Courses of June 9 (end) and June 12

At the end of the class of Friday, I also made various remarks and gave some examples.

Let R be a real closed field. (The theory RCF of real closed fields is axiomatised by saying that every polynomial of odd degree has a root, and every square is a 4-th power.) Let R^{fin} be the convex hull of $\mathbb{Z}$ inside R: $\{a \in R \mid \text{for some } n \in \mathbb{N}, -n < a < n\}$. If R is non-archimedean, this is a proper subring of R, and is a valuation ring: if $a \in R \setminus R^{fin}$, this is because $|a|$ is very large, hence $|a^{-1}|$ is very close to 0 and is in R^{fin}. The maximal ideal of R^{fin} is the ideal of *infinitesimals*: $\mathcal{M} = \{a \in R \mid \text{for all } n \in \mathbb{N}^{>0}, 0 < |a| < 1/n\}$.
We define a valuation on R by setting $v(x) \geq 0$ if and only if $x \in R^{fin}$. Note that $R^{>0}$ is a torsion free divisible subgroup of $R^\times$, and therefore the value group Γ of v is also divisible, and there is a cross section $s : \Gamma \to K^{>0}$ (i.e., a group homomorphism such that $v \circ s = id$). Let k be the residue field of R. It is archimedean, and therefore isomorphic to a subfield of $\mathbb{R}$.
Claim. R embeds into $k((t^\Gamma))$.
One shows easily, using the Henselianity of R (why is it Henselian? Because it is real closed, with residue field real closed) that R contains an isomorphic copy of k: without loss of generality we identify k with this copy. Then, we notice that because $R^{>0}$ is divisible, we can find a cross section s of the valuation. So, R contains a copy of the ring $k[t^\Gamma]$, obtained by sending t^g to $s(g)$ for $g \in \Gamma$. It also contains a copy of the field of fractions $k(t^\Gamma)$ of $k[t^\Gamma]$, and is an immediate extension of $k(t^\Gamma)$. Let $A \subset R$ be maximal such that there is an embedding f of A into $k((t^\Gamma))$. Then A is a Henselian valued field, hence relativaly algebraically closed in R. If $a \in R \setminus A$, then a is transcendental, and as usual we consider $I = \{v(c-a) \mid a \in A\}$, select a sequence c_α, $\alpha < \kappa$, in A, such that $\gamma_\alpha = v(a - c_\alpha)$ is cofinal in I, and strictly increasing with α. For any $g \in \Gamma$ and $b = \sum_{\gamma \in \Gamma} b_\gamma t^\gamma \in k((t^\Gamma))$, we define the truncation of b at g to be $b|_g = \sum_{\gamma \leq g} b_\gamma t^\gamma$. Then $b|_g \in k((t^\Gamma))$. We define $b_\alpha = f(c_\alpha)|_{\gamma_\alpha}$. Note that for $\alpha < \beta < \kappa$, we have $(b_\beta)|_{\gamma_\alpha} = b_\alpha$, and therefore the series b defined by $\text{supp}(b) = \bigcup_{\alpha<\kappa} \text{supp}(b_\alpha)$ and $b|_{\gamma_\alpha} = b_\alpha$ is uniquely defined and belongs to $k((t^\Gamma))$; the map $A(a) \to f(A)(b)$ which sends a to b is an isomorphism of valued fields.

Remarks 20. Some general remarks.

(1) Basically the same technique of proof (by truncation) shows that $k((t^\Gamma))$ has no proper immediate extension. It is therefore Henselian.

(2) Let K be a valued field. A sequence $(a_\alpha)_{\alpha<\kappa}$ of elements of K is called a *Cauchy sequence* if for every $\gamma \in v(K^\times)$, there is some α_0 such that for $\alpha_0 < \alpha < \beta$ one has $v(a_\beta - a_\alpha) > \gamma$. One can also define it as a sequence such that the values $v(a_{\alpha+1} - a_\alpha)$ are strictly increasing and cofinal in $v(K^\times)$.

(3) The valued field is complete if all Cauchy sequences have limits in K.

(4) The *completion* of a valued field K is defined as in the classical case: the cardinal κ is the *cofinality* of Γ, i.e., the smallest cardinal such that there is a sequence $\gamma_\alpha, \alpha < \kappa$, which is

cofinal in Γ. One then looks at all Cauchy sequences indexed by κ, puts a ring structure on it, and quotients by the ideal of those whose limit is 0.

