Henselian Local Rings: Around a Work in Progress

Mariemi Alonso[1], Henri Lombardi[2], Hervé Perdry[3]

[1] Universidad Complutense de Madrid, Facultad de Ciencias Matemáticas,
Departamento de Algebra.
m_alonso@mat.ucm.es
[2] Université de Franche-Comté, U. F. R. des Sciences et Techniques,
Département de Mathématiques pures et appliqués.
henri.lombardi@univ-fcomte.fr
[3] Università di Pisa, Dipartimento di Matematica L. Tonelli.
perdry@mail.dm.unipi.it

Abstract. An introduction to the theme of local rings and Henselian local rings is given through numerous examples. We outline an elementary and effective construction of the Henselization of a local ring and an effective proof of about a classical result in Henselian local rings. This paper anounces a joint work of the three authors.

Keywords. Local rings, Henselian local rings.

Introduction

This paper gives an short insight of a work in progress [1] on a constructive and elementary treatment of the theory of local rings. We will sketch here the construction of the Henselization of a local ring. A similar construction for valued fields can be found in [3], [4], [5].

An excellent reference for the topic of Henselian local rings is the book by Jean–Pierre Lafon, [2], which we used a lot in our work.

1 Rings and Local Rings

Here we give some basic definitions. In the whole paper, all the rings are commutative with a unity.

1.1 Radicals

Definition 1. *The* Jacobson radical *of a ring A is*

$$\mathcal{J}_A = \{x \in A \,:\, \forall y \in A \ 1 + x \cdot y \in A^\times\}.$$

In classical mathematics, $\mathcal{J}_A$ is the intersection of all maximal ideals of A.

Dagstuhl Seminar Proceedings 05021
Mathematics, Algorithms, Proofs
http://drops.dagstuhl.de/opus/volltexte/2006/437

Definition 2. *A ring A is* local *if, and only if,*

$$\forall x \in A,\ x \in A^\times \text{ or } (1+x) \in A^\times.$$

We have the following classical result:

Lemma 1. *If A is a local ring, then $\mathcal{J}_A = A \setminus A^\times$, and it is the unique maximal ideal of A. We denote it by $\mathfrak{m}_A$ or simply by $\mathfrak{m}$.*

Definition 3. *The* residue field *of local ring A with maximal ideal $\mathfrak{m}$ is $\mathbf{k} = A/\mathfrak{m}$. If $\mathbf{k}$ is* discrete *(ie we can decide effectively whether $x \in \mathbf{k}$ is zero or not, or equivalently if some $x \in A$ is in $\mathfrak{m}$ or not), A will be called* residually discrete*.*

The field $\mathbb{R}$ of real number is not a discrete field, but it verifies $\forall x \in \mathbb{R}, x \in \mathbb{R}^\times$ or $1 + x \in \mathbb{R}^\times$. Now the ring A defined by $A = S^{-1}\mathbb{R}[T]$, where S is the set of polynomials g with $g(0) \in \mathbb{R}^\times$, is indeed a local ring: the statement $\forall x \in A,\ x \in A^\times$ or $(1+x) \in A^\times$ holds. The residue field of A is $\mathbb{R}$, and the quotient map $A \longrightarrow \mathbb{R}$ is given by $f/g \mapsto f(0)/g(0)$. This provides an example of local ring A which is not residually discrete.

In this article, from now on, we are going to deal with residually discrete local rings.

1.2 Examples of local rings

Our first example is a recipe to build a local ring from any ring with a prime ideal.

1. Localization in a prime ideal Let R be a commutative ring, and $\mathfrak{P}$ a prime ideal in R. Then $S = R \setminus \mathfrak{P}$ is a multiplicative part of R: if $x, y \in S$, then $x \cdot y \in S$.

We fit the set $R \times S$ with the following laws:

$$\begin{array}{rcl} (r,s) + (r',s') & = & (rs' + r's, ss') \\ (r,s) \times (r',s') & = & (rr', ss') \\ (r,s) \sim (r',s') & \Leftrightarrow & \exists s'' \ :\ (rs' - r's)s'' = 0 \end{array}$$

The relation $\sim$ is an equivalence relation, compatible with the two laws $+$ and $\times$; the quotient $R \times S/\sim$ fitted with the corresponding quotient laws is a local ring, denoted by $R_\mathfrak{P}$, the *localization of R in $\mathfrak{P}$*.

