Introduction to Valuation Theory

Talk in the seminar on "Field Arithmetic"

Tel Aviv, 23 March 2013

The aim of this talk is to introduce the basic notions of valuation theory, starting with discrete valuation, then general valuations with emphasize on extensions of valuations to algebraic extensions and Henselizations. We give only a few proofs. Most of the statements we make will be proved in subsequent talks of the seminar.

1. The field of real numbers. Our starting point is the field $\mathbb{R}$ of real numbers equipped with the ordering relation $a < b$ defined by "there exists $x \neq 0$ such that $b - a = x^2$ ". The **absolute value** on $\mathbb{R}$ is then the function $|\ |$ defined by $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x \leq 0$. It satisfies the following conditions: BALa input, 21

(1a) $|x| \geq 0$, $|1| = 1$, and $|x| = 0$ if and only if $x = 0$.

(1b) $|xy| = |x| \cdot |y|$.

(1c) $|x + y| \leq |x| + |y|$.

The absolute value gives rise to a topology on $\mathbb{R}$ whose basic open sets are the open intervals $\{x \in \mathbb{R} \mid\ |x - a| < \varepsilon\}$ for some $a \in \mathbb{R}$ and $\varepsilon > 0$. This topology has the following properties:

(2a) $\mathbb{R}$ is **Hausdorff**: distinct points of $\mathbb{R}$ have disjoint open neighborhoods.

(2b) $\mathbb{R}$ is **locally compact**: Every $x \in \mathbb{R}$ has a compact closed neighborhood (theorem of Heine-Borel).

(2c) $\mathbb{R}$ is **complete**: Every Cauchy sequence of real numbers converges (to a unique point).

(2d) $\mathbb{R}$ is **locally connected**. Every closed interval $[a, b]$ is **connected** (i.e. $[a, b]$ is not a disjoint union of two open subsets).

(2e) $\mathbb{Q}$ is dense in $\mathbb{R}$. Thus, $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\ |$.

2. The p-adic absolute value. The field $\mathbb{Q}$ has, along with the real topology, also a p-adic topology for each prime number p. Like the real topology, the p-adic topology is defined by a **p-adic absolute value** $|\ |_p$ of $\mathbb{Q}$ defined as follows. Each nonzero $x \in \mathbb{Q}$ has a presentation $x = \frac{a}{b}p^k$, where $a, b \in \mathbb{Z}$ are not divisible by p and $k \in \mathbb{Z}$. Moreover, BALb input, 64

k is uniquely determined by x. We set $|x|_p = p^{-k}$. We also set $v_p(x) = k$ and call v_p the **p-adic valuation** of $\mathbb{Q}$. Finally we set $|0|_p = 0$ and $v_p(0) = \infty$. The p-adic absolute value satisfies the following rules:

(3a) $|x|_p$ is a non-negative real number, $|p|_p = p^{-1}$, and $|x|_p = 0$ if and only if $x = 0$.

(3b) $|xy|_p = |x|_p|y|_p$

(3c) $|x + y|_p \leq \max(|x|_p, |y|_p)$.

Note that (3a) and (3c) imply the triangle inequality $|x + y|_p \leq |x|_p + |y|_p$. In general, the triangle inequality is weaker than (3c). For example, $|p+p^2|_p = |p(1+p)|_p = p^{-1} < |p|_p + |p^2|_p$.

The properties (3) of the p-adic absolute value translate into properties of the p-adic valuation. To this end we view the symbol ∞ as bigger than every integer. Moreover, we impose the following rule: $\infty + a = \infty$ for each $a \in \mathbb{Q}$. Then:

(4a) $v_p(x)$ is an integer, $v_p(p) = 1$, and $v_p(x) = \infty$ if and only if $x = 0$.

(4b) $v_p(xy) = v_p(x) + v_p(y)$.

(4c) $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

By (4b), $v_p(1) = v_p(-1) = 0$, hence $v_p(-y) = v_p(y)$ for every $y \in \mathbb{Q}$.