(5) You probably know that a field K is algebraically closed if and only if it is perfect and $\mathcal{G}al(K^{alg}/K) = 1$, and that a field K is real closed if and only if $\mathcal{G}al(K^{alg}/K)$ is finite, if and only if $\mathcal{G}al(K^{alg}/K) \simeq \mathbb{Z}/2\mathbb{Z}$. There is a similar result concerning $\mathbb{Q}_p$, by J. Koenigsmann: A field K is elementarily equivalent to $\mathbb{Q}_p$ if and only if $\mathcal{G}al(K^{alg}/K) \simeq \mathcal{G}al(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$.

Course of June 12

Study of the field of p-adic numbers

There are several languages in which they eliminate quantifiers. It turns out that the Pas language is not quite enough, as it doesn't capture e.g. the formula $\exists y\, y^p = x$. One introduces a language with ω sorts: the VF and VG sorts as before; the RF_n-sorts, with universe $\mathcal{O}/(p^n)$, and one defines the $\underline{\mathrm{ac}}_n$ maps: $K^\times \to \mathcal{O}/(p^n)$ in a manner analogous to the way the $\underline{\mathrm{ac}}$-map was defined (multiplicative, coincides with the natural map on $\mathcal{O}^\times$). One can then show that the theory of $\mathbb{Q}_p$ in this language eliminates the VF (and RF_n) quantifiers. To get full qe, one needs enlarge $\mathcal{L}_{VG}$ to $\mathcal{L}_{\mathrm{Pres}}$. We will study another language.

The language of Macintyre.
Consider, for $n \geq 2$, the predicate P_n, which defines the set of n-powers: $P_n(x) \iff \exists y\, y^n = x$. Then observe that in $\mathbb{Q}_p$ one has:
$(p \neq 2)$: $v(x) \geq 0 \iff P_2(1 + px^2)$,
$(p = 2)$: $v(x) \geq 0 \iff P_3(1 + px^3)$.
One also has (contrary to what I said in class), that $v(x) \geq v(y) \iff P_2(px^2 + y^2)$ (or $P_3(2x^3 + y^3)$). We will show that the theory of $\mathbb{Q}_p$ eliminates quantifiers in the language $\mathcal{L}_{\mathrm{Mac}} = \{+, -, \cdot, 0, 1, P_n\}_{n\in\mathbb{N}}$. The theory of $\mathbb{Q}_p$, pCF, is axiomatised by the following axioms: Field K, and defining axioms for the P_n's; $P_2(1 + px^2)$ defines a valuation subring $\mathcal{O}$ of K, with p generating the maximal ideal, and $\mathcal{O}/(p) \simeq \mathbb{F}_p$; the valuation is Henselian, and the value group Γ (isomorphic to $K^\times/\mathcal{O}^\times$) has a smallest strictly positive element $v(p)$ (which we denote by 1), and for every n, the axiom $\forall x \exists y \bigvee_{i=0}^{n-1} v(xy^n p^i) = 0$. (So the last series of axioms axiomatise the theory of $(\mathbb{Z}, +, -, <, 0, 1)$.)

We will use the following result, which we will (maybe) prove later:

Lemma 21. *Let K be a Henselian field of characteristic 0, and assume that its value group has a smallest strictly positive element (denoted 1) and that $v(p) = e1$ for some integer $e > 0$ and prime p. (So $v(p) > 0$, the residue characteristic is p). Then if L is a finite normal extension of K, we have $[L : K] = [\Gamma_L : \Gamma_K][k_L : k_K]$. (I.e., in Ostrowski's theorem, $d = 1$).*

Theorem 22. *The theory pCF eliminates quantifiers in the language $\mathcal{L}_{\mathrm{Mac}}$.*

Proof. The strategy is similar to the one for proving Theorem 5. Take two $\aleph_1$-saturated models of pCF, M and N, and countable subrings A of M, B of N, with an $\mathcal{L}_{\mathrm{Mac}}$-isomorphism

