KRASNER'S LEMMA

1. Hypotheses and notations. Let K be a complete nonarchimedean filed. Let K^{sep} be the separable closure of K. Let K^{alg} be the algebraic closure of K. If $\alpha \in K^{\text{sep}}$, let

$$r(\alpha) = \min\{|\alpha - \sigma\alpha| : \sigma \in \text{Gal}(K^{\text{sep}}/K), \sigma\alpha \neq \alpha\}.$$

Note that $r(\alpha) > 0$ unless $\alpha \in K$ already.

Lemma 2 (Krasner' Lemma)**.** *For $\alpha \in K^{\text{sep}}$, let $\beta \in K^{\text{alg}}$ be an element such that*

$$|\alpha - \beta| < r(\alpha)$$

then $\alpha \in K(\beta)$.

Proof. If the degree of α is one then there is nothing to prove. Assume now α is not in K. Let h be the minimal polynomial of α with respect to $K(\beta)$. As α is separable over K, α is separable over $K(\beta)$. Let L be the smallest Galois extension of $K(\beta)$ containing α. Then all conjugates of α over $K(\beta)$ lies in L, and $\text{Gal}(L/K(\beta))$ preserves the absolute value $|\cdot|$ by the uniqueness of extensions of $|\cdot|$ to L. For each $\sigma \in \text{Gal}(L/K(\beta))$, we have by the hypothesis

$$|\sigma\alpha - \alpha| \geq r(\alpha) > |\alpha - \beta|.$$

Recall that in a nonarchimedean field, if $|a| > |b|$, then $|a + b| = |a|$. Hence we have

$$|\sigma\alpha - \beta| = |\sigma\alpha - \alpha| > |\alpha - \beta| = |\sigma(\alpha - \beta)| = |\sigma\alpha - \beta|.$$

This is a contradiction. □

Next we shall use Krasner's Lemma to deduce some consequences about roots of *monic* polynomials. The upshot is that if f and g are two monic polynomials that are sufficiently close to each other, then we can make a root of g sufficiently close to a root of f, smaller than difference of any roots of f. This enables us then to apply Krasner's lemma. Let us first prove some preliminary results that justifies the assertion that *roots of polynomials vary continuously with respect to the coefficients.* In the sequel, for a polynomial h with coefficients in K let $|h|_1$ is the 1-Gauß norm of a polynomial.

Lemma 3. *Let $f \in K[T]$ be a monic polynomial. Let $\alpha \in K^{\text{alg}}$ be a root of f. Then we have $|\alpha| \leq |f|_1$.*

Proof. Write $f(T) = T^n + \sum_{v=1}^n a_v T^{n-v}$. Let $\alpha \in K^{\text{alg}}$ be such that $|\alpha| > |f|_1 \geq 1$. Then $|\alpha^n| > |f|_1|\alpha^{n-1}| \geq |a_v||\alpha|^{n-v}$. Thus $|f(\alpha)| = |\alpha|^n \neq 0$. This shows that all roots of f are contained in the closed disk centered at 0 with radius $|f|_1$. □

Date: June 6, 2018.

Lemma 4. *Let $f, g \in K[T]$ be* monic *polynomials of degree n. Let $\alpha \in K^{\text{alg}}$ be a root of f. Then*

$$|g(\alpha)| \leq |f - g|_1 |f|_1^{n-1}.$$

Proof. Write $f(T) = T^n + \sum_{v=1}^n a_v T^{n-v}$, and $g(T) = T^n + \sum b_v T^{n-v}$. Then

$$g(\alpha) = g(\alpha) - f(\alpha) = \sum_{v=1}^{n} (b_v - a_v)\alpha^{n-v}.$$

Hence

$$\begin{aligned} |g(\alpha)| &\leq \max_{1 \leq v \leq n} |f_v - g_v||\alpha|^{n-v} \\ &\leq |f - g|_1 \max_{1 \leq v \leq n} |\alpha|^{n-v} \\ &\leq |f - g|_1 \cdot |f|_1^{n-1}. \end{aligned}$$

thanks to Lemma 3 and the fact that $|f|_1 \geq 1$ □

Lemma 5 (Continuity of roots)**.** *Let $f, g \in K[T]$ be monic polynomials of the same degree n. Let α be a root of f. Then there exists a root β of g such that*

$$|\alpha - \beta| \leq \sqrt[n]{|f - g|_1} \cdot |f|_1.$$

Proof. Let $g(T) = \prod_{i=1}^n (T - \beta_i)$ be the factorization, in K^{alg}, of g into linear factors. Assume that $|\beta_j - \alpha| > \sqrt[n]{|f - g|_1} \cdot |f|_1$ for all j. Then we have

$$|g(\alpha)| > |f - g|_1 |f|_1^n.$$

This contradicts to Lemma 4 since $|f|_1 \geq 1$. □

Recall that Hensel's lemma says that if $f \in K^\circ[T]$ has a solution α modulo the maximal ideal $K^{\circ\circ}$, and if moreover $f'(\alpha) \not\equiv 0$ modulo $K^{\circ\circ}$, then f has a zero β in K° such that $\beta \equiv \alpha$ modulo $K^{\circ\circ}$. This is generally not true if α is a double root of f modulo $K^{\circ\circ}$. The following consequence of Krasner's lemma is a sort of compensation.

