A proof of Greenberg's Theorem using ultrapowers

Margarete Ketelsen

Technische Universität Dresden

ALGAR 2021
19 August 2021

Notation

Let K be a field and

$$v : K^\times \to \Gamma$$

a valuation on K. (Γ can be any ordered abelian group.)
We write

- $\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$ for the valuation ring.
- $\mathfrak{m}_v = \{x \in K : v(x) > 0\}$ for the maximal ideal.
- $\Gamma_v = vK = v(K^\times)$ for the value group.
- $Kv = \mathcal{O}_v/\mathfrak{m}_v$ for the residue field.

We write (K, v) or (K, v, Γ_v) for the valued field.

Ershov's Generalization of Greenberg's Theorem

Theorem (Ershov 1967, Proposition 3.1.7 in [2])

Let (K, v) be a henselian and defectless valued field and let $f_1, ..., f_m \in \mathcal{O}_v[X_1, \ldots, X_n]$ polynomials, such that for every $\gamma \in \Gamma_v$ there are $x_1, \ldots, x_n \in \mathcal{O}_v$ with

$$v(f_i(x_1, \ldots, x_n)) > \gamma \text{ for } i = 1, \ldots, m.$$

Then there exist $y_1, \ldots, y_n \in \mathcal{O}_v$ with

$$f_i(y_1, \ldots, y_n) = 0 \text{ for } i = 1, \ldots, m.$$

Henselian and Defectless

Remark

- "henselian" means that the valuation extends uniquely to every algebraic extension. Or equivalently, (some variant of) Hensel's Lemma holds.
- "defectless" means that there is equality in the fundamental inequality for any finite extension.
- henselian and defectless $\implies [L:K] = e(w|v)f(w|v) = (wL:vK)[Lw:Kv]$, for any finite field extension L of K, where w is the unique prolongation of v to K.
- Complete discretely valued fields are henselian and defectless.
- The valuation v does not need to be discrete. The proof also works for positive characteristic.

The Model Theory in the Proof

For the proof we will need an extension (K^*, v^*) of (K, v) that satisfies:

1. (K^*, v^*) is again henselian.
2. If $\{f_1, ..., f_m\}$ has a zero in $\mathcal{O}_{v^*}$, then it already has a zero in $\mathcal{O}_v$.
3. There is $\gamma_0 \in \Gamma_{v^*}$ with $\gamma_0 \gg \Gamma_v$, i.e. $\gamma_0 > \gamma$ for every $\gamma \in \Gamma_v$.
   There is some $\underline{x}^* \in (K^*)^n$ with $v^*(f_i(\underline{x}^*)) > \gamma_0$.
4. $K^* v^* | Kv$ is separable.
5. Γ_{v^*}/Γ_v is torsion-free.

We will construct this extension via an ultrapower construction.

Ultrapowers

Ultrafilters

Let I be an infinite set.

Definition

A set $\mathcal{F} \subseteq \mathcal{P}(I)$ is called *filter* if

1. $\emptyset \notin \mathcal{F}$
2. $U \in \mathcal{F}, V \supseteq U \implies V \in \mathcal{F}$
3. $U, V \in \mathcal{F} \implies U \cap V \in \mathcal{F}$

for any $U, V \in \mathcal{P}(I)$.
In addition, we call $\mathcal{F}$ an *ultrafilter* if for any $U \in \mathcal{P}(I)$

4. $U \in \mathcal{F}$ or $I \setminus U \in \mathcal{F}$

holds.

Remark

The ultrafilters are exactly the maximal filters (with respect to inclusion).

Example

- $\mathcal{F}_{\{a\}} := \{A \subset I : a \in A\}$, the *principal filter* is an ultrafilter for $a \in I$.
- $\mathcal{F}_0 := \{A \subseteq I : I \setminus A \text{ is finite.}\}$, the *Fréchet filter* is a filter, bot not an ultrafilter.

Lemma

Every filter is contained in an ultrafilter

Proof. Zorn's Lemma.