A useful supplement to the rule (4) is:

(4d) If $v_p(x) \neq v_p(y)$, then $v_p(x + y) = \min(v_p(x), v_p(y))$.

Indeed, assume that $v_p(x) < v_p(y)$ but $v_p(x + y) \neq \min(v_p(x), v_p(y))$. Then, by (4c), $v_p(x + y) > \min(v_p(x), v_p(y)) = v_p(x)$. Hence,

$$v(x) = v((x + y) + (-y)) \geq \min(v(x + y), v(-y)) > v(x),$$

which is a contradiction.

The completion of $\mathbb{Q}$ with respect to the p-adic valuation is the **field of p-adic numbers** which we denote by $\hat{\mathbb{Q}}_p$ (although it is usually denoted by $\mathbb{Q}_p$). Each element x of $\hat{\mathbb{Q}}_p$ can be uniquely represented as a series $x = \sum_{i=m}^{\infty} a_i p^i$, where $m \in \mathbb{Z}$ and $0 \leq a_i \leq p-1$ for each $i \geq m$. We extend v_p to the p-adic valuation of $\hat{\mathbb{Q}}_p$ by $v_p(x) = m$ if $a_m \neq 0$. Then v_p satisfies (4) for all $x, y \in \hat{\mathbb{Q}}_p$.

The **p-adic topology** on $\hat{\mathbb{Q}}_p$ is the collection of all subsets of $\hat{\mathbb{Q}}_p$ which are unions

of **basic p-adic open sets**. Each of the latter has the form:

$$D(a,m) = \{x \in \hat{\mathbb{Q}}_p \mid \ v_p(x-a) > m\}$$

for some $a \in \hat{\mathbb{Q}}_p$ and $m \in \mathbb{Z}$.

As in the case of $\mathbb{R}$, the field $\hat{\mathbb{Q}}_p$ is Hausdorff, locally compact, complete, and $\mathbb{Q}$ is dense in $\hat{\mathbb{Q}}_p$. However, in contrast to $\mathbb{R}$, the field $\hat{\mathbb{Q}}_p$ is not locally connected. Indeed, every basic open subset of $\hat{\mathbb{Q}}_p$ is also closed.

To prove this statement consider $c \notin D(a,m)$. Then, $v_p(c-a) \leq m$ and $D(c,m) = \{x \in \hat{\mathbb{Q}}_p \mid \ v_p(x-c) > m\}$ is a p-adically open neighborhood of c in $\hat{\mathbb{Q}}_p$. Each $x \in D(c,m)$ satisfies $v_p(x-c) > m \geq v_p(c-a)$, so by (4d), $v_p(x-a) = v_p((x-c)+(c-a)) = v_p(c-a) \leq m$, hence $x \notin D(a,m)$. Therefore, $D(c,m)$ is an open neighborhood of c in $\hat{\mathbb{Q}}_p \smallsetminus D(a,m)$. It follows that $\hat{\mathbb{Q}}_p \smallsetminus D(a,m)$ is open in $\hat{\mathbb{Q}}_p$, hence $D(a,m)$ is closed in $\hat{\mathbb{Q}}_p$.

Consequently, $\hat{\mathbb{Q}}_p$ is **totally disconnected**.

Finally we recall that if an infinite series $\sum_{i=1}^{n} x_i$ of real numbers converges, then x_i tends to zero as i tends to infinity. In $\mathbb{Q}_p$ the latter condition is even sufficient for the convergence of the series. Indeed, by (4c),

$$v_p(\sum_{i=m}^{n} x_i) \geq \min(v_p(x_m), v_p(x_{m+1}), \ldots, v_p(x_n))$$

for all $m \leq n$, and we may now apply the completeness of $\hat{\mathbb{Q}}_p$. It follows that every series of the form $\sum_{i=m} a_i p^i$ with $0 \leq a_i < p-1$ converges in $\hat{\mathbb{Q}}_p$. In particular, we find that $\frac{1}{1-p} = \sum_{p=0}^{\infty} p^i$ in $\hat{\mathbb{Q}}_p$.