Corollary 6. *Let K be a complete nonarchimedean field. Let $f \in K[T]$ be a monic separable polynomial. Then there exists $\epsilon = \epsilon(f) > 0$ such that if we can find $\alpha \in K$ such that $|f(\alpha)| < \epsilon$, then f has a root in K.*

Proof. Let α_i, $i = 1, 2, \ldots, n$, are the roots of f. Let r be the infimum of $|\alpha_i - \alpha_j|$. Fix a nonzero element ϖ in $K^{\circ\circ}$. Assume that $\epsilon < r^n |f|_1^{-1}$. Then $g(T) = f(T) - f(\alpha)$ is a polynomial with coefficients in K such that $|g - f|_1 < \epsilon$. Therefore, by Lemma 5, there is a root β of g such that

$$|\beta - \alpha| \leq r.$$

As all the Galois conjugates of α are roots of $f(T)$, we have $r \leq r(\alpha)$. By Krasner's Lemma, Lemma 2, we conclude that $\alpha \in K(\beta) = K$, as desired. □

In particular, the lemma says that, if K is discretely valued, for each monic polynomial $f \in K^\circ[T]$, there exists N, if f has a root modulo the Nth power of the maximal ideal, then f has a root in K°.

Corollary 7. *Let f be a monic, separable, irreducible polynomial of degree n. Then there exists $\epsilon = \epsilon(f)$ such that for any g a monic polynomial of degree n with $|g - f|_1 < \epsilon$, we have*

1. *g is irreducible and separable,*
2. *for each root α of f, g has a root β such that $K(\beta) = K(\alpha)$.*

Proof. Set $\epsilon = (|f|_1^{-1} r(\alpha))^n$. Since f is irreducible and separable, its roots consists of all the K-conjugates of α. If $|f - g|_1 < \epsilon$, then there is a root β of g such that

$$|\beta - \alpha| < r(\alpha)$$

and Krasner's lemma, Lemma 2, then implies that $K(\alpha) \subset K(\beta)$. By the hypothesis, $[K(\alpha) : K] = n$; since $\deg g = n$, we have $[K(\beta) : K] \leq n$. The inclusion $K(\alpha) \subset K(\beta)$ then implies that g is irreducible and $K(\beta) = K(\alpha)$, which in turn implies that β, hence g, is separable. □

Corollary 8. *Let C be an algebraically closed nonarchimedean field. Let $\widehat{C}$ be the completion of C. Then $\widehat{C}$ is algebraically closed.*

Proof. Let $f(T)$ be a monic separable irreducible polynomial with coefficients in $\widehat{C}$. We shall prove that $f(T)$ has a root. Let ϵ be the constant in Corollary 7. Using the density of C inside $\widehat{C}$ we can find a monic polynomial $g(T)$ with coefficients in C such that $|g - f|_1 < \epsilon$. Then g is irreducible and separable. As C is algebraically closed, g has degree 1, and thus f must have degree 1. Now that any irreducible polynomial with coefficients in $\widehat{C}$ must be of the form $f(T^q)$ where q is some power of p, the characteristic of C, and f is a separable irreducible polynomial. Hence all purely inseparable irreducible polynomial are $T^q - a$, $a \in \widehat{C}$. Let $\{a_n\}$ be a sequence in C that converges to $a \in \widehat{C}$. Then there is a subsequence of $a_n^{1/q}$ that converge to a root of the equation $T^q - a = 0$. Hence the equation $T^q - a = 0$ is also solvable in $\widehat{C}$. This completes the proof that $\widehat{C}$ is algebraically closed. □

Here we mention yet another application of the Krasner's lemma, found in a paper by de Jong–Starr [1, Lemma 1.4(b)] that proves any rationally connected variety over the function field of a curve over an algebraically closed field has a rational point.

Lemma 9. *Let k be an algebraically closed field. Let A be a complete discrete valuation ring with residue field k. Let $\mathfrak{m}$ be the maximal ideal of A. Let $\mu : A \to R$ be a finite, generically étale homomorphism of complete discrete valuation rings. Then there exists a positive integer N such that the following property holds: For each finite local A-algebra B that is a discrete valuation ring, if there exists a an isomorphism $R/\mathfrak{m}^n R \to B/\mathfrak{m}^n B$ for some $n > N$, then R is isomorphic to B as an A-algebra.*

Proof. Since A has algebraically closed residue field, every finite local A-algebra has residue field k. Thereby the algebras B and R are all totally ramified, and we can write $R = A[T]/(f(T))$, $B = A[T]/(g(T))$ for some Eisenstein polynomials $f, g \in A[T]$. See [2, Chapter I, Proposition 18].

Let K be the fraction field of A. Then K is a complete discretely valued field. By the hypothesis, f is a separable irreducible element in $K[T]$. The for n sufficiently large, the isomorphism modulo $\mathfrak{m}^n$ implies that we can arrange that $|f - g| < \epsilon$ with respect to the $\mathfrak{m}$-adic metric, where ϵ is as in Corollary 7. By the hypothesis, g has a root β in $L = \mathrm{Frac}(B)$. Corollary 7 implies there is a root α of f in K^{sep} satisfying $K(\alpha) = K(\beta) = L$. Thus f has a root in L. Since f has integral coefficients, it is necessary that $\alpha \in B$, by Lemma 3. We can then define a map $R \to B$ that is generically étale and has degree 1. Thus R is isomorphic to B, as desired. □

References

[1] Aise Johan de Jong and Jason Michael Starr, *Every rationally connected variety over the function field of a curve has a rational point*, Amer. J. Math. Vol. 125, no. 3, pp. 567–580, 2003.

[2] Jean-Pierre Serre, *Local fields*, vol. 67, Graduate Texts in Mathematics, Translated from the French by Marvin Jay Greenberg, Springer-Verlag, New York-Berlin, 1979, pp. viii+241.