Math 676. Completion of algebraic closure

1. Introduction

Let K be a field complete with respect to a non-trivial non-archimedean absolute value $|\cdot|$. It is natural to seek a "smallest" extension of K that is both complete and algebraically closed. To this end, let $\overline{K}$ be an algebraic closure of K, so this is endowed with a unique absolute value extending that on K. If K is discretely-valued and π is a uniformizer of the valuation ring then by Eisenstein's criterion we see that $X^e - \pi \in K[X]$ is an irreducible polynomial with degree e for any positive integer e, so $\overline{K}$ has infinite degree over K. In particular, $\overline{K}$ with its absolute value is *never* discretely-valued. In general if K is not algebraically closed then $\overline{K}$ *must* be of infinite degree over K. Indeed, recall from field theory that if a field F is not algebraically closed but its algebraic closure is an extension of finite degree then F admits an ordering (so F has characteristic 0 and only ± 1 as roots of unity) and $F(\sqrt{-1})$ is an algebraic closure of F (see Lang's *Algebra* for a proof of this pretty result of Artin and Schreier). However, a field K complete with respect to a non-trivial non-archimedean absolute value *cannot* admit an order structure when the residue characteristic is positive (whereas there are examples of order structures on $\mathbf{R}((t))$). Indeed, this is obvious if K has positive characteristic, and otherwise K contains some $\mathbf{Q}_p$ and hence it is enough to show that the fields $\mathbf{Q}_p$ do not admit an order structure. For $p > 3$ there are roots of unity in $\mathbf{Q}_p$ other than ± 1, and for $p > 2$ there are many negative integers n that satisfy $n \equiv 1 \bmod p$ and thus admit a square root in $\mathbf{Q}_3$. Similarly, any negative integer n satisfying $n \equiv 1 \bmod 8$ has a square root in $\mathbf{Q}_2$. This shows that indeed $[\overline{K} : K]$ must be infinite if the complete non-archimedean field K is not algebraically closed and its residue field has positive characteristic.

Although finite extensions of K are certainly complete with respect to their canonical absolute value (the unique one extending the absolute value on K), for infinite-degree extensions of K it seems plausible that completeness (with respect to the canonical absolute value) may break down. Indeed, it is a general fact that $\overline{K}$ is *not* complete if it has infinite degree over K. See 3.4.3/1 in the book "Non-archimedean analysis" by Bosch *et al.* for a proof in general, and see Koblitz' introductory book on p-adic numbers for a proof of non-completeness in the case $K = \mathbf{Q}_p$. We do not require these facts, but they motivate the following question: is this completion of $\overline{K}$ algebraically closed? If not, then one may worry that iterating the operations of algebraic closure and completion may yield a never-ending tower of extensions. Fortunately, things work out well:

Theorem 1.1. *The completion $\mathbf{C}_K$ of $\overline{K}$ is algebraically closed.*

The field $\mathbf{C}_K$ is to be considered as an analogue of the complex numbers relative to K, and for $K = \mathbf{Q}_p$ it is usually denoted $\mathbf{C}_p$. Observe that since $\mathrm{Aut}(\overline{K}/K)$ acts on $\overline{K}$ by isometries, this action uniquely extends to an action on $\mathbf{C}_K$ by isometries. The algebraic theory of infinite Galois theory therefore suggests the natural question of computing the fixed field for $\mathrm{Aut}(\overline{K}/K)$ on $\mathbf{C}_K$. Observe that this is not an algebraic problem, since the action on $\mathbf{C}_K$ makes essential use of the topological structure on $\mathbf{C}_K$. It is a beautiful and non-trivial theorem of Tate that if $\mathrm{char}(K) = 0$ and K is discretely-valued with residue field of characteristic p (for example, a local field of characteristic 0) then the subfield of $\mathrm{Gal}(\overline{K}/K)$-invariants in $\mathbf{C}_K$ coincides with K. That is, "there are no transcendental invariants" in such cases. This theorem is very important at the beginnings of p-adic Hodge theory.

The purpose of this handout is to present a proof of Theorem 1.1. Note that this theorem is proved in Koblitz' book in the special case $K = \mathbf{Q}_p$, but his proof unfortunately is written in a way that makes it seem to use the local compactness of $\mathbf{Q}_p$. The proof we give is a more widely applicable variant on the same method, and we use the same technique to also prove a result on continuity of roots that is of independent interest.