3. General valuations. Note that Condition (4) makes use of the ordering of the additive (abelian) group $\mathbb{Z}$. In general, an **ordered (additive) group** Γ is an additive group with a binary relation $<$, called an **ordering**, that satisfies the following rules for all $\alpha, \beta, \gamma \in \Gamma$: BALc input, 192

(5a) Either $\alpha < \beta$, or $\alpha = \beta$, or $\beta < \alpha$.

(5b) If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$.

(5c) If $\alpha < \beta$, then $\alpha + \gamma < \beta + \gamma$.

Condition (5) implies a **cancellation rule**:

(6) If $\alpha, \beta \in \Gamma$ satisfy $e\alpha < e\beta$ for some positive integer e, then $\alpha < \beta$.

As in the case of $\mathbb{Z}$, we attach a symbol ∞ to Γ and impose the following rules:

(7a) $\alpha < \infty$,

(7b) $\alpha + \infty = \infty$, and $\infty + \infty = \infty$

A **valuation** of a field K with **value group** Γ is a surjective map $v\colon K \to \Gamma \cup \{\infty\}$ that satisfies the following conditions:

(8a) $v(x) = \infty$ if and only if $x = 0$; there exists $y \in K^\times$ with $v(y) \neq 0$.

(8b) $v(xy) = v(x) + v(y)$.

(8c) $v(x + y) \geq \min(v(x), v(y))$.

The proof of (4d) in the case of v_p holds also in the general case:

(8d) If $v(x) \neq v(y)$, then $v(x + y) = \min(v(x), v(y))$.

We denote Γ by Γ_v and note that $\Gamma = v(K^\times)$. We observe that

$$O_v = \{x \in K \mid\ v(x) \geq 0\}$$

is a subring of K that we call the **valuation ring** of v. By (8b), $v(1) = 0$ and $v(x^{-1}) = -v(x)$ if $x \neq 0$. Hence, by the second part of (8a), O_v is properly contained in K. Moreover, $U_v = \{u \in K \mid\ v(u) = 0\}$ is the group $O_v^\times$ of invertible elements of O_v. It follows that $\mathfrak{m}_v = \{x \in K \mid\ v(x) > 0\}$ is the unique maximal ideal of O_v. The quotient field $\bar{K}_v = O_v/\mathfrak{m}_v$ is the **residue field** of K at v. The homomorphism $x \to x + \mathfrak{m}$ from O_v onto $\bar{K}_v$ is called the **residue map**.

For example, the valuation ring of the p-adic valuation v_p of $\hat{\mathbb{Q}}$ is the ring $\hat{\mathbb{Z}}_p$ (usually denoted by $\mathbb{Z}_p$) of **p-adic integers**. It consists of all power series $\sum_{i=0}^{\infty} a_i p^i$ with $0 \leq a_i \leq p - 1$, in particular $\frac{1}{1-p} = \sum_{i=0}^{\infty} p^i \in \hat{\mathbb{Z}}_p$. The residue field of v_p is the field $\mathbb{F}_p$ of p elements and the residue map $\hat{\mathbb{Z}}_p \to \mathbb{F}_p$ maps $\sum_{i=0}^{\infty} a_i p^i$ onto $a_0 + p\mathbb{Z}$.

Conversely, a proper subring O of K is a **valuation ring** of K if

(9) for each $x \in K^\times$ either $x \in O$ or $x^{-1} \in O$.

Now consider the multiplicative group $O^\times$ of invertible elements of O and the quotient group $K^\times/O^\times$. For each $x, y \in K^\times$ we let $x' = xO^\times$, $y' = y^\times$, and write $x' \leq y'$ if $x^{-1}y \in O$. Then (9) guaranties that $\leq$ is an ordering on (the multiplicative group)

$K^\times/O^\times$. Now we take an additive copy Γ of $K^\times/O^\times$ and let $v(x)$ be the image of x' in Γ. Then, v is a valuation of K with $O_v = O$ and $\Gamma_v = \Gamma$.