There is a canonical map from R to $R_\mathfrak{P}$, given by $x \in R \mapsto \overline{(x,1)} \in R_\mathfrak{P}$ (where $\overline{(r,s)}$ is the class of (r,s) modulo $\sim$). The maximal ideal of $R_\mathfrak{P}$ is the image of $\mathfrak{P}$ under this map.

In the special case where R is an domain and F is its fraction field, then $R_\mathfrak{P}$ is a subring of F:

$$R_\mathfrak{P} = S^{-1}R = \left\{ \frac{r}{s} \ :\ r \in R, s \notin \mathfrak{P} \right\}.$$

Now we use the recipe to give various examples.

2. Example Let $p \in \mathbb{Z}$ be a prime number. The localization of $\mathbb{Z}$ in $\langle p \rangle$, denoted by $\mathbb{Z}_{(p)}$, is the ring

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \ : \ b \not\equiv 0 \text{ modulo } p \right\}$$

of elements of $\mathbb{Q}$ which are "defined modulo p". The maximum ideal of $\mathbb{Z}_{(p)}$ is the ideal of the fractions a/b with $b \not\equiv 0$ modulo p and $a \equiv 0$ modulo b, the residue field is $\mathbb{F}_p = \mathbb{Z}/p \cdot \mathbb{Z}$, and the quotient map $\mathbb{Z}_{(p)} \longrightarrow \mathbb{F}_p$ is the evaluation modulo p.

3. Other example Let $\mathfrak{P}$ the ideal of $\mathbb{Q}[X]$ generated by X, $\mathfrak{P} = \langle X \rangle$. The localization of $\mathbb{Q}[X]$ in $\mathfrak{P}$ is the ring

$$A = \mathbb{Q}[X]_{\mathfrak{P}} = \left\{ \frac{f}{g} \ : \ g(0) \neq 0 \right\} \subset \mathbb{Q}(X).$$

It is a local ring (and even a valuation ring), with maximal ideal

$$\mathfrak{m} = \left\{ \frac{f}{g} \ : \ f(0) = 0 \right\}.$$

The residue field of A is $\mathbb{Q}$, and the quotient map $A \longrightarrow \mathbb{Q} = A/\mathfrak{m}$ is given by the evaluation in $X = 0$.

4. Power Series The ring of power series $\mathbb{Q}[[X]]$ is the ring of formal series

$$Q[[X]] = \{a_0 + a_1 X + a_2 \cdot X^2 + \cdots \ : \ k \in \mathbb{Z}, \ \forall i, \ a_i \in \mathbb{Q}\}$$

with the classical and natural addition and multiplication laws on it. It is a local ring; its maximal ideal is generated by X: it is the set of series $\sum a_i \cdot X^i$ with constant term $a_0 = 0$. Its residue field is $\mathbb{Q}$ and the quotient map $\mathbb{Q}[[X]] \longrightarrow \mathbb{Q}$ is the evaluation in $X = 0$.

There is a natural injection $A = \mathbb{Q}[X]_{\langle X \rangle} \longrightarrow \mathbb{Q}[[X]]$, which is a morphism of local rings (it sends the maximal ideal of A in the maximal ideal of $\mathbb{Q}[[X]]$).

Remark We are not being very fair with these examples. The experienced reader will remark that these are very special local rings, namely *valuation rings*. In these rings, given two element x or y, either x divides y or y divides x.

5. An example with two variables Let A be the ring $\mathbb{Q}[X, Y]$ localized in the prime ideal $\langle X, Y \rangle$. The A is a local ring but is not a valuation ring. Its residue field is $\mathbb{Q}$

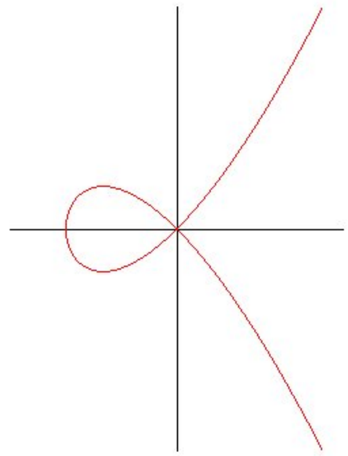
Very similarly to the ring $A = Q[X]_{\langle X \rangle}$ of example 3, this ring can be embedded in the bigger local ring $Q[[X, Y]]$, the ring of formal series in two variables.