2. Proof of Theorem 1.1

Choose $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{C}_K[X]$ with $n > 0$. Since $\overline{K}$ is dense in $\mathbf{C}_K$, there exists polynomials

$$f_j = X^n + a_{n-1,j}X^{n-1} + \cdots + a_{0,j} \in \overline{K}[X]$$

with $a_{ij} \to a_i$ in $\mathbf{C}_K$ as $j \to \infty$. If $a_i \neq 0$ then we may arrange that $|a_{ij} - a_i| < \min(|a_i|, 1/j)$ for all j, so $|a_{ij}| = |a_i|$ for all j. If $a_i = 0$ then we may take $a_{ij} = 0$ for all j. Hence, for all $0 \le i \le n-1$ we have $|a_{ij}| = |a_i|$ and $|a_{ij} - a_i| < 1/j$ for all j. Of course, we have no control over the finite extensions $K(a_{ij}) \subseteq \overline{K}$ as j varies for a fixed i.

Since $\overline{K}$ is algebraically closed, we can pick a root $r_j \in \overline{K}$ for f_j for all j. The idea is to find a subsequence of the r_j's that is Cauchy, so it has a limit r in the *complete* field $\mathbf{C}_K$, and clearly $f(r) = \lim f_j(r_j) = 0$. This gives a root of f in $\mathbf{C}_K$. Since $f_j(r_j) = 0$ for all j, we have

$$|r_j^n| = \left| -\sum_{i=0}^{n-1} a_{ij} r_j^i \right| \le \max_i |a_{ij}||r_j|^i = \max_i |a_i||r_j|^i$$

because $|a_{ij}| = |a_i|$ for all j. Hence, for each j there exists $0 \le i(j) \le n-1$ such that $|r_j|^n \le |a_{i(j)}||r_j|^{i(j)}$, so $|r_j| \le |a_{i(j)}|^{1/(n-i(j))}$. Thus,

$$|r_j| \le C \stackrel{\text{def}}{=} \max(|a_0|^{1/n}, |a_1|^{1/(n-1)}, \dots, |a_{n-1}|)$$

for all j. Note that C only depends on the coefficients a_i of f.

Since f and f_j are monic with the same degree $n > 0$, we have

$$|f(r_j)| = |f(r_j) - f_j(r_j)| = \left| \sum_{i=0}^{n-1} (a_i - a_{ij}) r_j^i \right| \le \max_{0 \le i \le n-1} |a_i - a_{ij}||r_j|^i \le \max_{0 \le i \le n-1} |a_i - a_{ij}| \cdot \max(1, C^{n-1})$$

because $|r_j|^i \le C^i \le C^{n-1}$ for all i if $C \ge 1$ and $|r_j|^i \le C^i \le 1$ for all i if $C \le 1$. Recall that we choose a_{ij} so that $|a_{ij} - a_i| < 1/j$ for all j, so we conclude

$$|f(r_j)| \le \frac{\max(1, C^{n-1})}{j}$$

for all j. Hence, $f(r_j) \to 0$ as $j \to \infty$. We shall now use this fact to infer that $\{r_j\}$ has a Cauchy subsequence in $\mathbf{C}_K$, which in turn will complete the proof.

Let L be a finite extension of $\mathbf{C}_K$ in which the monic f splits, say $f(X) = \prod_k (X - \rho_k)$. We (uniquely) extend the absolute value on the (complete) field $\mathbf{C}_K$ to one on L, so we may rewrite the condition $f(r_j) \to 0$ as

$$\lim_{j \to \infty} \prod_{k=1}^{n} (r_j - \rho_k) = 0$$

in L. In other words, $\prod_{k=1}^{n} |r_j - \rho_k| \to 0$ in $\mathbf{R}$. Hence, by the pigeonhole principle, since there are only finitely many k's we must have that for some $1 \le k_0 \le n$ the sequence $\{|r_j - \rho_{k_0}|\}_j$ has a subsequence converging to 0. Some subsequence of the r_j's must therefore converge to ρ_{k_0} in L, so this subsequence is Cauchy in $\mathbf{C}_K$.

3. Continuity of roots

Let $f = \sum a_i X^i \in K[X]$ be monic of degree $n > 0$, so the roots of f in $\mathbf{C}_K$ lie in $\overline{K}$. An inspection of the proof of Theorem 1.1 shows that the argument yields the following general result:

Lemma 3.1. *Let $\{f_j\}$ be a sequence of monic polynomials $f_j = \sum a_{ij} X^j$ of degree n in $K[X]$ such that $a_{ij} \to a_i$ as $j \to \infty$ for all $0 \le i \le n-1$. Let $r_j \in \overline{K}$ be a root of f_j for each j. There exists a subsequence of $\{r_j\}$ that converges to a root of f in $\overline{K}$.*

We may now deduce the following general result that is usually called "continuity of roots" (in terms of their dependence on the coefficients of f).

