Courses of June 8 and 9

Here are the lemmas necessary for the proof of step 6 of Theorem 5.

Lemma 8. *Let Γ be an ordered abelian group, $m_1, \dots, m_n$ be distinct integers, $\beta_1, \dots, \beta_n \in \Gamma$, and $(\gamma_\alpha)_{\alpha<\kappa}$ a strictly increasing sequence of elements of Γ without last element. Then there is some α_0 and i such that for $\alpha > \alpha_0$, for every j one has*

$$m_i\gamma_\alpha + \beta_i < m_j\gamma_\alpha + \beta_j.$$

Proof. Do the case $n = 2$, with $m_1 < m_2$. One needs to compare

$$\beta_1 = \beta_2 \text{ with } (m_2 - m_1)\gamma_\alpha.$$

The term on the right hand side (rhs) is strictly increasing. So, either it stays always smaller than the lhs, or it becomes bigger (and stays bigger).

Lemma 9. *Let (L, v) be an immediate extension of the valued field (K, v). Assume that K is Henselian, with no proper immediate algebraic extension. Let $a \in L$ with a transcendental over K. If $P(T) \in K[T]$ is monic, then there is some δ such that on the ball $B(a; \delta)$, $v(P(x) - P(a))$ grows with $v(x - a)$. Furthermore, $v(P(x))$ is constant on $B(a; \delta)$.*

Proof. Let $I = \{v(a - c) \mid c \in K\}$. Then I is an initial segment of Γ_K, with no last element. The proof is by induction on the degree of P. If it equals 1, then P is linear, hence of the form $T - c$. Take $\delta > v(c - a)$. We will assume that $P(T)$ is irreducible over K.
Assume the result shown for polynomials of lower degree, and write

$$P(x) = P(a) + \sum_{i\geq 1}^{\deg(P)} D_i(P)(a)(x - a)^i.$$

Let $\beta_i = v(D_i(P)(a))$. We let $(\gamma_\alpha)_{\alpha<\kappa}$ be a strictly increasing sequence of elements of I, which is cofinal in I. Since I has no greatest element, this sequence has no last element. Choose i and α_0 as in the previous lemma for $\beta_j + j\gamma_\alpha$, $j = 1, \dots, \deg(P)$. Then $v(P(x) - P(a)) = \beta_i + iv(x - a)$ as soon as $v(x - a) > \gamma_{\alpha_0}$. This shows the first assertion.
If for some $\alpha > \alpha_0$, we have $v(P(a)) \leq \beta_i + i\gamma_\alpha$, then $v(P(a)) < \beta_i + i\gamma_{\alpha+1}$ and for any $x \in B(a; \gamma_{\alpha+1})$ we have $v(P(x)) = v(P(a))$. Assume therefore that there is no such α: for all α, we have $v(P(a)) > \beta_i + i\gamma_\alpha$. Hence for $x \in B(x, \gamma_\alpha)$, we have $v(P(x)) = \beta_i + iv(x - a)$, which grows with $v(x - a)$. However, no polynomial of lower degree has this property.
We let b be a root of the polynomial $P(T)$ (in K^{alg}). Every element of $K(b)$ is of the form $Q(b)$, for some $Q(T) \in K[T]$ of degree $< \deg(P)$, and we extend the valuation to $K(b)$ by setting $v(Q(T))$ to be the eventual value of $v(Q(c))$ for $c \in K$ sufficiently close to a. One checks that this defines a valuation, and that $K(b)/K$ is immediate. But ... K is supposed to be Henselian, with no proper algebraic immediate extension.
(The only delicate point is to check that the valuation we defined behaves well for multiplication.

Let $f(T), g(T)$ be polynomials of degree less than degree of P, write $f(T)g(T) = q(T)P(T) + h(T)$ with $\deg(h) < \deg(P)$, and let α_0 be given by the lemma for f, g, q. Then $f(x)g(x) - h(x) = q(x)P(x)$ on $B(a; \gamma_{\alpha_0})$, one verifies that the rhs is strictly increasing, whence the lhs must be too, and therefore $v(h(x)) = v(f(x)g(x))$ on $(B; \gamma_{\alpha_0})$.)

Remarks 10. What we did above, is to use pseudo-convergent sequences without saying it. For a complete treatment of these, see the paper of Kaplansky [3].

Remarks 11. Steps 1 and 2 of the proof were taking place entirely in the residue field and value group. I.e., we were just extending an embedding of k_A to k_C, and an embedding of Γ_A to Γ_C, using the fact that the original embeddings $k_A \to k_N$ and $\Gamma_A \to \Gamma_N$ were elementary. In other words, if k_A and Γ_A had extra structure, we could have transported it as well. This give the following:

Corollary 12. *Let $\mathcal{L}'_{\mathrm{Pas}}$ be the language obtained from $\mathcal{L}_{\mathrm{Pas}}$ by increasing the languages of the sorts VG and RF (but not the language of the sort VF). Let $T'_{0,0} = T_{0,0}$ (viewed as a theory in $\mathcal{L}'_{\mathrm{Pas}}$). Then $T'_{0,0}$ eliminates the quantifiers of sort VF.*

Corollary 13. *Let (M, v) and (N, w) be Henselian valued field of residual characteristic 0. If $\Gamma_M \equiv \Gamma_N$ (in $\mathcal{L}_{VG}$) and $k_M \equiv k_N$ (in $\mathcal{L}_{RF}$), then $M \equiv N$. Similarly, if $M \subset N$, then $M \prec N \iff \Gamma_M \prec \Gamma_N$ and $k_M \prec k_N$.*