6. An example from algebraic geometry Let $f(X, Y) \in Q[X, Y]$, with $f(0, 0) = 0$. Let $R = Q[X, Y]/\langle f \rangle$, the ring of polynomial functions on the curve $f(X, Y) = 0$. Let $\mathfrak{P}$ be the ideal of R generated by x and y (mod f). It is the prime ideal of functions which are 0 on the point $(0, 0)$.

The local ring $A = R_{\mathfrak{P}}$ is the ring of rational functions on the curve which are defined on the point $(0, 0)$. The residue field of A is $\mathbb{Q}$, and the quotient map $A \longrightarrow \mathbb{Q}$ is given by the evaluation in $(0, 0)$.

This local ring reflects local properties of the curve at the point $(0, 0)$ (one may localize in an other point). One very well-known property is that this local ring is a valuation ring if, and only if, the point $(0, 0)$ is regular.

This gives a wide class of local rings which are not valuation rings. If we consider for example the singular cubic $Y^2 = X^3 + X^2$ drawn here, which is singular in $(0, 0)$, the ring A constructed as above is a local ring which is not a valuation ring.



2 Henselian Local Rings

2.1 Definition and examples

Definition 4. *Let A be a local ring with maximal ideal $\mathfrak{m}$. We say that A is* Henselian *if all monic polynomial $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in A[X]$ with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$ has a root in $\mathfrak{m}$.*

This property is known under the name of *Hensel's Lemma*: a Henselian local ring is a local ring in which Hensel's Lemma holds.

It is easy to show that if $f(X) = X^n + \cdots + a_1 \cdot X + a_0$ with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$ has a root in $\mathfrak{m}$, then this root is unique: let $\alpha \in \mathfrak{m}$ be such a root; write $f(X) = g(X) \cdot (X - \alpha)$ with $g(X) = X^{n-1} + \cdots + b_1 \cdot X + b_0 \in A[X]$, and $b_0 - \alpha \cdot b_1 = a_1 \in A^\times$, so that $b_0 \in A^\times$. If $\beta \in \mathfrak{m}$, then $g(\beta) \in A^\times$, and $f(\beta) = 0 \Rightarrow \beta = \alpha$.

Examples The ring $A = Q[X]_{\langle X \rangle}$ is not Henselian, but the ring $Q[[X]]$, which is a complete discrete valuation ring, is Henselian.

More precisely, $Q[[X]]$ is complete for the absolute value $|a| = 2^{-v(a)}$ where $v\left(\sum a_i \cdot X^i\right) = \min\{i \,:\, a_i \neq 0\}$; if $f(X)$ verifies the condition of the definition, it is easy to verify that the sequence defined by $u_0 = 0$ and $u_{n+1} = u_n - f(u_n)/f'(u_n)$ is Cauchy and converges to an $\alpha \in \mathfrak{m}$ which is a root of f.

2.2 A simple property of Henselian local rings

In this section, A will be a Henselian residually discrete local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k}$. We denote by $a \in A \mapsto \overline{a} \in \mathbf{k}$ the quotient map, and extend it to a map $A[X] \longrightarrow k[X]$ by setting $\overline{\sum_i a_i \cdot X^i} = \sum \overline{a_i} \cdot X^i$.

We are going to show that a polynomial $f(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0$ with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$ has a (unique) root in $\mathfrak{m}$: in the definition 4, one may drop the hypothesis "f is monic". It seems clear that this kind of result should be the consequence of some variable change; and it is indeed the case — but it seems that this variable change is absent from the classical literature, where this result is derived from a general result of structure of étale algebras on a Henselian local ring.

Here is the the change of variable we propose. The proof is elementary, nevertheless it is a bit tedious.