Valuations v and v' of a field K are **equivalent** if there exists an isomorphism $\varphi\colon \Gamma_v \to \Gamma_{v'}$ of valued groups such that $\varphi(v(x)) = v'(x)$ for every $x \in K^\times$. This property is equivalent to the equality $O_v = O_{v'}$.

4. Examples of Valuations. If the value group Γ_v of a valuation v of a field K is isomorphic to $\mathbb{Z}$ (as ordered groups), then v is a **discrete valuation**. For example, v_p is a discrete valuation of $\mathbb{Q}$ and of $\hat{\mathbb{Q}}_p$ for every prime number p. BALd input, 301

More generally, if R is a unique factorization domain and p is a prime element of R, we may define a discrete valuation v_p on $K = \mathrm{Quot}(R)$ as follows: Each $x \in K^\times$ can be represented as $x = \frac{a}{b}p^k$ with $a, b \in R$ not divisible by p and $k \in \mathbb{Z}$. Then $v_p(x) = k$. For example if K_0 is a field, then $K_0[X]$ is a unique factorization domain. So each irreducible polynomial p gives rise to a discrete valuation v_p of $K_0(X)$ as above. The same applies to the ring $K_0[X^{-1}]$ and the irreducible polynomial X^{-1} of that ring. The corresponding valuation of $K_0(X)$ is denoted by v_∞. In particular, $v_\infty(X) = -1$. It follows from (8d) that $v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f)$ for $f, g \in K[X]$. Moreover, one can prove that every valuation v of $K_0(X)$ which is **trivial** on K_0 (i.e. $v(a) = 0$ for each $a \in K_0^\times$) is equivalent to one of the above valuations. In general, if a valuation v of a field K is trivial on a subfield K_0, we say that v is a **valuation of** K/K_0.

A valuation v of a field K is of **rank** 1 if Γ_v is isomorphic to a subgroup of $\mathbb{R}$. For example, every discrete valuation is of rank 1. Like v_p, every rank-1 valuation has a completion $\hat{K}_{0,v}$. For example, the completion of $K_0(X)$ at the valuation defined by the irreducible polynomial X is the field $K_0((X))$ of **formal power series**.

One knows that $K_0[X, Y]$ is also a unique factorization domain. Thus, each irreducible polynomial gives rise to a discrete valuation of $K = K_0(X, Y)$. All other valuations of K which are trivial on K_0 have rank at most 2 (i.e. the value group is isomorphic to a subgroup of $\mathbb{Z} \oplus \mathbb{Z}$ with the lexikographic ordering). For example, there are infinitely many rank 2 valuations of K/K_0 such that both X and Y are mapped to 0 under the residue map.

5. Extensions of Valuations. We call a pair (K, v) a **valued field** whenever K is a field and v is a valuation of K. Another valued field (L, w) is an **extension** of (K, v) and we say that w **lies over** v, if $K \subseteq L$ and $O_w \cap K = O_v$ (so $w|_K$ is equivalent to v). In this case we also have $\mathfrak{m}_w \cap O_v = \mathfrak{m}_v$, hence the map $x + \mathfrak{m}_v \mapsto x + \mathfrak{m}_w$ defines an embedding $\bar{K}_v \to \bar{L}_w$ of the corresponding residue fields. Similarly, $O_w^\times \cap O_v = O_v^\times$, hence the map $xO_v^\times \mapsto xO_w^\times$ defines an embedding $\Gamma_v \to \Gamma_w$ of the value groups. We consider these embeddings as inclusions and call $e_{w/v} = (\Gamma_w : \Gamma_v)$ the **ramification index** and $f_{w/v} = [\bar{L}_w : \bar{K}_v]$ the **residue degree** of the valued field extension $(L, w)/(K, v)$ (or, briefly of w/v). BALe input, 358

A theorem of Chevalley guarantees that each valuation of K extends to a valuation of L.

