

# Absolute Values and Completions

B.SURY

This article is in the nature of a survey of the theory of complete fields. It is not exhaustive but serves the purpose of familiarising the readers with the basic notions involved. Hence, complete (!) proofs will not be given here. It is no surprise that algebraic number theory benefits a lot from introducing analysis therein. The familiar notion of construction of real numbers is just one aspect of this facility.

## § 1. Discrete valuations

**Definition 1.1.** Let  $K$  be any field. A surjective map  $v : K^* \rightarrow \mathbf{Z}$  is called a *discrete valuation* if:

$$v(xy) = v(x) + v(y),$$

$$v(x + y) \geq \text{Inf}(v(x), v(y))$$

Here, for notational purposes, one also defines  $v(0) = \infty$ . Note also that one must have  $v(1) = 0 = v(-1)$ .

**Premier example 1.2.** For each prime number or, more generally, for any non-zero prime ideal  $P$  in a Dedekind domain  $A$ , one has the  *$P$ -adic valuation*  $v_P$  given by the prescription  $v_P(x) = a$  where the fractional principal ideal  $(x) = P^a I$  with  $I$  coprime to  $P$ . This is a discrete valuation on the quotient field  $K$  of  $A$ .

**Lemma 1.3.** (a) If  $v$  is a discrete valuation on a field  $K$ , then  $A_v := \{x \in K : v(x) \geq 0\}$  is a local PID. Its maximal ideal is  $P_v = \{x \in K : v(x) > 0\}$ . ( $A_v$  is called the *valuation ring* of  $v$ ).

(b) For a discrete valuation  $v$  on a field  $K$ , if  $k_v$  denotes the residue field  $A_v/P_v$  and  $U_i = 1 + P_v^i$  for  $i > 0$ , then  $A_v^*/U_1 \cong k_v^*$  and  $U_i/U_{i+1} \cong P_v^i/P_v^{i+1} \cong k_v^+$ .

(c) If  $A$  is a Dedekind domain,  $v$  a discrete valuation on its quotient field  $K$  and,  $A \subset A_v$ , then  $P := A \cap P_v$  is a non-zero prime ideal of  $A$ . Moreover,  $v = v_P$ ,  $PA_v = P_v$ ,  $A/P \cong A_v/P_v$ .

**Proof.** Quite easy.

**Exercise 1.4.** Let  $v$  be a discrete valuation on a number field  $K$ . Then  $\mathcal{O}_K \subseteq A_v$ .

**Proposition 1.5.** *On a number field  $K$ , the map  $P \mapsto v_P$  sets up a bijection between non-zero prime ideals of  $\mathcal{O}_K$  and discrete valuations.*

**Indication of proof.** The proof follows from the easily proved step: If  $A \subseteq B$  are discrete valuation rings with the same quotient field  $K$ . Then  $A = B$ .

**Proposition 1.6.** *Let  $F$  be any field and  $K = F(X)$ , the function field in one variable over  $F$ . Define  $v_\infty(f/g) = \deg(g) - \deg(f)$ . Then,*

- (a)  $v_\infty$  defines a discrete valuation on  $K$  which is zero on  $F^*$ ,
- (b)  $v_P$ , as  $P$  runs through the prime ideals of  $F[X]$  along with  $v_\infty$  exhaust all the possible discrete valuations on  $K$  that are trivial on  $F^*$ ,
- (c) (Product formula) For each  $f \in K^*$ , one has

$$v_\infty(f) + \sum_P f_P v_P(f) = 0$$

where  $P$  runs through the non-zero prime ideals of  $F[X]$  and  $f_P = [F[X] : P]$  is the degree of any polynomial generating  $P$ .

**Proof.** (a) is obvious.

(b) Let  $v$  be any discrete valuation on  $K$  which is trivial on  $F^*$ . First, suppose that  $v(X) \geq 0$ . Then,  $v(f) \geq 0 \forall f \neq 0 \in F[X]$ . As  $v$  surjects onto integers, there is some monic irreducible polynomial  $f$  such that  $v(f) > 0$ . If  $v(g) > 0$  for another monic, irreducible polynomial  $g$ , then  $v(1) = v(sf + tg) > 0$ , which is a contradiction. Thus,  $v(g) = 0$  for all monic irreducible polynomials  $g \neq f$ . Thus, writing any  $h \in F[X]$  as a product of irreducibles, one gets  $v(h) \in v(f)\mathbf{Z}$ . As  $v$  is surjective,  $v(f) = 1$  i.e.,  $v = v_f$ . Therefore, we have shown that if  $v(X) \geq 0$ , then  $v = v_P$  for some non-zero prime ideal  $P$ .