Proof. Pass to elementary extensions of M and N if necessary to assume that they have $\underline{\mathrm{ac}}$ maps, and use the theorem: a sentence of $\mathcal{L}_{\mathrm{Pas}}$ is equivalent to a sentence built from sentences of $\mathcal{L}_{VG}$ or of $\mathcal{L}_{RF}$, and from quantifier-free formulas. But the only $\mathcal{L}_{VF}$ terms are polynomials over $\mathbb{Z}$.
Alternatively: the 3-sorted structures $\mathcal{M}$ and $\mathcal{N}$ have as isomorphic substructures $(\mathbb{Z}, 0, \mathbb{Z})$, by an isomorphism which satisfies the conditions of the proof. Hence is elementary.

Corollary 14. *Let $\mathcal{L}'_{VG}$ be a language containing $\mathcal{L}_{VG}$ and assume that T'_{RG} is a theory extending the theory of ordered abelian groups with ∞ and which eliminates quantifiers. Let $\mathcal{L}_{RF}$ be a language extending the language of rings, and T_{RF} a theory which contains the theory of fields of characteristic 0 and eliminates quantifiers. Then the theory $T'_{0,0} = T_0 \cup T'_{VG} \cup T'_{RF}$ eliminates quantifiers.*

Remarks 15. Why couldn't we replace the $\underline{\mathrm{ac}}$ map by res? Where did we use the $\underline{\mathrm{ac}}$ map in the proof? Only in Step 0, to make sure that we saw enough of the residue field. Indeed, consider $R = \mathbb{Q}[t, t\sqrt{2}]$, with the t-adic valuation. Then $R/(t) \simeq \mathbb{Z}$: it doesn't see $\sqrt{2}$.
This problems disappears if we extend the languages $\mathcal{L}_{VF}$ (and $\mathcal{L}_{RF}$) by adding the multiplicative inverse map $^{-1}$ (with $0^{-1} = 0$). Our 3-sorted structures can now again be (K, Γ_K, k_K), with the $\underline{\mathrm{ac}}$-map replaced by the residue map; we extend the residue map to the whole field by setting it equal to 0 outside of $\mathcal{O}_v$. We get the same quantifier elimination for the appropriate theory obtained by replacing the axioms concerning $\underline{\mathrm{ac}}$ by those concerning res.

Example 16. Consider $\mathbb{C}((t))$, with the usual t-adic valuation. We know it is Henselian, with residue field $\mathbb{C}$ (which eliminates quantifiers in $\mathcal{L}_{RF}$). However, $\mathbb{Z}$ does not eliminate quantifiers in $\mathcal{L}_{VG}$. It turns out that there is a simple language in which it doess:

$$\mathcal{L}_{\text{Pres}} = \{+, -, 0, 1, <, \equiv_n\}_{n\in\mathbb{N}}$$

where $\equiv_n$ is interpreted as $x \equiv_n y \iff \exists z,\ nz = (x-y)$. (Here of course, nz is an abbreviation for $z + z + \cdots + z$ n-times). So defining $\mathcal{L}'_{VG} = \mathcal{L}_{\text{Pres}}$, we have quantifier elimination of $T'_{0,0}$, which is obtained by adding the following axioms to the theory of ordered abelian groups: 1 is the smallest positive element; for all n, the axiom $\forall x \bigvee_{i=0}^{n-1} x \equiv_n i$.

Example 17. Consider now $\mathbb{R}((t))$ with the t-adic valuation. The theory of real closed fields, RCF, does not eliminate quantifiers. However, it suffices to add $<$ to the language to get it. The proof is based on Sturm's algorith, for deciding if poynomials (in 1 variable) have roots, and how many. So, take $\mathcal{L}'_{VG} = \mathcal{L}_{\text{Pres}}$, and $\mathcal{L}'_{RF} = \{+, -, \cdot, 0, 1, <\}$ to get qe.

Definition 18. Let S be a $(\emptyset)$-definable set in some model M. One says that S is *stably embedded* if for every n, every definable subset of S^n (maybe with parameters) can be defined with parameters from S.

Corollary 19. *Let $\mathcal{M} = (M, \Gamma_M, k_M)$ be a model of $T_{0,0}$. Then k_M and Γ_M are stably embedded.*

Proof. We may assume that M is countable. If not, there is some $D \subset k_M^n$ which is definable with parameters c in M, but is not definable by any $\mathcal{L}_{RF}(k_M)$-formula. Thus the following type is consistent:

$$\Sigma(x, y) := \{x \in D \wedge y \notin D\} \cup \{\varphi(x) \iff \varphi(y) \mid \varphi(x) \text{ a } \mathcal{L}_{RF}(k_M)\text{-formula}\}.$$

Realise it in some $\aleph_1$-saturated extension N of M, by $\bar{b}_1$, $\bar{b}_2$. Then the partial isomorphism $(M, \Gamma_M, k_M(\bar{b}_1)) \to (M, \Gamma_M, k_M(\bar{b}_2))$ which is the identity on $\mathcal{M}$ and sends $\bar{b}_1$ to $\bar{b}_2$ is elementary, by (the proof of) Theorem 5, because it is elementary on $k_M(\bar{b}_1)$. This contradicts the fact that D (which was defined over M) contains $\bar{b}_1$ and not $\bar{b}_2$.
The proof is similar for Γ_M.