Lemma 2. *Let $f(X) = a_n \cdot X_n + \cdots + a_1 \cdot X + a_0$, with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$. There exists a monic polynomial $g(X) \in A[X]$, $g(X) = X^n + \cdots + b_1 \cdot X + b_0$, with $b_1 \in A^\times$ and $b_0 \in \mathfrak{m}$, such that the following equality holds in $A(X)$:*

$$-a_0 \cdot g(X) = (X+1)^n \cdot f\left(\frac{-a_0 \cdot a_1^{-1}}{X+1}\right).$$

Proof. Let $h(X) = (X+1)^n \cdot f\left(\frac{-a_0 \cdot a_1^{-1}}{X+1}\right) \in A(X)$. It is easy to check that $h(X)$ is in fact a polynomial of degree n. We write $h(X) = c_n \cdot X^n + \cdots + c_1 \cdot X + c_0$.

We have

$$c_{n-k} = a_0 \cdot \left(\binom{n}{k} + \sum_{j=1}^{k} (-1)^j \cdot a_j \cdot a_0^{j-1} \cdot a_1^{-j} \cdot \binom{n}{j}\right) = a_0 \cdot b_{n-k},$$

where b_{n-k} is in A. Of course we let $g(X) = \sum_i b_i \cdot X^i$, and the desired equality is verified.

Now it is easy to check that $c_n = a_0$, so that $b_n = 1$. We have $c_0 = h(0)$, hence

$$c_0 = f\left(-\frac{a_0}{a_1}\right) = a_0^2 \cdot \left(a_n \cdot \left(\frac{a_0}{a_1}\right)^{n-2} + a_{n-1} \cdot \left(\frac{a_0}{a_1}\right)^{n-3} + \cdots + a_2\right) = a_0^2 \cdot u,$$

with $u \in A$, so that $b_0 = a_0 \cdot u \in \mathfrak{m}$.

Writing

$$h'(x) = n \cdot (X+1)^{n-1} f\left(\frac{-a_0 \cdot a_1^{-1}}{X+1}\right) + a_0 \cdot a_1^{-1} \cdot (X+1)^{n-2} f'\left(\frac{-a_0 \cdot a_1^{-1}}{X+1}\right),$$

we get $c_1 = h'(0) = n \cdot a_0^2 \cdot u + a_0 \cdot a_1^{-1} \cdot f'(a_0 \cdot a_1^{-1})$. We have $f'(a_0 \cdot a_1^{-1}) - a_1 \in \mathfrak{m}$, so that $b_1 = n \cdot a_0 \cdot u + (1 + \mu)$ with $\mu \in \mathfrak{m}$, and $b_1 \in A^\times$.

It is now easy to conclude.

Proposition 1 (Hensel's Lemma II). *Let $f(X) = a_n \cdot X_n + \cdots + a_1 \cdot X + a_0$, with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$. Then f has a (unique) root in $\mathfrak{m}$.*

Proof. Let $g(X)$ be the polynomial associated to f by the previous lemma, and $\alpha \in \mathfrak{m}$ its root. Then $(1+\alpha) \in A^{\times}$; we put $\beta = \frac{-a_0 \cdot a_1^{-1}}{\alpha+1}$, and we have $-a_0 \cdot g(\alpha) = (\alpha+1)^n \cdot f(\beta)$, so that $f(\beta) = 0$.

And the proof of the following proposition is very easy; it is left to the reader.

Proposition 2. *Let $f(X) = a_n \cdot X_n + \cdots + a_0 \in A[X]$ such that $\overline{f}(X) \in \mathbf{k}[X]$ has a simple root $a \in \mathbf{k}$. Then there exists a (unique) root $\alpha \in A$ of f, such that $\overline{\alpha} = a$.*

3 Henselization of a local ring

3.1 The Henselization; some examples

Remember the example of the non-Henselian ring $A = Q[X]_{\langle X \rangle}$ embedded in the Henselian local ring $Q[[X]]$; let B be the ring of elements of $Q[[X]]$ which are root of a polynomial with coefficients in A.