If  $v(X) < 0$ , it is easy to see by induction on the degree that  $v(h) = v(X)\deg(h)$  for any  $h \in F[X]$ . By surjectivity again, one gets  $v(X) = -1$  and so  $v = v_\infty$ .

(c) Finally, writing any  $f \in K^*$  as  $f = u \prod_i p_i^{v_{p_i}(f)}$  and comparing degrees, one gets the product formula.

## § 2. Absolute values

**Definition 2.1.** On a field  $K$ , an *absolute value* is a function  $|\cdot|: K \rightarrow \mathbf{R}^{\geq 0}$  such that

- (a)  $|x| = 0 \Leftrightarrow x = 0$ ,
- (b)  $|xy| = |x||y|$ , and
- (c)  $|x + y| \leq |x| + |y|$ .

**Remarks and examples 2.2.** (a) Clearly, an absolute value on a field defines a metric on it.

We shall always omit from consideration the *trivial absolute value* which is  $\equiv 1$  on  $K^*$ .

*Easy exercise:* On a finite field, show that the only absolute value is the trivial one. What does this give in relation to proposition 1.6?

(b)  $|\cdot|$  is called a *non-archimedean absolute value* if

$$|x + y| \leq \text{Max}(|x|, |y|).$$

This is stronger than the property 2.1(c).

*Trivial exercise:* Why is the word non-archimedean used here?

An absolute value which is not non-archimedean is called archimedean!

(c) If  $v$  is a discrete valuation on  $K$ , then for any fixed positive  $\lambda < 1$ , the prescription  $|x| = \lambda^{v(x)}$  gives a non-archimedean absolute value. Note that the value group  $|K^*|$  is discrete in  $\mathbf{R}^{\geq 0}$ .

*Exercise:* An absolute value on a field  $K$  has a value group  $|K^*|$  which is discrete if, and only if, it arises from a discrete valuation on  $K$ . (*Hint:* If  $|K^*|$  is discrete, choose the maximal element  $\lambda \in |K^*| \cap (0, 1)$ .)

If  $|\cdot|$  is a discrete absolute value on  $K$ , one notes that the corresponding valuation ring and its maximal ideal are, respectively,  $\{x \in K : |x| \leq 1\}$  and  $\{x \in K : |x| < 1\}$ . A generator of  $P$  is often called a *uniformising parameter*.

(d) If  $K$  is any field and  $\sigma : K \rightarrow \mathbf{C}$  any embedding, then  $|x|_\sigma := |\sigma(x)|$  defines a nontrivial absolute value on  $K$ . Here the right side has the usual absolute value on  $\mathbf{C}$ . This is archimedean.

(e) The square of the usual absolute value on  $\mathbf{C}$  is *not* an absolute value. However, if  $|\cdot|$  is a non-archimedean absolute value on a field  $K$ , so is  $|\cdot|^t$  for any positive real  $t$ .

**Definition 2.3.** Two absolute values  $|\cdot|_1$  and  $|\cdot|_2$  on  $K$  are said to be *equivalent* if  $\exists t > 0$  such that  $|x|_1 = |x|_2^t$  for all  $x \in K$ .

**Exercise:** Two absolute values are equivalent if, and only if, they define equivalent topologies.

**2.4. Product formula over  $\mathbf{Q}$ .** Let us apply the above generalities to  $\mathbf{Q}$ . We have the archimedean absolute value  $|\cdot|_\infty$  coming from the inclusion of  $\mathbf{Q}$  in  $\mathbf{R}$ . For each prime number  $p$ , we have the  $p$ -adic absolute value which we normalise as follows. Define  $|p|_p = 1/p$  i.e., we have taken  $\lambda = 1/p$  in

2.2(c). Then, we have, for each  $x \in \mathbf{Q}^*$ ,

$$|x|_\infty \prod_p |x|_p = 1.$$

That this is a product formula analogous to 1.6(c) for function fields is justified by the following easy result:

**Theorem (Ostrowski) 2.5.** *Any non-trivial absolute value on  $\mathbf{Q}$  is equivalent exactly to one of  $|\cdot|_\infty$  or  $|\cdot|_p$  for some prime  $p$ .*

**Sketch of proof.** Suppose  $|\cdot|$  is any absolute value. If  $|n| \leq 1$  for all integers  $n$ , it is easy to prove that  $|\cdot| = |\cdot|_p$  for some prime  $p$ . This is just as in the proof of 1.6. Now, suppose that there is a positive integer  $n$  with  $|n| > 1$ . Write  $|n| = |n|_\infty^t = n^t$  for some  $t > 0$ . Use the  $n$ -adic expansion to show this holds (with the same  $t$ ) for any integer in place of  $n$ .

**Exercise 2.6.** (a) *An absolute value on a field  $K$  is non-archimedean if, and only if,  $\mathbf{Z}_K$  is bounded.*

(b) *If  $\text{Char}(K) > 0$ , then any absolute value on  $K$  is non-archimedean.*

(c) *Any discrete absolute value is non-archimedean.*

(d) *The restriction of a nontrivial absolute value on a number field to  $\mathbf{Q}$  is again nontrivial.*

(e) *An absolute value  $|\cdot|$  is non-archimedean if, and only if,  $|z| < 1$  implies that  $|1+z| < 1$ .*

**Corollary 2.7.** *Any nontrivial absolute value on an algebraic number field  $K$  is equivalent to exactly one of the archimedean ones coming from the various embeddings of  $K$  in  $\mathbf{C}$  or to a discrete one coming from a prime ideal of  $\mathcal{O}_K$ .*

**Proof.** This follows from 1.5, 2.5 and 2.6(d).

**Remarks 2.8.** The non-archimedean absolute values have properties which look strange in the first instance as we are used to the usual notion of absolute value coming from the reals which is archimedean. For instance, a series converges if, and only if, its  $n$ -th term tends to 0 (!) Any triangle is isosceles (!) Every point inside a circle is its centre (!) etc.

### § 3. Completions

**Definition 3.1.** Let  $(K, |\cdot|)$  be a field with an absolute value. A *completion* of  $(K, |\cdot|)$  is an absolute-valued field  $(L, |\cdot|_L)$  which is complete as a metric space and has the property that there is some embedding  $i : K \rightarrow L$  with the image of  $K$  dense and  $|x| = |i(x)|_L$  for  $x \in K$ .

**Proposition 3.2.** *Each  $(K, |\cdot|)$  has a completion. Further, if  $(L, |\cdot|)$  and  $(L', |\cdot|')$  are two completions where  $i : K \rightarrow L$  and  $i' : K \rightarrow L'$  are corresponding embeddings, then there is an isomorphism  $\sigma : (L, |\cdot|) \rightarrow (L', |\cdot|')$  of absolutely-valued fields such that  $i' = \sigma \circ i$ .*

The proof will not be given here but the argument is entirely analogous to the construction of the reals from the rationals in terms of Cauchy sequences.

**Corollary 3.3.** *Let  $(K, |\cdot|)$  be an absolutely-valued field and  $(\hat{K}, |\cdot|_0)$  its completion. Then,  $|\cdot|$  is non-archimedean if, and only if,  $|\cdot|_0$  is so. Moreover, in this case, the value groups of  $K$  and  $\hat{K}$  are the same.*

**Proof.** The proof is a direct consequence of the construction of  $\hat{K}$ .

*Exercise:* Prove this without using the construction.

**Theorem 3.4. (Gelfand-Tornheim-Ostrowski)** *Any field  $k$  which is complete with respect to an archimedean absolute value is isomorphic to  $\mathbf{R}$  or  $\mathbf{C}$  as absolutely-valued fields.*

**Proof.** For a proof, see Cassels' *Local fields*.

**Proposition 3.5. (Series expansion)** *Suppose  $(k, |\cdot|)$  is complete with respect to a discrete absolute value. Denote by  $A$  and  $P$  the corresponding valuation ring and its maximal ideal. Fix a set of representatives  $\Sigma$  in  $A$  for the residue field  $A/P$ . Then, for any uniformising parameter  $\pi$ , elements  $\alpha$  of  $k$  admit Laurent series expansions of the form  $\sum_{i=-n}^{\infty} a_i \pi^i$  where the 'digits'  $a_i \in \Sigma$  of  $\alpha$  are uniquely determined.*

