say that $u(K) = \infty$.

Example: Over any field K, the quadratic form $q(x) = x^2$ is anisotropic. Over the complex numbers, any quadratic form in at least 2-variables is isotropic, so $u(\mathbb{C}) = 1$. Indeed this holds for any algebraically closed field. Moreover, we say a field is **quadratically closed** if it admits no nontrivial quadratic extension – equivalently, $K^\times = K^{\times 2}$. Then:

Exercise 3.10: Let L/K be a degree n field extension. Let $b_1, \ldots, b_n$ be a K-basis for L. Define a polynomial $N(x)$ by $N_{L/K}(x_1 b_1 + \ldots + x_n b_n)$ (i.e., the norm from L down to K).
a) Show that for all $0 \neq x \in K^n$, $N(x) \neq 0$.
b) Suppose $n = 2$. Show that the equivalence class of the quadratic form $N(x)$ is well-defined independent of the chosen basis of L/K.

Exercise 3.11: Let K be any field of characteristic different from 2. Show that $u(K) = 1$ iff K is quadratically closed.

Example: For any $n \in \mathbb{Z}^+$, the quadratic form $q(x) = x_1^2 + \ldots + x_n^2$ is anisotropic over $\mathbb{R}$, since it is always strictly positive when evaluated at any nonzero vector. Thus $u(\mathbb{R}) = \infty$. The same holds for any **formally real** field. (However the converse is not true, e.g. a rational function field in infinitely many indeterminates over $\mathbb{C}$ has u-invariant ∞.)

Proposition 12. *The u-invariant of any finite field is* 2.

Proof. Since every finite field admits a quadratic extension, it follows from Exercise 3.10 that the u-invariant is at least 2. The fact that any quadratic form in at least 3-variables over a finite field has a nontrivial zero is a special case of the Chevalley-Warning theorem. □

Lemma 13. *Let K be a Henselian, discretely valued field with valuation ring R, uniformizer π, and residue field k of characteristic different from 2. Let $n \in \mathbb{Z}^+$ and $a_1, \ldots, a_n \in R^\times$, and let $0 \leq r \leq n$. Consider the quadratic forms*

$$q_1(x_1, \ldots, x_r) = a_1 x_1^2 + \ldots + a_r x_r^2$$
$$q_2(x_{r+1}, \ldots, x_n) = a_{r+1} x_{r+1}^2 + \ldots + a_n x_n^2$$
$$q(x) = q_1(x_1, \ldots, x_r) + \pi q_2(x_{r+1}, \ldots, x_n).$$

Then q is isotropic over K iff at least one of q_1, q_2 is isotropic over K.

Proof. Clearly q_2 is isotropic iff πq_2 is isotropic ("isotropy is a similarity invariant"). Just as clearly, if a subform of a quadratic form is isotropic, then so is the quadratic form. Thus certainly the isotropy of either q_1 or q_2 implies the isotropy of q, so it

suffices to show the converse: assume q is isotropic. Then by the usual rescaling arguments there exists a *primitive vector* x such that $q(x) = 0$: that is, each coordinate of x lies in R and at least one coordinate of x is not divisible by π.
Case 1: Suppose first that there exists $1 \leq i \leq r$ with $x_i \neq 0$. Then reducing mod p gives $q_1 \equiv 0 \pmod{p}$ and $\frac{\partial q_0}{\partial x_i} = 2a_i x_i \neq 0 \pmod{p}$, so by Hensel's Lemma q_1 is isotropic.
Case 2: Then we have that $p \mid x_i$ for $1 \leq i \leq r$, so $q_1(x_1, \ldots, x_r) \equiv 0 \pmod{p}^2$. Therefore reducing modulo p^2 and dividing by p, we see that $q_1(x_{r+1}, \ldots, x_n) \equiv 0 \pmod{p}$. Applying Hensel's Lemma as in Case 1, we see q_2 is isotropic over $\mathbb{Q}_p$. □

Theorem 14. *Let K be a Henselian discretely valued field with residue field k. We suppose that the characteristic of k is different from 2. Then*

$$u(K) = 2u(k).$$

In particular, for an odd prime p, $u(\mathbb{Q}_p) = 4$.