It can be checked that B is a Henselian local ring, and moreover that if C is a Henselian local ring and $\phi : A \longrightarrow C$ is a morphism of local rings (ie, it sends the maximal ideal of A in the maximal ideal of C), then there exists a unique morphism of local rings $\phi : B \longrightarrow C$ such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, hook] & C \\ B \arrow[ur, "\psi"'] & \end{tikzcd}$$

In other words, ϕ, which is defined on A, can be extended to the whole ring B. We say that B is a Henselization of A.

More generally, this property defines the Henselization of any local ring A; a consequence is that the Henselization of A is unique up to *unique* isomorphism.

An other example Now turn to our example from algebraic geometry: let R be the ring $Q[X,Y]/\left\langle X^3 + X^2 - Y^2 \right\rangle = Q[x,y]$ (x and y are the class of X and Y modulo $X^3 + X^2 - Y^2$) and $A = R_{\langle x,y \rangle}$ be its localization in $(0,0)$. It is a local ring which is not a valuation ring (this reflects the fact that $(0,0)$ is a singular point of the cubic).

The Henselization reflects other properties of the curve in $(0,0)$. Locally, this curve looks like the cross of two lines; nevertheless A is not isomorphic to $B = (Q[U,V]/\langle UV \rangle)_{\langle u,v \rangle}$, the local ring of the curve $UV = 0$ in $(0,0)$. But we have a good surprise: its Henselization A^h its isomorphic to B^h (which can be seen as a subring of $Q[[u,v]]$, similarly to what happens in the previous example). The Henselization "separates" the two branches. We are going to sketch the construction of homomorphism between these two rings.

Let $\alpha \in \mathfrak{m}_{A^h} \subset A^h$ be the root of $T^2 + 2 \cdot T - x$, whose existence is predicted by Hensel's Lemma. Hence $1+\alpha$ is a unit, and $(1+\alpha)^2 = 1 + x$.

Let $\phi_0 : B \longrightarrow A^h$ the morphism defined by

$$\begin{array}{rrcl} \phi_0 : & B & \longrightarrow & A^h \\ & u & \longmapsto & y + x \cdot (1+\alpha) \\ & v & \longmapsto & y - x \cdot (1+\alpha) \end{array}$$

One can check that ϕ_0 is a well defined morphism of local rings; note in particular that $\phi_0(u) \cdot \phi_0(v) = y^2 - x^2(1+x) = 0 = \phi_0(uv)$, which is a key point. Now ϕ_0 can be extended to a morphism $\phi : B^h \longrightarrow A^h$.

We are going to define the inverse morphism. Let $\beta \in \mathfrak{m}_{B^h}$ the root of $(u-v) \cdot T^3 + (3 \cdot (u-v) + 2) \cdot T^2 + (3 \cdot (u-v) + 4) \cdot T + (u-v)$ whose existence is predicted by Hensel's Lemma (the non-monic case); we define $\psi_0 : A \longrightarrow B^h$ by

$$\begin{array}{rrcl} \psi_0 : & A & \longrightarrow & B^h \\ & x & \longmapsto & (u-v) \cdot (1+\beta)/2 \\ & y & \longmapsto & (u+v)/2 \end{array}$$

Note again that $\psi_0(x)^3 + \psi_0(x)^2 = \psi_0(y)^2$, which is an important point to show that the application is well defined (this time the verification is a bit longer, but using a lot $uv = 0$ this can be done in a pretty reasonable time) (of course the equation defining β was build from $\left[\frac{1}{2}(u-v) \cdot (1+T)\right]^3 + \left[\frac{1}{2}(u-v) \cdot (1+T)\right]^2 = \frac{1}{4}(u^2+v^2)$).

Now ψ_0 can be extended to a morphism $\psi : A^h \longrightarrow B^h$. Checking that ψ and ϕ are inverse of each other is again a tedious but easy computation.

3.2 Construction of the Henselization

In this section, A is again a residually discrete local ring with maximal ideal $\mathfrak{m}$. We give only a sketch of the construction.