**Proof**

For any  $\alpha \in k^*$ , one has  $\pi^n \alpha \in A$  for some  $n$ . So, it suffices to show that each  $\alpha \in A$  has an expansion as claimed. By the very definition of  $\Sigma$ , there is  $a_0 \in \Sigma$  such that  $\alpha - a_0 \in P$ . So,  $\alpha = a_0 + \pi \alpha_1$ . Continuing with  $\alpha_1$  and so on, one gets a series expansion. It makes sense as the  $n$ -th term tends to 0. Uniqueness is easy to prove.

**Example 3.6.** Look at the completion  $\mathbf{Q}_p$  of  $\mathbf{Q}$  with the  $p$ -adic absolute value. Its valuation ring is usually denoted by  $\mathbf{Z}_p$ . One calls  $\mathbf{Q}_p$  and  $\mathbf{Z}_p$  the  $p$ -adic numbers and the  $p$ -adic integers respectively. Note that  $p$  is a uniformising parameter and  $\Sigma$  can be taken to be the finite set  $\{0, 1, \dots, p-1\}$ . Thus, every  $p$ -adic number has a unique expansion as  $\sum_{i=-n}^{\infty} a_i p^i$  where its 'digits'  $a_i$  are between 0 and  $p-1$ . Note the analogy with the decimal expansions of real numbers. The only difference here is that there are infinitely

many positive powers of  $p$  and only finitely many negative powers. So, it is worthwhile to think of  $p$  as  $1/10$ .

**Lemma 3.7.** *Suppose  $(k, |\cdot|)$  is complete with respect to a discrete absolute value. Denote by  $A$  and  $P$  the corresponding valuation ring and its maximal ideal. Then,  $k$  is locally compact if, and only if,  $A$  is compact which is again if, and only if,  $A/P$  is finite.*

**Proof.** If  $A$  is compact, then evidently  $k$  is locally compact since  $k = \cup_n \pi^{-n}A$ . Assume  $k$  is locally compact. Let  $C$  be a compact neighbourhood of  $0$ . Then, for large enough  $n$ ,  $\pi^n A \subseteq C$ . As  $\pi^n A$  is closed, it is compact also. Thus, we have shown the equivalence of compactness of  $A$  and local compactness of  $k$ .

If  $A$  is compact, then from the openness of  $P$  in  $k$ , we get that  $A/P$  is compact as well as discrete and therefore, finite. To prove finally that the finiteness of  $A/P$  implies the compactness of  $A$ , it suffices to prove sequential compactness as  $A$  is a metric space. Let  $\{a^{(n)}\}$  be any infinite sequence in  $A$ . Write the series expansion  $a^{(n)} = \sum_{r \geq 0} a_{n,r} \pi^r$ . As  $n$  varies, the elements  $a_{n,0}$  run over a finite set (viz., a set of representatives of  $A/P$ ). Thus, they are all equal for infinitely many  $n$ . Replace the original sequence with a subsequence for which the terms  $a_{n,0}$  are all the same, say  $a_0$ . Proceeding this way, one finally concludes that there is a subsequence of the original sequence which converges to an element of  $A$ .

**Hensel's lemma 3.8.** *Suppose  $(k, |\cdot|)$  is complete with respect to a discrete absolute value. Denote by  $A$  and  $P$  the corresponding valuation ring and its maximal ideal. If  $f(X) \in A[X]$  is a polynomial which factors modulo  $P$  into two coprime polynomials  $\bar{g}, \bar{h}$ , then there exist  $g, h \in A[X]$  such that  $f = gh$  and  $\deg(g) = \deg(\bar{g})$ .*