Proof. Let $q = q(x_1, \ldots, x_n)$ be a nonsingular quadratic form over K with $n > 2u(k)$. Then q is equivalent (after a linear change of variables) to a form $q = q_1 + \pi q_2$ as in the statement of Lemma 13. By our hypothesis on n, at least one of q_1, q_2 has more than $u(k)$ variables, so the reduction modulo (π) is isotropic by assumption and then the form itself is isotropic by Hensel's Lemma. Thus $u(K) \leq 2u(k)$.

Conversely, if $u(k) = r$, let $\overline{q}(x_1, \ldots, x_r)$ be an anisotropic form over k. We may lift each coefficient of $\overline{q}$ to an element of $R^\times$ and thus get a quadratic form $q(x_1, \ldots, x_r)$. Now q itself is anisotropic over K: indeed, if not, there would exist a primitive vector x such that $q(x) = 0$ and then reduction modulo (π) would show that $\overline{q}$ is isotropic. It then follows from Lemma 13 that the quadratic form $q(x_1, \ldots, x_n) + \pi q(x_{n+1}, \ldots, x_{2n})$ is isotropic over K. □

Example: Suppose that $p \equiv 3 \pmod{4}$. Then $(\frac{-1}{p}) = -1$, so $x^2 + y^2$ is anisotropic mod p. The above proof shows that $x_1^2 + x_2^2 + px_3^2 + px_4^2$ is anisotropic over $\mathbb{Q}_p$.

Exercise 3.12: Show that for every $a \in \mathcal{N}$, there exists a field K with $u(K) = 2^a$.
Exercise 3.13:
a) Show that the quadratic form $q(x, y, z) = x^2 + y^2 + z^2$ is anistropic over $\mathbb{Q}_2$.
b)* For each odd prime p, find $a, b, c \in \mathbb{Z}$ such that $q = ax^2 + by^2 + cz^2$ is anisotropic over $\mathbb{Q}_p$.

Exercise 3.13.5: Show that $u(\mathbb{Q}_2) = 4$. (See e.g. [Lam] for one approach: this is somewhat involved.)

3.4. **Roots of unity in local fields.**

For any field F, we denote by $\mu(F)$ the torsion subgroup of $F^\times$ – or, more colloquially, the **roots of unity** in F.

We are interested in the roots of unity of a valued field (K, v). Note that we certainly have $\mu(K) \subset R^\times$: all roots of unity have valuation 0. As usual, we can say something in this level of generality, but to get definitive results we will restrict to p-adic fields and/or Laurent series fields.

We define $\mu'(K)$ as follows: if the residue field k has characteristic 0, then $\mu'(K) =$

$\mu(K)$. However, if the residue field k has characteristic $p > 0$, then $\mu'(K)$ is, by definition, the group of all roots of unity of K of order coprime to p. Note also that $\mu'(k) = \mu(k)$, since a field of characteristic p has no nontrivial p-power roots of unity.

This somewhat curious definition is justified by the following result.

Proposition 15. *Let (K, v) be a Henselian valued field. Then the restriction of the mod $\mathfrak{m}$ reduction map to $\mu'(K)$ is an isomorphism of groups $r' : \mu'(K) \xrightarrow{\sim} \mu(k)$.*

Proof. As observed above, every root of unity of K lies in the valuation ring. Moreover, certainly the image of an element of finite order under a group homomorphism has finite order, so there is no doubt that there is a homomorphism $r : \mu(K) \to \mu(k)$. Note though that because – when $\mathrm{char}(k) = p > 0$ – k has no p-power roots of unity, the reduction map restricted to $\mu[p^\infty](K)$ is trivial, so we may as well restrict our attention to the complementary subgroup $\mu'(K)$.
Let $x \in \mu(k) = \mu'(k)$ have order n. Put $P(t) = t^n - 1$; then $P'(x) = nx^{n-1} \neq 0$. By Hensel's Lemma, there exists $\tilde{x} \in K$ reducing to x and such that $x^n = 1$. Since $\tilde{x}^n = 1$, the order of $\tilde{x}$ divides n; since $q(\tilde{x}) = x$, n divides the order of $\tilde{x}$, thus $\tilde{x}$ has exact order n. The surjectivity of r' follows. But moreover, suppose that the kernel of ρ' is nontrivial. Then, being a nontrivial torsion group with no elements of order p, the kernel contains an element of prime order $\ell \neq p$, i.e., there exists a primitive ℓth root of unity $\tilde{x}$ such that $r(\tilde{x}) = 1$ and therefore $r(\tilde{x}^k) = 1$ for all k. But by virtue of being a primitive ℓth root of unity, we have $\tilde{x}^{\ell-1} + \ldots + \tilde{x} + 1 = 0$ and reducing this equation modulo the maximal ideal gives $\ell = 0$, a contradiction. Therefore r' is an isomorphism. □