Chevalley's theorem: *Let R be an integral domain with quotient field K and let L be a field extension of K. Let φ be a homomorphism of R into a field $\bar{K}$. Then L has a valuation w such that $R \subseteq O_w$, $\bar{L}_w$ is contained in the algebraic closure of $\bar{K}$, and the residue map $O_w \to \bar{L}_w$ extends φ. In particular, $\mathfrak{m}_w \cap R = \mathrm{Ker}(\varphi)$.*

Proposition 5.4 of [Jar91] restates the theorem in the language of "places".

Corollary: *Let (K, v) be a valued field and L a field extension of K. Then L has a valuation w that lies over v and $\bar{L}_w$ is an algebraic extension of $\bar{K}_v$.*

6. Finite Algebraic Extensions. BALf input, 403

The fundamental Inequality: *Let (K, v) be a valued field and L a finite extension of K. Then v has only finitely many inequivalent extensions $w_1, \ldots, w_r$ to L. Moreover, $\sum_{i=1}^{r} e_{w_i/v} f_{w_i/v} \leq [L : K]$.*

The fundamental inquality has at least three proofs. One of them that appears in [Bou89, p. 420, Thm. 1] uses "completions", the second one applies the notion of "defect" [EnP05]. The third one which we will hear in the next lecture substitutes the completions of Bourbaki by "Henselian closures".

The fundamental inequality becomes equality for discrete valuations in separable extensions:

THE FUNDAMENTAL EQUALITY ([EnP05]): *Let (K, v) be a discrete valued field and L a finite separable extension of K. Then v has finitely many extensions $w_1, \ldots, w_r$ to L and $\sum_{i=1}^{r} e_{w_i/v} f_{w_i/v} = [L : K]$.*

7. INTEGRAL EXTENSIONS. Let R be an integral domain with quotient field K and let L be a field extension of K. An element x of L is **integral** over K if x is a zero of a monic polynomial with coefficients in R. With other words, there exist $a_0, \ldots, a_{n-1} \in R$ such that INT input, 435

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0. \tag{10}$$

The set of all elements of L that are integral over R form a ring called the **integral closure of R in L** [Lan93, Chap. VII, Sec. 1]. If R coincides with its integral closure in K, we say that R is **integrally closed**. It is not difficult to prove that every unique factorization domain is integrally closed. For example, $\mathbb{Z}$ and all of the ring of polynomials $K_0[X_1, \ldots, X_n]$ over an arbitrary field K_0 are integrally closed. Finite extensions of $\mathbb{Q}$ are called **number fields**. The integral closure of $\mathbb{Z}$ in a number field K is referred to as the **ring of integers** of K.

The next result describes the integral closure of a valuation ring in a finite extension of its quotient field in terms of valuations. To this end we consider an integral domain R, a field extension L of R, and a valuation w of L. We say that w is **integral on** R if $w(a) \geq 0$ for all $a \in R$.

LEMMA ON VALUATIONS AND INTEGRAL ELEMENTS:

(a) *Every valuation ring R of a field K is integrally closed.*

(b) *Let R be an integral domain and L an algebraic extension of* $\mathrm{Quot}(R)$*. Then $x \in L$ is integral over R if and only if $w(x) \geq 0$ for every valuation w of L which is integral on R.*

Proof of (a): Consider an element $x \in K$ satisfying a monic equation (10). Denote the valuation that corresponds to R by v. If $x \notin R$, then $v(x^{-1}) > 0$. Multiplying (10) by x^{-n}, we get $1 = -a_{n-1}x^{-1} - \cdots - a_0 x^{-n}$. Then, $0 = v(1) \geq \min(v(a_{n-1}x^{-1}, \ldots, v(a_0 x^{-n})) > 0$, which is a contradiction. Consequently, $x \in R$, as asserted.