**Exercises 3.9.** (a) *Prove Hensel's lemma.*

(b) *Find the order and structure of  $\mathbf{Q}_p^*/(\mathbf{Q}_p^*)^2$ .*

(c) *Prove that the only automorphism of  $\mathbf{Q}_p$  is the identity.*

Let  $K$  be an algebraic number field. Start with a discrete absolute value on it (this will come from a prime ideal). Let  $A$  be the corresponding valuation ring and  $P$  its maximal ideal. If  $L$  is a finite extension of  $K$  and  $B$  the integral closure of  $A$  in  $L$ , one can write  $PB = P_1^{e_1} \cdots P_g^{e_g}$ . Let  $Q$  denote one of the  $P_i$ 's. Let  $K_P$  and  $L_Q$  denote the completions of  $K$  and  $L$  with respect to the  $P$ -adic and the  $Q$ -adic absolute values. If  $\hat{A}, \hat{B}$  denote their valuation rings and  $\hat{P}, \hat{Q}$  their maximal ideals, it is routine to prove:

**Exercise 3.10.** (a)  $\hat{P} = P\hat{A}, \hat{Q} = Q\hat{B}$ ,

(b)  $\hat{P}\hat{B} = \hat{Q}^{e_1}$ ,

(c)  $[L_Q : K_P] = e_1 f_1$ .

The next proposition is crucial to many of the results to follow.

**Proposition 3.11. (Extensions of valuations over complete fields)**

Let  $(K, |\cdot|)$  be a complete field. If  $L$  is a finite extension of  $K$ , then there is exactly one absolute value on  $L$  which extends  $|\cdot|$ . Moreover,  $L$  is complete with respect to it.

**Proof.** The archimedean case is taken care of by Theorem 3.4. So, we assume that the absolute value is non-archimedean. Let us first prove the existence of an extension. Define  $|x|_L = |N_{L/K}(x)|$  for any  $x \in L$ . The first two properties are clear and we only need to prove that if  $x \in L$  satisfies  $|x|_L \leq 1$ , then  $|1+x|_L \leq 1$ . In other words, if  $|N_{L/K}(x)| \leq 1$ , then  $|N_{L/K}(1+x)| \leq 1$ . Let  $f(T) = a_0 + a_1 T + \cdots + T^n$  be the minimal polynomial of  $x$  over  $K$ . Now,  $|a_0| = |N_{L/K}(x)| \leq 1$  i.e.,  $a_0 \in A$ , the valuation ring of  $K$ . Now,  $g(T) = f(T-1)$  is clearly the minimal polynomial of  $1+x$  over  $K$ . Therefore,

$$|N_{L/K}(1+x)| = |g(0)| = |f(-1)| = |a_0 - a_1 + a_2 - \cdots|.$$

So, if we show that  $|a_i| \leq 1$ , it would follow that  $|N_{L/K}(1+x)| \leq 1$ . Suppose the contrary. Let  $a_r$  be such that  $|a_r| > 1$ , that  $|a_r| = M := \text{Max}(|a_i|)$  and that  $r$  is the maximal index  $i$  so that  $|a_i| = M$ . With this notation, we have  $a_r^{-1} \in A$  and  $a_i a_r^{-1} \in A$  for all  $i$  and  $a_i a_r^{-1} \in P$  for all  $i > r$ , where  $P$  is the maximal ideal of  $A$ . Thus, the polynomial  $a_r^{-1} f(T) \in A[X]$  reduces modulo  $P$  to the polynomial  $\bar{h}(T) = X^r +$  smaller degree terms. Applying Hensel's lemma to the factorisation  $\bar{h}(T)U(T)$  where  $U$  is the constant polynomial 1, we have  $f = h(T)u(T)$  for some lifts such that  $h(T) \bmod P$  is  $\bar{h}(T)$ . But, as  $r < n$ , this means that  $f$  is reducible, a contradiction, which implies that all  $a_i \in A$ . This proves the existence.

We prove the uniqueness when  $K$  is locally compact, which is the main case of interest to us. The general case is not too difficult and one can look at Cassels's book (loc. cit.). Let  $\{v_1, \dots, v_n\}$  be a  $K$ -basis of  $L$ . We claim that any extension  $|\cdot|_L$  is equivalent to the *sup-norm*  $|\cdot|_0$  with respect to this basis.

Firstly,  $|x|_L = |a_1 v_1 + \cdots + a_n v_n|_L \leq n \sup_i (|a_i|_0) |x|_0$ . Here, we haven't used the local compactness but we shall use it for the opposite implication. By the local compactness of  $K$ , there is some  $y \in L$  such that  $|y|_L = \text{Min}(|x|_L : |x|_0 = 1)$ . Now, let  $0 \neq x \in L$ . Write  $x = a_1 v_1 + \cdots + a_n v_n$ . If  $|a_r|_L = |x|_0 = \text{Max}(|a_i|_L)$ , then  $x = a_r z$  with  $|z|_0 = 1$ .