In particular, this shows that the group of roots of unity in $\mathbb{Q}_p$ of order prime to p is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, hence cyclic of order $p-1$. Next we wonder whether there are any p-power roots of unity in $\mathbb{Q}_p$. If there are any such, there are primitive pth roots of unity, so that the pth cyclotomic polynomial $\Phi_p(t)$ would have a root over $\mathbb{Q}_p$. It is well-known from basic algebraic number theory that $\Phi_p(t)$ is irreducible over $\mathbb{Q}$, a textbook application of Eisenstein's criterion. As we now explain, the standard application of Eisenstein's criterion in fact gives the irreducibility over $\mathbb{Q}_p$ as well. Recall:

Corollary 16. *(Corollary to Gauss's Lemma) Let R be a GCD-domain with fraction field K, and let $f \in R[t]$ be a polynomial.*
a) The following are equivalent:
(i) f is irreducible in $R[t]$.
(ii) f is primitive and irreducible in $K[t]$.
b) The following are equivalent:
(i) f is reducible in $K[t]$.
(ii) There exist $g, h \in R[t]$ such that $\deg(g), \deg(h) < \deg(f)$ and $f = gh$.

Proof. See e.g. §11 of my notes on Commutative Algebra:
`http://math.uga.edu/~pete/integral.pdf`. □

Theorem 17. *(Schönemann-Eisenstein Criterion) Let R be a domain with fraction field K, and let $f(t) = a_d t^d + \ldots + a_1 t + a_0 \in R[t]$. Suppose that there exists a prime ideal $\mathfrak{p}$ of R such that $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ for all $0 \leq i < d$ and $a_0 \notin \mathfrak{p}^2$.*
a) If f is primitive, then f is irreducible over $R[t]$.
b) If R is a GCD-domain, then f is irreducible over $K[t]$.

Proof. a) Suppose to the contrary that f is primitive and reducible over $R[t]$: i.e., there exists a factorization $f = gh$ with $g(t) = b_m t^m + \ldots + b_1 t + b_0$, $h(t) = c_n t^m + \ldots + c_1 t + c_0$, $\deg(g), \deg(h) < \deg(f)$ and $b_m c_n \neq 0$. Since $a_0 = b_0 c_0 \in \mathfrak{p} \backslash \mathfrak{p}^2$, it follows that exactly one of b_0, c_0 lies in $\mathfrak{p}$: say it is c_0 and not b_0. Moreover, since $a_d = b_m c_n \notin \mathfrak{p}$, $c_n \notin \mathfrak{p}$. Let k be the least index such that $c_k \notin \mathfrak{p}$, so $0 < k \leq n$. Then $b_0 c_k = a_k - (b_1 c_{k-1} + \ldots + b_k c_0) \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that at least one of $b_0,\ c_k$ lies in $\mathfrak{p}$, a contradiction.
b) If R is a GCD-domain, and suppose for a contradiction that f is reducible over $K[t]$, then by Corollary 16b), we may write $f = gh$ with $g, h \in R[t]$ and $\deg(g), \deg(h) < \deg(f)$. Then the proof of part a) goes through to give a contradiction. □

Remark: For our purposes we wish to apply this to the valuation ring R attached to a (as always rank one, unless otherwise specified) valuation v on the fraction field K, with $\mathfrak{p}$ the unique maximal ideal of R. Notice that in this case we may pass to the completion $\hat{K}$ and its valuation ring $\hat{R}$ without disturbing any of the hypotheses, so we get an automatic strengthening of Eisenstein's Criterion: f is irreducible not merely over $K[t]$ but also over $\hat{K}[t]$.

Remark: In particular, if (R, v) is a DVR with uniformizing element π, then Eisenstein's criterion applied to $P_n(t) = t^n - \pi$ gives rise to a totally ramified extension of degree n for all $n > 1$, as we have seen before.

Exercise 3.14: Let (K, v) be a nontrivial valued field, with valuation ring R and maximal ideal $\mathfrak{m}$. Show that the following are equivalent:
(i) $\mathfrak{m}^2 \subsetneq \mathfrak{m}$.
(ii) $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = \{0\}$.
(iii) R is Noetherian.
(iv) Γ is discrete.