Ultrapowers

of Valued Fields

Let (K, v, Γ). We now consider the set

$$K^I = \prod_{i \in I} K = \{(a_i)_{i \in I} : a_i \in K\}$$

of sequences in K.
Given an ultrafilter $\mathcal{F}$ we have the following equivalence relation on K^I:

$$(a_i)_{i \in I} \sim (b_i)_{i \in I} :\Longleftrightarrow \{i \in I : a_i = b_i\} \in \mathcal{F}$$

and we write $[a]$ for the equivalence class of $a \in K^I$.

Ultrapowers

of Valued Fields

Now, the *ultrapower* of K is given by

$$K^* := K^I/\mathcal{F} := K^I/\sim := \left\{[a] : a \in K^I\right\}$$

and we define addition and multiplication on K^* componentwise as follows

$$[(a_i)_i] + [(b_i)_i] := [(a_i + b_i)_i]$$

$$[(a_i)_i] \cdot [(b_i)_i] := [(a_i \cdot b_i)_i]\,.$$

Addition and multiplication are well-defined and K^* is again a field. (easy exercise)

Ultrapowers
of Valued Fields

We repeat a similar construction for the value group Γ and get its ultrapower

$$\Gamma^* = \Gamma^I/\mathcal{F},$$

and again Γ^* is an ordered abelian group by

$$[(\gamma_i)_i] + [(\delta_i)_i] := [(\gamma_i + \delta_i)_i]$$

$$[(\gamma_i)_i] \leq [(\delta_i)_i] :\Longleftrightarrow \{i \in I : \gamma_i \leq \delta_i\} \in \mathcal{F}$$

Now we define a valuation $v^*\colon K^* \to \Gamma^* \cup \{\infty^*\}$.

$$v^*([(a_i)_i]) := [(v(a_i))_i]$$

Definition (diagonal embedding)

$$\iota\colon K \to K^*, a \mapsto [(a)_i]$$

$$\iota\colon \Gamma \to \Gamma^*, \gamma \mapsto [(\gamma)_i]$$

For $a \in K$, we have

$$v^*(\iota(a)) = v^*([(a)_i]) = [(v(a))_i] = \iota(v(a)).$$

Thus v^* is a prolongation of the valuation v of K to K^*.
In the following, we will say that $K \subseteq K^*$ and that $(K, v) \leq (K^*, v^*)$ is an extension of valued fields.

Łoś's Theorem

Theorem

In (K, v) and in (K^*, v^*) the same formulas with no free variables and with parameters in K hold.

Example (formulas with parameters in K)

- $\exists X (f(X) = 0)$ for some $f \in K[X]$, i.e. f has a zero. The coefficients are parameters in K.
- $\forall a_0, \ldots, a_{n-2} \exists X ((v(a_0) > 0 \wedge \ldots \wedge v(a_{n-2}) > 0) \rightarrow X^n + X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0 = 0)$, i.e. every polynomial $X^n + X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0$ with $a_0, \ldots, a_{n-2}$ in the maximal ideal has a zero, this is a variant of Hensel's Lemma.

Non-examples:

- $\exists X (f(X) = 0)$ with $f \in K^*[X] \setminus K[X]$. (Parameters are not in K.)
- $\forall X \exists n \in \mathbb{N} : n > v(X)$, i.e. the value group is archimedean ordered. (Quantifiers over $\mathbb{N}$ are not allowed.)

Some Remarks

- In model theory, an extension with this property is called *elementary extension*: $(K, v) \prec (K^*, v^*)$
- More generally, if (K_i, v_i, Γ_i) is a valued field for every $i \in I$, then one can define the *ultraproduct* by taking

$$\prod_{i \in I} K_i = \{(a_i)_{i \in I} : a_i \in K_i\}$$

  instead of K^I and defining the analog equivalence relation there.
- This construction works for any model-theoretic structure.
- One can prove the existence of an extension with the desired properties using the *compactness theorem* from model theory instead.