$f : A \to B$, which we wish to extend to some $a \in M \setminus A$. We first take a countable elementary substructure C of M which contains A and a, and we will extend f to C.
Step 0: extend f to the fraction field of A.
Note that $P_n(ab^{-1}) \iff P_n(ab^{n-1})$. So f extends to an $\mathcal{L}_{\text{Mac}}$-isomorphism.
Step 1 and 2 are unnecessary.
Step 3. Extend f to A^h (the henselization of A). That the field isomorphism extends is clear (recall that f is an isomorphism of valued fields). Since A^h/A is immediate, the extension respects the P_n's (cf Lemma 7).
In fact we will do all the remaining steps of the proof of Thm 5 at once. We know that the residue field of C is $\mathbb{F}_p$. Because C is countable, we can find a sequence of subfields $(C_n)_{n\in\mathbb{N}}$ such that $C = \bigcup_n C_n$, $C_0 = A^{alg} \cap C$, for every n, $C_n^{alg} \cap C = C_n$, and $trdeg(C_{n+1}/C_n) = 1$.
The extension C_0 of A is purely ramified. Note the following:
$(*)$ *To extend f to C_0, it suffices to be able to extend f to any finitely generated subextension $E = A(a_1, \ldots, a_m)$ of C_0.*
This follows by compactness, and because N is $\aleph_1$-saturated. So, let $E = A(a_1, \ldots, a_m)$. As $E \subset A^{alg}$, we know that E is purely ramified (by Lemma 21), and that $v(E^\times)/v(A^\times)$ is finite, hence a direct sum of finite cyclic groups, say $\langle\gamma_1\rangle + v(A^\times) \oplus \cdots \oplus \langle\gamma_r\rangle + v(A^\times)$. By Lemma 7 (2), there are $b_1, \ldots, b_r \in E$ such that $v(b_i) = \gamma_i$, and $b_i^{m_i} \in A$, where m_i is the order of γ_i modulo $v(A^\times)$. As $N \models P_{m_i}(f(b_i^{m_i}))$ for all i, we may extend, by sending b_i to an m_i-th root of $f(b_i^{m_i})$. It will automatically be an isomorphism of valued fields.
Hence, using compactness, we extend f to all of C_0. As $C_0 = A^{alg} \cap C$, if we show that $f(C_0) = B^{alg} \cap N$, then this f will also preserve the predicates P_n. But if this was not the case, we would argue again that there would be some element c in $B^{alg} \cap N$ with $c^m \in B$, and reach a contradiction, since f was preserving the P_n's on A and hence on B.
Extending from C_n to C_{n+1}.
There are two possible cases for the extension C_{n+1}/C_n: either it is immediate, or it is ramified.
In the immediate case, we proceed as in the proof of Step 6 of Thm 5 (see pages 7 and 8 of the notes): select an a, extend to $A(a)$ and then to $A(a)^h$; by Lemma 21, $A(a)^h = A(a)^{alg} \cap C$.
In the ramified case. Observe that $v(C^\times)/\mathbb{Z}$ is divisible (where $\mathbb{Z}$ is the subgroup generated by $v(p)$). And therefore, so is $v(C_{n+1}^\times)/v(C_n^\times)$, and it is isomorphic to $\mathbb{Q}$ (because of the tr.deg 1 assumption). If E is a finitely generated extension of C_n contained in C_{n+1}, then $v(E^\times)/v(C_n^\times)$ is isomorphic to $\mathbb{Z}$. Let γ be a generator of $v(E^\times)$ modulo $v(C_n^\times)$, let $a \in E$ be such that $v(a) = \gamma$. Then $v(E^\times) = v(C_n^\times) \oplus \langle\gamma\rangle$, E is an immediate extension of $C_n(a)$ (because one cannot increase the residue field), so is contained in $C_n(a)^h$. Extend f by sending a to some element b with $v(b) = \gamma'$, where γ' satisfies the following set of formulas:

$$\Sigma(\xi) := \{m\xi + f_\Gamma(\alpha) > 0 \mid \Gamma_C \models m\gamma + \alpha > 0,\ m \in \mathbb{Z}, \alpha \in v(C_n^\times)\}.$$

As $C_n(a)/C_n$ is purely ramified, and by our choice of γ' and b, this is an isomorphism of valued fields. Then extend to $C_n(a)^h$, which contains E.
So, using $(*)$, this shows that we can extend f to all of C_{n+1}. As with C_0 one shows that $f(C_{n+1})^{alg} \cap N = f(C_{n+1})$. We know that $f(C_{n+1})$ is Henselian; also we know that $v(f(C_{n+1}^\times))/v(f(C_n^\times))$ is divisible, hence $f(C_{n+1})^{alg}/f(C_{n+1})$ cannot be ramified. This finishes the proof. (Henselian

+ unramified + same residue field + Lemma 21 means equal).

Corollary 23. *Consider the theory T of $\mathbb{Q}_p$ in the language of rings. Then this theory is model complete, i.e.: every formula is equivalent, modulo T, to an existential formula.*

Proof. $P_n(x)$ is equivalent to an existential formula in the language of rings. And so is $\neg(P_n(x))$: As $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^n$ is finite, and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there are integers $1, i_1, \ldots, i_m$ which represent the cosets of $(\mathbb{Q}_p^\times)^n$ in $\mathbb{Q}_p^\times$. So $\neg P(x) \iff \bigvee_{j=1}^m P_n(i_j x)$.