In particular, for a (rank one) valuation ring, Eisenstein's criterion can only be successfully applied if the valuation is discrete.

Exercise 3.15*: Give an example of a non-Noetherian valuation ring R (necessarily of higher rank) to which Eisenstein's Criterion can be nontrivially applied.

Coming back down to earth, we apply the Eisenstein Criterion to $\mathbb{Q}_p$ and $f(t) = \Phi_p(t+1)$. We have

$$f(t) = \frac{(t+1)^p - 1}{t+1-1} = t^{p-1} + \binom{p}{1} t^{p-2} + \ldots + \binom{p}{p-2} t + p.$$

Applying the Eisenstein criterion to $\mathbb{Z}_p$ and $\mathfrak{p} = (p)$, we conclude that $f(t)$ is irreducible in $\mathbb{Q}_p[t]$ hence also $\Phi_p(t) = f(t-1)$ is irreducible in $\mathbb{Q}_p$. Therefore $\mathbb{Q}_p$ does not contain a primitive pth root of unity. In conclusion:

Theorem 18. *For any prime p, $\mu(\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.*

This raises a question: how did we know that Eisenstein's Criterion would apply here, after a change of variables? We will see later on that in the case of (K, v) a discretely valued field, Eisenstein's criterion can be applied (possibly to a different

polynomial which generates the same field extension) iff L/K is totally ramified at v.

Exercise 3.16: Let p be any prime number and r any positive integer. Let $\Phi_{p^r}(t) \in \mathbb{Q}[t]$ be the degree p^r cyclotomic polynomial. Show that $\Phi_{p^r}(t)$ is irreducible over $\mathbb{Q}_p$.

3.5. **Krasner's Lemma and Applications.**

Theorem 19. *(Krasner's Lemma) Let $(K, |\ |)$ be a Henselian non-Archimedean normed field with (uniquely normed) algebraic closure $\overline{K}$. Let $\alpha, \beta \in \overline{K}$. Write out the distinct K-conjugates of α as $\alpha = \alpha_1, \ldots, \alpha_n$. Suppose that for all $i > 1$ we have*

$$|\alpha - \beta| < |\alpha - \alpha_i|.$$

a) Then $K(\alpha, \beta)/K(\beta)$ is purely inseparable.
b) It follows that if α is separable over K, $K(\alpha) \subset K(\beta)$.

Proof. Part b) immediately follows from part a). As for part a), it suffices to show the following: for every $K(\beta)$-algebra embedding τ of $K(\alpha, \beta)$ into an algebraic closure $\overline{K}$, $\tau(\alpha) = \alpha$. As we have seen before, the uniqueness of extended norms implies that we have, for all $i > 1$,

$$|\tau(\alpha) - \beta| = |\tau(\alpha) - \tau(\beta)| = |\alpha - \beta| < |\alpha - \alpha_i|$$

and hence

$$|\tau(\alpha) - \alpha| \leq \max |\tau(\alpha) - \beta|, |\beta - \alpha| < |\alpha - \alpha_i|.$$

Since this holds for all $i > 1$ and $\tau(\alpha)$ is certainly a conjugate of α, we must have $\tau(\alpha) = \alpha$, qed. □

Exercise 3.17: Let $(K, ||)$ be an algebraically closed normed field. a) Let $n \in \mathbb{Z}^+$. Let $D(n)$ be the set of all degree n polynomials with coefficients in K which have n distinct roots, viewed as a subset of K^{n+1} in the evident way. Show that $D(n)$ is open in (the product topology on) K^{n+1}.
a') Suppose that K is any algebraically closed field. Show that $D(n)$ is open in K^{n+1} in the Zariski topology.
b) Show that the roots are continuous functions of the coefficients in the following sense: for all $\epsilon > 0$, there exists $\delta > 0$ such that: for any two polynomials $f(t) = \sum_n a_n t^n$ and $g(t) = \sum_n b_n t^n$ with $|a_i - b_i| < delta$ for all i, there exist orderings of the roots $\alpha_1, ..., \alpha_n$ of f and $\beta_1, ..., \beta_n$ of g such that $|\alpha_i - \beta_i| < \epsilon$ for all i.
c) Suppose that you restrict to degree n polynomials in $D(n)$. State and prove a version of part b) which does not involve permuting the roots. (Suggestion: consider disjoint open disks about each of the roots and argue that under sufficiently small changes of the coefficients, the roots stay inside the disjoint disks.)