Proof of (b): The arguments of the proof of (a) show that if an element x of L is integral over R, then $w(x) \geq 0$ for every valuation w of L which is integral on R.

Conversely, suppose that $w(x) \geq 0$ for every valuation w which is integral on R. Assume without loss that $x \neq 0$.

If x^{-1} is not invertible in $R[x^{-1}]$, then $R[x^{-1}]$ has a prime ideal $\mathfrak{p}$ that contains x^{-1}. By Chevalley's theorem, L has a valuation w such that $\mathfrak{m}_w \cap R[x^{-1}] = \mathfrak{p}$. In particular, $w(x^{-1}) > 0$, so $w(x) < 0$, in contrast to our assumption.

It follows that $x \in R[x^{-1}]$. Hence, there exist $a_0, \ldots, a_{n-1} \in R$ such that $x = a_0 + a_1 x^{-1} + \cdots + a_{n-1} x^{1-n}$. Therefore, $x^n = a_0 x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}$, so x is integral over R. ∎

Next let L/K be a finite extension. We describe the valuation rings of L that lie over a valuation ring of K.

To this end recall that the **local ring** of an integral domain R at a prime ideal $\mathfrak{p}$ is the following subring of $\mathrm{Quot}(R)$:

$$R_{\mathfrak{p}} = \Big\{ \frac{a}{b} \,\Big|\, a \in R,\ b \in R \setminus \mathfrak{p} \Big\}.$$

This subring has a unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. If $\mathfrak{q}$ is a prime ideal of R, then $\mathfrak{q}R_{\mathfrak{p}}$ is a proper prime ideal of $R_{\mathfrak{p}}$ if and only if $\mathfrak{q} \subseteq \mathfrak{p}$. In this case, $R \cap \mathfrak{q}R_{\mathfrak{p}} = \mathfrak{q}$. Moreover, the map $\mathfrak{q} \mapsto \mathfrak{q}R_{\mathfrak{p}}$ maps the set of all prime ideals of R that are contained in $\mathfrak{p}$ bijectively onto the set $\mathrm{Spec}(R_{\mathfrak{p}})$ of all proper prime ideals of $R_{\mathfrak{p}}$.

LEMMA ([Lan58, p. 18, Thm. 4]): *Let v be a valuation of a field K, L a finite extension of K, and $w_1, \ldots, w_r$ the inequivalent valuations of L that lie over v. Denote the integral closure of O_v in L by S. For each $1 \leq i \leq r$ let $\mathfrak{p}_i = \{x \in S \mid w_i(x) > 0\}$. Then $O_{w_i} = S_{\mathfrak{p}_i}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are all of the prime ideals of S that lie over $\mathfrak{m}_v$.*

8. GALOIS EXTENSIONS. Let $(L, w)/(K, v)$ be a Galois extension of valued fields and let $\sigma \in \mathrm{Gal}(L/K)$. Then, $w' = w \circ \sigma^{-1}$ is a valuation of L that lies over v, $\sigma O_w = O_{w'}$, $\sigma \mathfrak{m}_w = \mathfrak{m}_{w'}$, and $\Gamma_w = \Gamma_{w'}$. Thus, σ induces an isomorphism $\bar{\sigma}$ of the residue fields as BALg input, 550

shown in the following commutative diagram:

$$
\begin{array}{ccccccccc}
(11) & & 0 & \longrightarrow & \mathfrak{m}_w & \longrightarrow & O_w & \longrightarrow & \bar{L}_w & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \bar{\sigma}} & & \\
 & & 0 & \longrightarrow & \mathfrak{m}_{w'} & \longrightarrow & O_{w'} & \longrightarrow & \bar{L}_{w'} & \longrightarrow & 0
\end{array}
$$

In particular, $e_{w/v} = e_{w'/v}$ and $f_{w/v} = f_{w'/v}$.