So,  $|y|_L \leq |z|_L = |x/a_r|_L = |x|_L / |a_r|_L = |x|_L / |x|_0$ . In other

words,  $|x|_0 \leq |x|_L (1/|y|_L)$ . This proves that  $| \cdot |_L$  and the sup-norm  $| \cdot |_0$  are equivalent and proves the proposition.

**Corollary 3.12. (Unramified extensions)**

Suppose  $(k, | \cdot |)$  is complete with respect to a discrete absolute value. Denote by  $A$  and  $P$  the corresponding valuation ring and its maximal ideal. Let  $l$  be a finite extension of degree  $n$  over  $k$ . Let  $f$  and  $F$  denote the residue fields of  $k, l$  respectively. Then, the association  $e \mapsto (e \cap A) \bmod P$  is a bijection from  $\{e : k \subset e \subset l \text{ and } e \text{ unramified over } k\}$  to  $\{E : f \subset E \subset F\}$ .

In particular, there is a unique (upto isomorphism) unramified extension of any degree  $d$  viz., the splitting field over  $k$  of  $X^{d^q} - X$  where  $q = \#f$ .

The proof is a consequence of Hensel's lemma (*Exercise:* What is the polynomial factorisation to which Hensel is applied?) and the fact that over finite fields there is a unique extension, upto isomorphism, of a given degree.

**Definition 3.13.** If  $| \cdot |$  is a discrete absolute value on  $k$ , an *Eisenstein polynomial* is a polynomial  $f \in k[X]$  of the form  $\sum_{i=0}^n a_i X^i$  with  $a_i \in P$  for  $i < n$ ,  $a_n$  a unit and  $a_0 \in P \setminus P^2$ . It is an easy exercise to show that such a polynomial is irreducible.

**Proposition 3.14. (Totally ramified extensions)** Suppose  $(k, | \cdot |)$  is complete with respect to a discrete absolute value. Let  $A, P, \pi$  have the usual meaning. Then, an extension of  $k$  is totally ramified if, and only if, it is obtained by attaching a root of an Eisenstein polynomial.

**Proof.** Suppose that  $\alpha$  is a root of an Eisenstein polynomial  $f(X) = \sum_{i=0}^n a_i X^i$ . Then  $\sum_{i=0}^n a_i \alpha^i = 0$  and so

$$|\alpha^n| = |a_n \alpha^n| = |\sum_{i=0}^{n-1} a_i \alpha^i| = |a_0| = |\pi|.$$

Thus,  $k(\alpha)$  is totally ramified extension of  $k$ .

Conversely, suppose  $K$  is totally ramified over  $k$  of degree  $n$ . If  $\Pi_K$  is a uniformising parameter for  $K$ , then the powers  $\Pi_K^i, i < n$ , must be linearly independent over  $k$  as total ramification forces their absolute values to be in distinct cosets of the value groups of  $k$  in  $K$ . Thus, they form a  $k$ -basis of  $K$ . Write  $\Pi_K^n + a_{n-1} \Pi_K^{n-1} + \dots + a_0 = 0$  with  $a_i \in k$ . But, the various roots of this polynomial give extensions of  $| \cdot |$  to  $K$  and must coincide by the uniqueness of such an extension. In other words, the roots of this polynomial have absolute value  $|\Pi_K|$ . As each  $a_i$  is a sum of roots, we have  $|a_i| < 1$  and  $|a_0| = |\text{product of the roots}| = |\Pi_K^n| = |\pi|$ . In other words, the polynomial  $\sum a_i X^i$  is an Eisenstein polynomial. The proposition is proved.

**Krasner's lemma 3.15.** Suppose  $(k, | \cdot |)$  is complete with respect to a discrete absolute value. Let  $\alpha, \beta$  be algebraic over  $k$  and suppose that  $\alpha$  is



separable over  $k(\beta)$ . Assume that  $\beta$  is ‘very close’ to  $\alpha$  in the sense that  $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$  for all  $k$ -isomorphisms of  $k(\alpha)$ . Then,  $k(\alpha) \subseteq k(\beta)$ .