Corollary 20. *(Krasner's Corollary) Let $f(t) = a_n t^n + \ldots + a_1 t + a_0$ be an irreducible separable degree n polynomial, and let α be one of its roots in a fixed algebraic closure $\overline{K}$. Then there exists $\delta > 0$ such that: for all $b_0, \ldots, b_n \in K$ with $|a_i - b_i| < \delta$ for all $0 \leq i \leq n$, the polynomial $g(t) := b_n t^n + \ldots + b_1 t + b_0$ is irreducible, separable, and has a root β such that $K(\alpha) = K(\beta)$.*

Proof. We apply Exercise 3.17 on continuity of roots of a polynomial with coefficients in a normed field in terms of the coefficients: for any $\epsilon > 0$, by taking δ sufficiently small we can ensure that the polynomial g is also separable and that

its roots $\beta_1, \ldots, \beta_n$, in some ordering, each lie within ϵ of the corresponding roots $\alpha_1, \ldots, \alpha_n$ of f. Taking $\epsilon = \min_{i>1} |\alpha_1 - \alpha_i|$ and applying part b) of Krasner's Lemma to β_1, we get that $K(\alpha_1) \subset K(\beta_1)$. However, since β_1 satisfies g, a polynomial of degree n, we have

$$n \geq [K(\beta_1) : K] \geq [K(\alpha_1) : K] = n.$$

Thus $[K(\beta_1) : K] = [K(\alpha_1) : K] = n$, so $g(t)$ is irreducible and $K(\alpha_1) = K(\beta_1)$. □

Corollary 21. *Let $(K, |\ |)$ be a non-Archimedean normed field with completion $\hat{K}$, and let $\mathcal{L}/\hat{K}$ be a finite separable field extension of degree d. Then there exists a degree d separable field extension L/K such that $\mathcal{L} = L\hat{K}$.*

Proof. By the Primitive Element Corollary, $\mathcal{L} \cong \hat{K}[t]/f(t)$, where $f(t) \in \hat{K}[t]$ is monic, separable of degree d. Since K is dense in $\hat{K}$, there exists a degree d polynomial $g(t) \in K[t]$ whose coefficients are all δ-close to the corresponding coefficients of $f(t)$, for any preassigned $\delta > 0$. By Krasner's Corollary, for sufficiently small δ, $g(t)$ is irreducible separable of degree d and there exist roots α_1 of f, β_1 of g such that $\hat{K}(\alpha_1) = \hat{K}(\beta_1)$. It follows that $\mathcal{L} = L\hat{K}$. □

Corollary 22. *Suppose that $(K, |\ |)$ is a separably closed normed field. Then its completion $(\hat{K}, |\ |)$ remains separably closed. In particular, defining $\mathbb{C}_p$ to be the completion of the algebraic closure of $\mathbb{Q}_p$, $\mathbb{C}_p$ is complete and algebraically closed.*

Proof. This follows immediately from Corollary 21. □

Corollary 21 can be viewed as saying that any one inert local extension of a NA normed field may be realized as the completion of a global extension. This result can be generalized in several ways: we can take work with several (but finitely many!) local extensions at once, each local extension need not be a field but only a separable algebra, and finally Archimedean places can be admitted. We get the following result, which has been of significant use to me in my own work (c.f. the proof of Theorem 6 in [Clark09]).

Theorem 23. *(Finite Local-Global Compatibility for Extensions) Let K be a field, and let $|\ |_1, \ldots, |\ |_g$ be inequivalent norms on K. For each $1 \leq i \leq g$, let $\hat{K}_i$ be the completion of K with respect to $|\ |_i$. Fix a positive integer d, and for each $1 \leq i \leq d$, let A_i be a degree d separable $\hat{K}_i$-algebra (i.e., a finite product of finite degree separable field extensions of K, with $\dim_{\hat{K}_i} A_i = d$. Then there exists a separable extension L/K of degree d and, for all $1 \leq i \leq g$, $\hat{K}_i$-algebra isomorphisms*

$$\Phi_i : L \otimes_K \hat{K}_i \xrightarrow{\sim} A_i.$$

Exercise 3.18: Prove Theorem 23.