LEMMA 8.1 ([Jar91, Cor. 8.2]): *Let L/K be a Galois extension, v a valuation of K, w an extension of v to L and w' another valuation of L. Then w' lies over v if and only if there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma O_w = O_{w'}$*

It follows that if w' lies over v, then w and w' satisfy all of the assertions mentioned above. Continuing with $(L, w)/(K, v)$ as before, we define the **decomposition group** of w/v as $D_{w/v} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma O_w = O_w\}$. The **decomposition field** of w/v is the fixed field of $D_{w/v}$ in L.

LEMMA 8.2: *Let $(L, w)/(K, v)$ be a Galois extension of valued fields and let $\sigma \in D_{w/v}$. Then $w \circ \sigma = w$.*

Proof: By assumption, $\sigma O_w = O_w$, hence $O_w = \sigma^{-1} O_w$, so $O_w = O_{w\circ\sigma}$. Since each element of L lies in a finite Galois extension of K which is contained in L, we may assume that L/K is finite. By the fundamental inequality, $e = (\Gamma_w : \Gamma_v)$ is finite. Thus, for each $x \in L$ there exists $a \in K$ such that $ew(x) = w(a)$. Hence, $w(x^e a^{-1}) = 0$, so $x^e a^{-1} \in O_w^\times$. Therefore, $x^e a^{-1} \in O_{w\circ\sigma}^\times$, hence, $w(\sigma(x^e a^{-1})) = 0$, so $ew(\sigma x) = w(\sigma a) = w(a) = ew(x)$. Consequently, by (6), $w(\sigma x) = w(x)$, as asserted. ∎

It follows from Diagram (11) that if $\sigma \in D_{w/v}$, then $\bar{L}_w = \bar{L}_{w\circ\sigma^{-1}}$ and σ induces a $\bar{K}_v$-automorphism $\bar{\sigma}$ of $\bar{L}_w$.

LEMMA 8.3 ([Jar91, Prop. 8.7]): *Let $(L, w)/(K, v)$ be a Galois extension of valued fields. Denote the image of an element x of O_w by $\bar{x}$. Assume that $\bar{L}_w/\bar{K}_v$ is a separable extension. Then $\bar{L}_w/\bar{K}_v$ is a Galois extension. Moreover, the map $\sigma \mapsto \bar{\sigma}$ defined by $\bar{\sigma}\bar{x} = \overline{\sigma x}$ is a homomorphism of $D_{w/v}$ onto $\mathrm{Gal}(\bar{L}_w/\bar{K}_v)$ (that we call the* **residue map***).*

LEMMA 8.4 ([Jar91, Prop. 8.6]): *Let $(L,w)/(K,v)$ be a Galois extension of valued fields, let L_0 be the decomposition field of w/v, and denote the restriction of w to L_0 by w_0. Then w_0/v is an* **immediate extension**, *that is $\bar{L}_{0,w_0} = \bar{K}_v$ and $\Gamma_{w_0} = \Gamma_v$. Moreover, w is the unique valuation (up to equivalence) of L that lies over w_0.*

The latter assertion is a consequence of Lemma 8.1.

9. HENSELIAN FIELDS. Kurt Hensel proved that every polynomial in $\hat{\mathbb{Z}}_p[X]$ that satisfies a certain condition (appearing in (a) of the following lemma) has a root in $\hat{\mathbb{Z}}_p$. Fields that has that property are called "Henselian fields". BALh input, 652

LEMMA AND DEFINITION OF HENSELIAN FIELDS ([Jar91, Prop.-Def. 11.1]): *We say that a valued field (K,v) is* **Henselian** *if it satisfies one of the following equivalent conditions:*

(a) *(Hensel) For every $f \in O_v[X]$ and $a \in O_v$ satisfying $v(f(a)) > 0$ and $v(f'(a)) = 0$ (equivalently, $\overline{f(a)} = 0$ and $\overline{f'(a)} \neq 0$) there exists a unique $x \in O_v$ such that $f(x) = 0$ and $v(x-a) > 0$.*

(b) *(Uniqueness of extensions) The valuation v has a unique extension (up to equivalence) to each algebraic extension.*