Properties following directly from Łoś's Theorem

- If (K, v) is henselian, then also the ultrapower (K^*, v^*) is.
- Let $f_1, \ldots, f_m \in \mathcal{O}_v[X_1, \ldots, X_n]$. If they have a common zero in $(\mathcal{O}_{v^*})^n$, then they also have in $\mathcal{O}_v^n$.
- Let $f_1, \ldots, f_m \in \mathcal{O}_v[X_1, \ldots, X_n]$. If for any $\gamma \in \Gamma$ there is some $\underline{x} \in \mathcal{O}_v^n$, such that

$$v(f_i(\underline{x})) > \gamma, i = 1, \ldots, m,$$

  then also for every $\gamma^* \in \Gamma^*$, there is some $\underline{x}^* \in (\mathcal{O}_{v^*})^n$ with

$$v^*(f_i(\underline{x}^*)) > \gamma^*, i = 1, \ldots, m.$$

- $K^*v^*|Kv$ is *separable*. (Note that in general $K^*|K$ is not algebraic.)
- Γ^*/Γ is torsion-free.

Separability for Transcendental Field Extensions

Definition

- A finitely generated field extension $L|K$ is *separably generated*, if a *separating transcendence basis* exists, i.e. there is a transcendence basis $t_1, \ldots, t_n$ such that $L|K(t_1, ...t_n)$ is a finite separable extension.
- A field extension $L|K$ is *separable*, if every finitely generated extension of K, which is contained in L is separably generated over K.

Theorem

$L|K$ is separable if and only if L and $K^{1/p}$ are linearly disjoint over K, i.e. every tuple $a_1, \ldots, a_n \in K^{1/p}$ that is linearly independent over K stays linearly independent over L.

The Infinitely Large Element

We don't want just any ultrapower, we want one where an "infinitely large element" exists, i.e. that there is some $\gamma_0 \in \Gamma^*$, such that $\gamma_0 > \gamma$ for every $\gamma \in \Gamma$.

! This is not true in general, but we can enforce this by choosing a suitable ultrafilter !

Set $I = \Gamma$. It is easy to verify that the set of cofinal subsets

$$\mathcal{F}_0 := \{U \subseteq I \mid \exists \gamma \in U : \forall \delta \in I : \delta \geq \gamma \Longrightarrow \delta \in U\}$$

is a filter on I. $\mathcal{F}_0$ is contained in an ultrafilter $\mathcal{F}$. The ultrapower of Γ with respect to this ultrafilter $\mathcal{F}$ possesses such an infinitely large element:
Let $\gamma_0 := [(\delta)_{\delta \in I}]$. Then for $\gamma \in \Gamma$, we have $\{\delta \in I : \delta \geq \gamma\} \in \mathcal{F}_0 \subseteq \mathcal{F}$, so $\gamma_0 \geq \gamma$.

From now on, we will accept, that there is an extension (K^*, v^*) of our henselian valued field (K, v) that satisfies:

1. (K^*, v^*) is again henselian.
2. If $\{f_1, ..., f_m\} \subseteq \mathcal{O}[X_1, \ldots, X_n]$ has a zero in $\mathcal{O}_{v^*}$, then it already has a zero in $\mathcal{O}_v$.
3. There is $\gamma_0 \in \Gamma_{v^*}$ with $\gamma_0 \gg \Gamma_v$, i.e. $\gamma_0 > \gamma$ for every $\gamma \in \Gamma_v$.
   There is $\underline{x}^* \in (K^*)^n$ with $v^*(f_i(\underline{x}^*)) > \gamma_0$.
4. $K^* v^* | K v$ is separable.
5. Γ_{v^*} / Γ_v is torsion-free.

Proof sketch

- Let (K^*, v^*) be the extension obtained from the ultrapower construction with the desired properties.
- Goal: Find a solution in K^*, then there is one in K.
- Let $\Delta \leq \Gamma_{v^*}$ be the smallest convex subgroup, that contains Γ_v.
- Consider the *decomposition* of $v^* = \bar{v} \circ w$ with respect to Δ, i.e.

$$\bar{v}\colon \begin{cases} (K^*w)^\times & \to & \Delta \\ x + \mathfrak{m}_w & \mapsto & v^*(x) \end{cases} \quad \text{and} \quad w\colon \begin{cases} (K^*)^\times & \to & \Gamma_{v^*}/\Delta \\ x & \mapsto & v^*(x) + \Delta. \end{cases}$$