3.6. **Multi-complete and multi-Henselian fields.**

Define a field K to be **multi-complete** if it is complete with respect to (at least) two inequivalent nontrivial norms. This seems like a strong property, and we seek to classify multi-complete fields.

Example: the complex field $\mathbb{C}$ is multi-complete. On the one hand $\mathbb{C}$ is complete with respect to the standard Archimedean norm. On the other hand, for any

prime p, let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with the p-adic norm. By Corollary 22, $\mathbb{C}_p$ is complete and algebraically closed. It is easy to see that $\#\mathbb{C}_p = \#\mathbb{C}$. By pure field theory – e.g. [Clark-FT, Cor. 78] – it follows that we have an isomorphism of abstract fields $\mathbb{C} \cong \mathbb{C}_p$.

Exercise 3.19: What is the cardinality of the set of pairwise inequivalent norms on $\mathbb{C}$ with respect to which $\mathbb{C}$ is complete?

Exercise 3.20: Suppose that K is a field which is complete with respect to an Archimedean norm $|| \; ||_1$ and also an inequivalent norm $|| \; ||_2$. Show that $K \cong \mathbb{C}$.

Thus in our study of multi-complete fields we may, and shall, restrict to non-Archimedean norms, or equivalently, to valuations.

Here is the main theorem for multi-complete fields.

Theorem 24. *(F.K. Schmidt* [Sch]*) A multi-complete field is algebraically closed.*

From this we can deduce a classification result for multi-complete fields.

Corollary 25. *(Schmidt) For a field K, the following are equivalent:*
(i) K is multi-complete.
(ii) K is algebraically closed and complete with respect to a nontrivial valuation.
(iii) K is algebraically closed and $(\#K) = (\#K)^{\aleph_0}$.

Proof. By Theorem 24, (i) $\implies$ (ii). Recall from Exercise 2.30.5 that a field which is complete with respect to a nontrivial norm satisfies $\#K = (\#K)^{\aleph_0}$, so (ii) $\implies$ (iii). Conversely, if K is algebraically closed and satisfies the cardinality condition, then K_v is complete, algebraically closed (c.f. Proposition 3.22 below) and of uncountably cardinality equal to that of K, so $K_v \cong K$. Thus (iii) $\equiv$ (ii). Finally, assume that K is algebraically closed and complete with respect to a nontrivial valuation v. Let $t \in K$ have negative valuation and which is transcendental over the prime subfield of K. (If every transcendental element t had non-negative valuation, then for any element of a of K, $v(a) = v(t + a - t) \geq \min v(t + a, -t) \geq 0$, so every element of K has non-negative valuation, and thus v is trivial.) By standard field theory – c.f. e.g. the proof of [Clark-FT, Thm. 80], the automorphim group of the algebraically closed field K acts transitively on the set of all transcendence bases for K over its prime subfield. In particular, there exists an automorphism σ such that $\sigma(t) = \frac{1}{t}$, and such an automorphism is evidently discontinuous for the valuation topology. Thus $\sigma^* v : x \mapsto v(\sigma(x))$ is an inequivalent complete valuation, i.e., K is multi-complete. □

It remains to prove Theorem 24. Rather than doing so now, we press on and introduce a small variant which we claim is more natural and more penetrating. Namely, we define a field K to be **multi-Henselian** if it is Henselian with respect to (at least) two inequivalent nontrivial valuations. Here is the main theorem of this section.

Theorem 26. *(Kaplansky-Schilling* [KS]*) A multi-Henselian field is separably closed.*

Proof. Let K be a field which is Henselian with respect to inequivalent, nontrivial valuations v_1 and v_2. Let L/K be a finite separable field extension. By the primitive

element theorem, we may write $L = K[t]/(P_1(t))$, where P_1 is an irreducible, monic, separable polynomial, say of degree d. Our task is to show that $d = 1$.

We will make an approximation argument using weak approximation, Krasner's Lemma and (an especially simple case of) Hensel's Lemma. Namely, by weak approximation the diagonal image of K in $K_{v_1} \times K_{v_2}$ is dense.

On the one hand, by Krasner's Lemma, there exists $\epsilon > 0$ such that any monic polynomial $Q \in K_{v_1}[t]$ each of whose coefficients is ϵ-close to the corresponding coefficients of P is also irreducible of degree d.