(c) *(Hensel-Rychlik) For every monic polynomial $f \in O_v[X]$, every $a \in O_v$, and every positive $\gamma \in \Gamma_v$ satisfying $v(f(a)) > 2v(f'(a)) + \gamma$ there exists $x \in O$ such that $f(x) = 0$ and $v(x-a) > v(f'(a)) + \gamma$.*

Examples:

(a) Every complete discrete valuation ring is Henselian. In particular, $\hat{\mathbb{Q}}_p$ is Henselian for each prime number p (This is Hensel's original Lemma). Similarly $K_0((X))$ is Henselian for every field K_0.

(b) Let p be a prime number, n a positive integer with $p \nmid n$, and $a \in \hat{\mathbb{Z}}_p$. Suppose there exists $b \in \hat{\mathbb{Z}}_p$ such that $\bar{b} \neq 0$ and $\bar{b}^n = \bar{a}$. Then the polynomial $f(X) = X^n - a$ satisfies $\overline{f(b)} = 0$ but $\overline{f'(b)} = \overline{nb^{n-1}} \neq 0$. Hence, there exists $x \in \hat{\mathbb{Z}}_p$ such that $f(x) = 0$, so $x^n = a$.

(c) Let p be an odd prime and k a divisor of $p-1$. Then $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, so $\mathbb{F}_p^\times$ has an element ζ of order k. Since the derivative of $X^k - 1$ is kX^{k-1},

this implies that ζ can be lifted to a root of unity $z \in \hat{\mathbb{Z}}_p$ of order k.

(d) Suppose $a \in \hat{\mathbb{Z}}_2$ satisfies $a \equiv 1 \mod 8$. Consider the polynomial $f(X) = X^2 - a$ and its derivative $f'(X) = 2X$. Then $v_2(f(1)) = v_2(1-a) \geq v_2(8) = 3 > 2v_2(2 \cdot 1) = 2v_2(f'(1))$. Hence, by Hensel-Rychlik, a is a square in $\mathbb{Z}_2$. ∎

LEMMA: *Let (K', v') be a separable algebraic extension of a valued field (K, v). Then the following statement are equivalent.*

(a) *(K', v') is Henselian and for every Henselian extension (L, w) of (K, v) there exists a (K, v)-**embedding** φ: $(K', v') \to (L, w)$. This means that φ: $K' \to L$ is a K-embedding of fields such that $w(\varphi(x)) = v'(x)$ for each $x \in K'$.*

(b) *The valuation v has an extension v_s to the separable closure K_s of K such that K' is the decomposition field of v_s/v.*

Whenever the equivalent conditions of the lemma are satisfied we say that (K', v') is a **Henselian closure** (sometimes also called a **Henselization**) of (K, v).

It follows from Condition (b) and from Lemma 8.4 that (K', v') is unique up to a K-isomorphism. Moreover, the extension $(K', v')/(K, v)$ is immediate.

If (K, v) is discrete, then (K', v') is the separable algebraic part of its completion $(\hat{K}, \hat{v})$. That is, if we embed K_s into the algebraic closure of $\hat{K}$, then $(K_s \cap \hat{K}, \hat{v}|_{K_s \cap \hat{K}})$ is a Henselian closure of (K, v). In general this is not the case.

References

[Bou89] N. Bourbaki, *Commutative Algebra, Chapters 1–7,* Springer, Berlin, 1989.

[EnP05] *A. J. Engler and A. Prestel,* Valued fields, Springer 2005, Berlin, Heidelberg.

[Jar91] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field,* in "Generators and Relations in Groups and Geometries" (A. Barlotti et al., eds), NATO ASI Series C **333**, 343–405, Kluwer, Dordrecht, 1991.

[Lan58] S. Lang, *Introduction to Algebraic Geometry,* Interscience Publishers, New York, 1958.

[Lan93] S. Lang, *Algebra, Third Edition,* Addison-Wesley, Reading, 1993.

23 March 2013