**Proof.** By the separability assumption, it suffices to show the conclusion that each  $k(\beta)$ -isomorphism  $\tau$  of  $k(\alpha, \beta)$  fixes  $\alpha$ . Note that any such  $\tau$  gives a new absolute value on  $k(\alpha, \beta)$  by  $|x|_\tau = |\tau(x)|$ . By the uniqueness, this gives that the hypothesis implies  $|\tau(\beta - \alpha)| < |\sigma(\alpha) - \alpha|$ . That is,  $|\beta - \tau(\alpha)| < |\sigma(\alpha) - \alpha|$ . So,  $|\tau(\alpha) - \alpha| < |\sigma(\alpha) - \alpha|$ . In other words,  $\tau(\alpha) = \alpha$ . The lemma follows.

**Definitions and remarks 3.16 (continuity of roots)** With  $k$  as before, let  $f(X) \in k[X]$  be a monic polynomial of degree  $n$  which factorises as  $\prod_{i=1}^t (X - a_i)^{r_i}$  in the algebraic closure of  $k$ . Let us define  $|f|$  to be the maximum of the absolute values of the coefficients of  $f$ . Clearly, if  $g \in k[X]$  is close to  $f$  i.e., if  $|f - g|$  is small, then for any root  $b$  of  $g$ , the value  $|f(b)| = |f(b) - g(b)|$  is small. In other words, as  $g$  comes close to  $f$ , any root of  $g$  comes close to some root of  $f$ . It is an easy exercise to see that if  $g$  is sufficiently close to  $f$  and if  $b_1, \dots, b_r$  are the roots (with multiplicity) of  $g$  which come close to a root  $a_i$  of  $f$ , then  $r = r_i$ .

**Corollary 3.17.** *With  $k, f$  as above, if  $f$  is irreducible and separable, then any monic  $g$  which is sufficiently close to  $f$  is irreducible too. Moreover, if  $b$  is a root of  $g$  coming close to a root  $a$  of  $f$ , then  $k(a) = k(b)$  if  $f, g$  are sufficiently close.*

**Proof.** The proof is immediate from 3.15 and 3.16.

**Corollary 3.18.** *Any finite extension  $k = \mathbf{Q}_p(\alpha)$  arises as the closure of a finite extension  $K$  of  $\mathbf{Q}$  where  $[k : \mathbf{Q}_p] = [K : \mathbf{Q}]$ .*

**Proof.** The proof is immediate from choosing a polynomial  $g \in \mathbf{Q}[X]$  which is close in the  $p$ -adic topology to the minimal polynomial of  $\alpha$  over  $\mathbf{Q}_p$  and applying 3.17.

Now, we can prove a remarkable theorem (contrast it with the situation of number fields !)

**Theorem 3.19.** *Any finite extension  $k$  of  $\mathbf{Q}_p$  has only finitely many extension fields (upto isomorphism) of a given degree.*

**Proof.** As there is a unique unramified extension of a given degree over any finite extension of  $\mathbf{Q}_p$  by Corollary 3.12, it suffices to prove the finiteness of the number of totally ramified extensions of a given degree  $n$ . In this case, Proposition 3.14 tells us that any such extension arises from an Eisenstein polynomial of degree  $n$ . As such a polynomial has a unit as the top coefficient and other coefficients coming from the maximal ideal  $P$ , we have a mapping

from the product  $U \times P \times \cdots \times P$  to the set of totally ramified extensions of degree  $n$ . Here, the factor  $P$  is repeated  $n - 1$  times. The crucial observation is that by 3.17, a neighbourhood of a point in this product determines fields which are all isomorphic. By the compactness of  $U$  and  $P$ , the theorem follows.

### REFERENCES

1. J. W. S. Cassels, *Global Fields, Chapter II in Algebraic Number Theory*, Cassels and Fröhlich Eds., Academic Press (1967).
2. J. W. S. Cassels, *Local Fields*, LMS Student Series 3, Cambridge University Press (1986).
3. Serge Lang, *Algebraic Number Theory*, Springer, Second Edition (1994).

B. Sury  
Indian Statistical Institute,  
Bangalore 560 059  
*e-mail*: bsury@isibang.ac.in