(Γ_{v^*}/Δ is again an ordered abelian group with

$$\gamma + \Delta < \delta + \Delta :\Longleftrightarrow \gamma + \Delta \neq \delta + \Delta \text{ and } \gamma < \delta)$$

Consider the *decomposition* of $v^* = \bar{v} \circ w$ with respect to Δ, i.e.

$$\bar{v}\colon \left\{ \begin{array}{rcl} (K^*w)^\times & \to & \Delta \\ x + \mathfrak{m}_w & \mapsto & v^*(x) \end{array} \right. \quad \text{and} \quad w\colon \left\{ \begin{array}{rcl} (K^*)^\times & \to & \Gamma_{v^*}/\Delta \\ x & \mapsto & v^*(x) + \Delta. \end{array} \right.$$

Note that:

- w is trivial on K.
- K embedds into K^*w via the residue mapping res_w.
- Let $\underline{x}^* \in (K^*)^n$ be the approximate solution for the infinitely large element $\gamma_0 \in \Gamma_{v^*}$, then

$$w(f_i(\underline{x}^*)) = v^*(f_i(\underline{x}^*)) + \Delta > \gamma_0 + \Delta > 0 + \Delta, \quad \text{i.e. } f_i(\underline{x}^*) \in \mathfrak{m}_w.$$

- $\bar{f}_i(\underline{\bar{x}}^*) = 0 \in K^*w, \quad \underline{\bar{x}}^* = (\bar{x}_1^*, \ldots, \bar{x}_n^*), \quad \bar{x}_i^* = x_i + \mathfrak{m}_w \in K^*w$

Thus we found a zero in K^*w.

Lemma

Let (K, v) be a henselian and defectless valued field and (L, w) some extension.

$$\Gamma_w/\Gamma_v \text{ torsion-free and } Lw|Kv \text{ separable} \implies L|K \text{ separable}$$

Apply the Lemma to

$$\bar{v} : \begin{cases} (K^*w)^\times & \to \quad \Delta \\ x + \mathfrak{m}_w & \mapsto \quad v^*(x) \end{cases}$$

Value group: $\Gamma_{\bar{v}} = \Delta \subseteq \Gamma_{v^*}$
Residue field: $(K^*w)\bar{v} = K^*v^*$
From our ultrapower construction, we know that

- $\Delta/\Gamma_v \leq \Gamma_{v^*}/\Gamma_v$ is torsion-free.
- $K^*v^*|Kv$ is separable.

$\implies$ Lemma: $K^*w|K$ is separable

From K^*w to K^*

Lemma

Let $K^*|K$ be a field extension, and w a henselian valuation on K^* that is trivial on K. (K embedds into K^*w via the residue mapping res_w. We write $K \subseteq K^*w$.)
Let $F \subseteq K^*w$ be a finitely generated separable extension of K. Then there exists some extension $F' \subseteq \mathcal{O}_w$ of K, such that the residue mapping res_w restricts to an isomorphism $F' \to F$.

Proof:

$$
\begin{array}{ccc}
K^* \supseteq \mathcal{O}_w & \xrightarrow{\mathrm{res}_w :\, x \mapsto x + \mathfrak{m}_w} & K^*w \\
\Big| & & \Big| \\
F' = K(t'_1, \ldots, t'_l)(\alpha') & \xrightarrow{\cong} & F = K(t_1, \ldots, t_l)(\alpha) \\
\Big| & & \Big| \\
K(t'_1, \ldots, t'_l) & \xrightarrow{\cong} & K(t_1, \ldots, t_l) \\
& \diagdown \quad \diagup & \\
& K &
\end{array}
$$

Bibliography

- Engler, A. J. and Prestel, A.: *Valued Fields*. Springer, 2005.
- Ershov, Yu. L.: *Multi-Valued Fields*. Springer, 2001.
- Ershov, Yu. L.: *Rational Points over Henselian Fields*. Algebra i Logika 6.3, 1967, p. 39-49 (in Russian).
- Hodges, W.: *A Shorter Model Theory*. Cambridge University Press, 1997.
- Lang, S.: *Algebra*. Springer, 2002.