On the other hand, let $P_2(t) = t(t+1)^{d-1}$. Then $P_2(t)$ is monic of degree d, and its reduction modulo v_2 is (of course) $t(t+1)^{d-1} \in k_{v_2}[t]$. We may therefore apply Hensel's Lemma to P_2 to see that it has a root in K. Well, that's silly – of course it has a root: $P_2(0) = 0$. But moreover, if $Q(t) \in K[t]$ is any polynomial which is sufficiently close to P_2 such that the coefficients of $P_2 - Q$ all have positive valuation, then the reduction of Q modulo the maximal ideal is also equal to $t(t+1)^{d-1}$. Therefore Hensel's Lemma applies equally well to show that Q has a rational root.

The endgame is thus: by weak approximation, we may choose a monic degree d polynomial Q which is, at the same time, sufficiently v_1-adically close to P_1 to be irreducible and sufficiently v_2-adically close to P_2 so as to have a rational root. Of course an irreducible polynomial with a rational root must have degree 1, qed. □

It is now a relatively easy matter to deduce Schimidt's Theorem from the Kaplansky-Schilling Theorem. What we need to show is that a field which is multi-complete and separably closed is algebraically closed. But in fact we can prove a stronger result, whose statement and proof are of independent interest.

Proposition 27. *Let K be a field which is complete with respect to a nontrivial extension and separably closed. Then K is algebraically closed.*

Proof. It is enough to show that K is perfect, i.e., that for all $a \in K$, there exists $\alpha \in K$ such that $\alpha^p = a$. So let $a \in K^\times$, and let α be the unique element of $\overline{K}$ such that $\alpha^p = a$. Our task is to show that indeed $\alpha \in K$.

For this, fix an element $c \in K$ with $v(c) > 0$ and consider the sequence of polynomials $P_n(t) = t^p - c^n t - a$. Evidently $\lim_{n\to\infty} P_n(t) = t^p - a$ and the only root of $t^p - a$ in $\overline{K}$ is α. Therefore, by the continuity of the roots of a polynomial as functions of the coefficients, if for each n we choose a root α_n of P_n in $\overline{K}$, then necessarily $\alpha_n \to \alpha$. But each P_n is separable and K is separably closed, so each α_n lies in K. Moreover, since the sequence $\{\alpha_n\}_{n=1}^\infty$ is convergent in $\overline{K}$, it is Cauchy in K, but K is assumed to be complete, so therefore $\lim_{n\to\infty} \alpha_n = \alpha$ lies in K. □

Exercise 3.21 (Kaplansky-Schilling [KS]) Deduce the following strengthening of Schmidt's theorem: Let v_1 and v_2 be inequivalent nontrivial valuations on a field K. Suppose that K is complete with respect to v_1 and Henselian with respect to v_2. Then K is algebraically closed of at least continuum cardinality.

Corollary 28. *Let $(K, ||\ ||)$ be an algebraically closed normed field. Then the completion of K is algebraically closed.*

Exercise 3.22: Deduce Corollary 28 from Corollary 22 and Proposition 27.

Similarly, we may classify all multi-Henselian fields, and this is simpler in that no conditions on the cardinality intervene.

Proposition 29. *Let K be a separably closed field, and let v be a valuation on K. Then K is Henselian with respect to v.*

Proof. By definition of Henselian, we must show that if L/K is a finite degree field extension, then there is a unique valuation on L extending v. If $L = L_n \supset L_{n-1} \supset \ldots \supset L_0 = K$ is a tower of finite degree purely inseparable extensions, then if every valuation v_i on L_i extends uniquely to a valuation on L_{i+1}, then certainly the valuation $v = v_0$ on K extends uniquely to L. Therefore we may assume that L/K is purely inseparable and *primitive*, i.e., generated by a single root of a purely inseparable polynomial, i.e., $L = K[t]/(P)$, where P has only one distinct root in an algebraic closure $\overline{K}$ of K.