Definition 5. *Let $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in A[X]$ a monic polynomial with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$. Then we denote by A_f the ring defined as follows: if $B = A[x] = A[X]/\langle f(X) \rangle$ (where x is the class of X in the quotient ring), let $S \subseteq B$ be the multiplicative part of B defined by*

$$S = \{g(x) \in B \, : \, g(X) \in A[X], \; g(0) \in A^\times\};$$

then A_f is B localized in S, that is $A_f = S^{-1} \cdot B$.

We fix a polynomial $f(X) \in A[X]$ such as in the above definition.

Lemma 3. *The canonical map $A \longrightarrow A_f$ is an injection. The ring A_f is a residually discrete local ring. Its maximal ideal is $\mathfrak{m} \cdot A_f$.*

Proof. See [1].

As a consequence, we can identify A with its image in A_f, and write $A \subseteq A_f$. The elements of A_f can be written formally as fractions $r(x)/s(x)$ with $r, s \in A[X]$ and $s(0) \in A^\times$.

Lemma 4. *Let $B, \mathfrak{m}_B$ be a local ring and $\phi : A \longrightarrow B$ a morphism of local rings (ie $\phi(\mathfrak{m}) \subseteq \mathfrak{m}_B$). Let $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in A[X]$ be a monic polynomial with $a_1 \in A^\times$ and $a_0 \in \mathfrak{m}$.*

If $\phi(f) = X^n + \cdots + \phi(a_1) \cdot X + \phi(a_0) \in B[X]$ has a root μ in $\mathfrak{m}_B$, then there exists a unique morphism of local rings $\psi : A_f \longrightarrow B$ such that the following diagram commutes:

$$\begin{tikzcd} A, \mathfrak{m} \arrow[r, "\phi"] \arrow[d, hook] & B, \mathfrak{m}_B \\ A_f, \mathfrak{m} \cdot A_f \arrow[ur, "\psi"'] & \end{tikzcd}$$

The morphism ψ sends the root $x \in \mathfrak{m} \cdot A_f$ on μ.

Proof. The proof is easy.

We now define an inductive system. Let $\mathcal{S}$ be the smallest family of local rings $(B, \mathfrak{m} \cdot B)$ such that
(1) $(A, \mathfrak{m}) \in \mathcal{S}$;
(2) if $(B, \mathfrak{m}_B) \in \mathcal{S}$, $f(X) = X^n + \cdots + a_1 \cdot X + a_0 \in B[X]$ with $a_1 \in B^\times$ and $a_0 \in \mathfrak{m}_B$, then $B_f, m_B \cdot B_f$ is in $\mathcal{S}$.

It is easy to see that $\mathcal{S}$ is an inductive system. The ring A is canonically embedded in each local ring $(B, \mathfrak{m}_B)$ in $\mathcal{S}$, and $\mathfrak{m}_B = \mathfrak{m} \cdot B$.

Now we define the Henselization of A by

$$A^h = \varinjlim_{B \in \mathcal{S}} B.$$

We have the following theorem.

Theorem 1. *The ring A^h is a Henselian local ring with maximal ideal $\mathfrak{m} \cdot A_h$. If $(B, \mathfrak{m}_B)$ is a Henselian local ring and $\phi : A \longrightarrow B$ a morphism of local rings, there exists a unique morphism of local ring ψ such that the following diagram commutes:*

$$\begin{tikzcd} A, \mathfrak{m} \arrow[r, "\phi"] \arrow[d, hook] & B, \mathfrak{m}_B \\ A^h, \mathfrak{m} \cdot A^h \arrow[ur, "\psi"'] & \end{tikzcd}$$

Proof. The proof is easy, by induction on the family $\mathcal{S}$.

References

1. Maria Emiliana Alonso, Henri Lombardi, Hervé Perdry. *Elementary Theory of Henselian Local Rings.* Draft.
2. Jean-Pierre Lafon, *Algèbre Locale*, 2002 Hermann (Paris).
3. Franz-Viktor Kuhlmann et Henri Lombardi. Construction du henslisé d'un corps valué. In *Journal of Algebra,* vol. 228 (2000), pages 624–632.
4. Hervé Perdry. *Aspects constructifs de la théorie des corps valués.* Thèse doctorale. Université de Franche-Comté, Besançon, 2001.
5. Hervé Perdry. Henselian Valued Fields: A Constructive Point of View. Submitted Paper.