CHAPTER III

EXTENSIONS OF ABSOLUTE VALUES

1. Norm and Trace

Let k be a field and E a vector space of dimension N over k. We write $\mathrm{End}_k(E)$ for the ring of k–linear endomorphisms of E and $\mathrm{Aut}_k(E) = \mathrm{End}_k(E)^\times$ for the multiplicative group of k–linear automorphisms of E. If $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_N$ is an ordered basis for E as a vector space over k, then this basis determines a unique ring isomorphism from $\mathrm{End}_k(E)$ onto the ring $M(N,k)$ of $N \times N$ matrices with elements in k. The restriction of this map to $\mathrm{Aut}_k(E)$ is an isomorphism from the multiplicative group $\mathrm{Aut}_k(E)$ onto $GL(N,k) = M(N,k)^\times$. In particular, T in $\mathrm{End}_k(E)$ is mapped to the matrix (t_{mn}), where

$$T(\boldsymbol{b}_n) = \sum_{m=1}^{N} t_{mn}\boldsymbol{b}_m \quad \text{for each } n = 1, 2, \ldots, N. \tag{1.1}$$

If

$$\boldsymbol{\alpha} = \sum_{n=1}^{N} \alpha_n \boldsymbol{b}_n$$

is an element of E expressed as a linear combination of basis vectors, then we have

$$\begin{aligned} T\Big\{\sum_{n=1}^{N} \alpha_n \boldsymbol{b}_n\Big\} &= \sum_{n=1}^{N} \alpha_n \Big\{\sum_{m=1}^{N} t_{mn}\boldsymbol{b}_m\Big\} \\ &= \sum_{m=1}^{N} \Big\{\sum_{n=1}^{N} t_{mn}\alpha_n\Big\}\boldsymbol{b}_m. \end{aligned}$$

This shows that the action of T on E corresponds to multiplication of the column vector $\boldsymbol{\alpha}$ on the left by the matrix (t_{mn}). If U is a second element of $\mathrm{End}_k(E)$, if

$$U(\boldsymbol{b}_n) = \sum_{m=1}^{N} u_{mn}\boldsymbol{b}_m \quad \text{for each } n = 1, 2, \ldots, N,$$

then the matrix corresponding to the composition of endomorphisms $T \circ U$ is the product matrix $(t_{mn})(u_{mn})$.

Let $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_N$ be a second ordered basis for E as a vector space over k. Then there exists a matrix $V = (v_{mn})$ in $GL(N, k)$ such that

$$\boldsymbol{c}_n = \sum_{m=1}^{N} v_{mn} \boldsymbol{b}_m \quad \text{for each } n = 1, 2, \ldots, N.$$

With respect to the ordered basis $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_N$ the matrix of T is easily seen to be

$$V^{-1}(t_{mn})V. \tag{1.2}$$

Therefore we define

$$\det : \mathrm{End}_k(E) \to k, \quad \text{and} \quad \mathrm{trace} : \mathrm{End}_k(E) \to k,$$

by

$$\det(T) = \det\{(t_{mn})\}, \quad \text{and} \quad \mathrm{trace}(T) = \mathrm{trace}\{(t_{mn})\}. \tag{1.3}$$

It follows from (1.2) that these maps do not depend on the choice of basis, hence they are well defined on $\mathrm{End}_k(E)$. We also define a map

$$\chi : \mathrm{End}_k(E) \to k[x]$$

as follows: if T is an element of $\mathrm{End}_k(E)$ then $\chi_T(x)$ is the polynomial in $k[x]$ given by

$$\chi_T(x) = \det(x\mathbf{1}_N - T),$$

where $\mathbf{1}_N$ is the $N \times N$ identity matrix. The polynomial $\chi_T(x)$ is called the *characteristic polynomial* of T. By selecting a basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_N$ and using (1.1), we find that $\chi_T(x)$ has the form

$$\chi_T(x) = x^N - \mathrm{trace}(T)x^{N-1} + \cdots + (-1)^N \det(T). \tag{1.4}$$