Now recall Theorem 2.5: if (K, v) is a valued field and L/K is a finite field extension, there is a bijective correspondence betweeen valuations on L extending v and prime ideals in the Artinian K_v-algebra $L \otimes_K K_v$. With our choice of $L = K[t]/(P(t)$, with P purely inseparable, we have $L \otimes_K K_v \cong K_v[t]/(P(t))$. But since P is purely inseparable, it has only one root in an algebraic closure, hence also in any field extension. Therefore over $K_v(t)$ we have a factorization $P = Q^e$, where Q is again irreducible, so $L \otimes_K K_v \cong K_v[t]/(Q^e)$, which is a local algebra with unique maximal ideal (Q). Therefore the extension of v to L is unique. □

Proposition 30. *Let K be a separably closed field which is* not *the algebraic closure of a finite field. Then K is multi-Henselian: indeed it is Henselian with respect to infinitely many pairwise inequivalent distinct valuations.*

Proof. By Proposition 27, K is Henselian with respect to all of its valuations. The remainder is just a rehash of some already proved valuation theory: if K is an algebraic extension of a finite field, then it admits only the trivial valuation. Otherwise, K admits at least one nontrivial valuation. Indeed, if K has characteristic 0 then it contains $\mathbb{Q}$ and hence has p-adic valuations for all p, each of which extends, by Theorem 2.1, to a valuation of K; this gives infinitely many inequivalent valuations. Otherwise K has characteristic $p > 0$ and thus contains $\mathbb{F}_p(t)$, a field which has infinitely many inequivalent valuations by Theorem 1.14. □

Remark: This is [KS, Theorem 2], except that the need to exclude the algebraic closure of a finite field is overlooked there.

Exercise 3.23: Show that in fact any multi-Henselian field is Henselian for *uncountably many* pairwise inequivalent valuations!

Exercise 3.24: Give an example of a field which is multi-Henselian but not multi-complete.

Finally, we give an application of these results.

Theorem 31. *(Continuity of Automorphisms) Let (K, v) be a field which is Henselian for a nontrivial valuation v. Suppose that* either
(i) K is not *separably closed, or*
(ii) K is complete with respect to v and is not *algebraically closed.*
Then every automorphism of K is continuous with respect to the valuation topology.

Proof. Let σ be an automorphism of K. By Exercise 2.31, σ is continuous with respect to the valuation topology iff σ is an automorphism of the valued field (K, v),

i.e., for all $x \in K$, we have $\sigma^* v = v$, where $\sigma^* v$ is the valuation $x \mapsto v(\sigma(x))$. It is easy to see that since v is Henselian, so is $\sigma^* v$ and that v is complete iff $\sigma^* v$ is complete (c.f. Exercise 2.32). Therefore if σ were *not* continuous with respect to the valuation topology, then v and $\sigma^* v$ would be inequivalent nontrivial valuations on K, i.e., K is multi-Henselian. Thus by Kaplansky-Schilling, K is separably closed. Similarly, if K is complete with respect to v, then it is multi-complete and thus, by Schmidt's theorem, algebraically closed, qed. □

This immediately implies the following result.

Corollary 32. *Let $K/\mathbb{Q}_p$ be a degree d field extension. Then $\#\operatorname{Aut}(K) \leq d$. In particular, $\mathbb{Q}_p$ is* rigid*, i.e., has no nontrivial field automorphisms.*

Note that a somewhat different proof of the rigidity of $\mathbb{Q}_p$ was sketched in Exercise 2.33. In fact, from this special case Corollary 32 easily follows, but we wished to bring this basic and important result more prominently to the reader's attention.

References

[BAII] N. Jacobson, *Basic algebra. II.* Second edition. W. H. Freeman and Company, New York, 1989.

[Cas] J.W.S. Cassels, *Rational quadratic forms.* London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[CL] J.-P. Serre, *Local fields.* Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[Clark09] P.L. Clark, *On the Hasse principle for Shimura curves.* Israel J. Math. 171 (2009), 349–365.

[Clark-CA] P.L. Clark, *Commutative Algebra*, `http://math.uga.edu/~pete/integral.pdf`

[Clark-FT] P.L. Clark, *Field Theory*, `http://math.uga.edu/~pete/FieldTheory.pdf`.

[Clark-QF] P.L. Clark, *Quadratic Forms*, `http://www.math.uga.edu/~pete/quadraticforms.pdf`.

[End] O. Endler, *Valuation theory.* To the memory of Wolfgang Krull (26 August 1899–12 April 1971). Universitext. Springer-Verlag, New York-Heidelberg, 1972.

[KS] I. Kaplansky and O. F. G. Schilling, *Some remarks on relatively complete fields.* Bull. Amer. Math. Soc. 48, (1942). 744–747.

[Lam] T.-Y. Lam, *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[Sch] F.K. Schmidt, *Mehrfach perfekte Körper.* Math. Ann. 108 (1933), no. 1, 1–25.