Theorem 3.2. *Let $r \in \overline{K}$ be a root of a degree-n monic polynomial $f = \sum a_i X^i \in K[X]$, with $\operatorname{ord}_r(f) = \mu > 0$. Fix $\varepsilon_0 > 0$ such all roots of f in $\overline{K}$ distinct from r have distance at least ε_0 from r. (If there are no other roots, we may use any $\varepsilon_0 > 0$.) For all $0 < \varepsilon < \varepsilon_0$ there exists $\delta = \delta_{\varepsilon,f} > 0$ such that if $g = \sum b_i X^i \in K[X]$*

is monic with degree n and $|a_i - b_i| < \delta$ for all i then g has exactly μ roots (with multiplicity) in the open disc $B_\varepsilon(r) = \{x \in \overline{K} \mid |x - r| < \varepsilon\}$.

Proof. We argue by contradiction. Fix a choice of ε. If there exists no corresponding δ, then we would get a sequence of monic polynomials $f_j = \sum a_{ij} X^i \in K[X]$ with degree n such that $a_{ij} \to a_i$ as $j \to \infty$ for each i and each f_j does not have exactly μ roots on $B_\varepsilon(r)$. Pick factorizations $f_j = \prod_{k=1}^n (X - \rho_{jk})$ upon enumerating the n roots (with multiplicity) for each f_j in $\overline{K}$. By Lemma 3.1 applied to $\{\rho_{j1}\}$, we can pass to a subsequence of the f_j's so $\rho_{j1} \to \rho_1$ with ρ_1 some root of f in $\overline{K}$. Successively working with $\{\rho_{jk}\}_j$ for $k = 2, \dots, n$ and passing through successive subsequence of subsequences, etc., we may suppose that there exist limits $\rho_{jk} \to \rho_k$ in $\overline{K}$ as $j \to \infty$ for each fixed $1 \le k \le n$.

Each ρ_k must be a root of f, but we claim more: every root of f arises in the form ρ_k for exactly as many k's as the multiplicity of the root. Working in the finite-dimensional $\overline{K}$-vector space of polynomials of degree $\le n$ (given the sup-norm with respect to an arbitrary $\overline{K}$-basis, the choice of which does not affect the topology), we have

$$f_j = \prod_{k=1}^n (X - \rho_{jk}) \to \prod_{k=1}^n (X - \rho_k),$$

yet also $f_j \to f$. Hence, $f = \prod_{k=1}^n (X - \rho_k)$ in $\overline{K}[X]$. That is, $\{\rho_k\}$ is indeed the set of roots of f in $\overline{K}$ counted with multiplicites. Hence, $r = \rho_k$ for exactly μ values of k, say for $1 \le k \le \mu$ by relabelling.

By passing to a subsequence we may arrange that for each $1 \le k \le n$, $|\rho_{jk} - \rho_k| < \varepsilon$ for all j. In particular, if $1 \le k \le \mu$ we have $|\rho_{jk} - r| < \varepsilon$. Since all roots r' of f distinct from r have distance $\ge \varepsilon_0 > \varepsilon$ from r, by the non-archimedean triangle inequality we have $|\rho_{jk} - r'| = |r - r'| \ge \varepsilon_0 > \varepsilon$ for all $1 \le k \le \mu$ and any j. However, if $k > \mu$ then ρ_k is such an r', yet $|\rho_{jk} - \rho_k| < \varepsilon$ for all j and all k, so for each fixed j we must have $|\rho_{jk} - r| \ge \varepsilon_0 > \varepsilon$ for all $k > \mu$. Thus, for the j's that remain (as we have passed to some subsequence of the original sequence), $\rho_{j1}, \dots, \rho_{j\mu}$ are precisely the roots of f_j (with multiplicity) that are within a distinct $< \varepsilon$ from the root r of f. This contradicts the assumption on the f_j's. ■

Here is an important corollary that is widely used.

Corollary 3.3. *Let $f \in K[X]$ be a separable monic polynomial with degree n. Choose $\varepsilon > 0$ as in Theorem 3.2. For each monic $g \in K[X]$ with degree n and coefficients sufficiently close to those of f, g is separable and each root of g in $K_{\rm sep}$ is within a distance $< \varepsilon$ from a unique root of f in $K_{\rm sep}$. Moreover, if f is irreducible then g is irreducible.*

Proof. We apply Theorem 3.2 with $\mu = 1$ to conclude that if such a g is coefficientwise sufficiently close to f then each of the n roots of g (with multiplicity) is within a distance $< \varepsilon$ from a unique root of f. In particular, g has n distinct roots and hence is separable. Thus, all roots under consideration lie in $K_{\rm sep}$. The uniqueness aspect, together with the fact that ${\rm Gal}(K_{\rm sep}/K)$ acts on $K_{\rm sep}$ by isometries, implies that the ${\rm Gal}(K_{\rm sep}/K)$-orbit of a root of g has the same size as the ${\rm Gal}(K_{\rm sep}/K)$-orbit of the corresponding nearest root of f. Hence, the degree-labelling of the irreducible factorization of g over K "matches" that of the separable f, and in particular if f is irreducible then g is irreducible. ■