If T is in $\mathrm{End}_k(E)$ and $f(x)$ is a polynomial in $k[x]$ then we can form the element $f(T)$ in $\mathrm{End}_k(E)$. In particular, using the characteristic polynomial $\chi_T(x)$ we can form the element $\chi_T(T)$. The map $f(x) \to f(T)$ is clearly a ring homomorphism from $k[x]$ into $\mathrm{End}_k(E)$. It follows that E is a left $k[x]$–module with respect to the operation

$$(f(x), \boldsymbol{b}) \to f(x)\boldsymbol{b} = f(T)\boldsymbol{b}.$$

Also, it is clear that the annihilator

$$\mathrm{Ann}(T) = \{f(x) \in k[x] : f(T)\boldsymbol{b} = \mathbf{0} \text{ for all } \boldsymbol{b} \in E\}$$

is a proper ideal in $k[x]$, and so generated by a unique monic polynomial $\mu_T(x)$ of positive degree. The polynomial $\mu_T(x)$ is called the *minimal polynomial* for the endomorphism T. We use these observations to prove the following classical result.

THEOREM 1.1 (CAYLEY-HAMILTON). *If T is an element of $\mathrm{End}_k(E)$ then $\chi_T(T) = \mathbf{0}_N$, where $\mathbf{0}_N$ is the zero endomorphism in $\mathrm{End}_k(E)$. Moreover, the minimal polynomial $\mu_T(x)$ divides the characteristic polynomial $\chi_T(x)$ in $k[x]$.*

PROOF. Let $\delta_{mn} = 1_k$ if $m = n$, and $\delta_{mn} = 0_k$ if $m \neq n$. Define

$$A = \big(a_{mn}(x)\big), \quad \text{where} \quad a_{mn}(x) = \delta_{mn}x - t_{mn},$$

so that A is an $N \times N$ matrix with entries in the ring $k[x]$. Then the identity (1.1) can be written as

$$\mathbf{0} = \sum_{m=1}^{N} (\delta_{mn}T - t_{mn})\boldsymbol{b}_m = \sum_{m=1}^{N} a_{mn}(T)\boldsymbol{b}_m \quad \text{for} \quad n = 1, 2, \ldots, N. \tag{1.5}$$

Let A_{rs} be the $(N-1) \times (N-1)$ submatrix obtained from A be removing the r-th row and the s-th column. Define the $N \times N$ matrix

$$A' = \big(a'_{rs}(x)\big) \quad \text{where} \quad a'_{rs}(x) = (-1)^{r+s} \det A_{sr}.$$

Then A and A' are $N \times N$ matrices with entries in the ring $k[x]$, and satisfy

$$AA' = (\det A)\mathbf{1}_N = (\chi_T(x))\mathbf{1}_N.$$

That is, we have

$$\sum_{l=1}^{N} a_{ml}(x)a'_{ln}(x) = \delta_{mn}\chi_T(x)$$

for each pair of integers $m = 1, 2, \ldots, N$ and $n = 1, 2, \ldots, N$. It follows that

$$\begin{aligned} \chi_T(x)\boldsymbol{b}_n &= \sum_{m=1}^{N} \delta_{mn}\chi_T(x)\boldsymbol{b}_m \\ &= \sum_{m=1}^{N} \Big(\sum_{l=1}^{N} a_{ml}(x)a'_{ln}(x)\Big)\boldsymbol{b}_m \\ &= \sum_{l=1}^{N} a'_{ln}(x)\Big(\sum_{m=1}^{N} a_{ml}(x)\boldsymbol{b}_m\Big) \end{aligned} \tag{1.6}$$

for each $n = 1, 2, \ldots, N$. Combining (1.5) and (1.6) we get

$$\chi_T(T)\boldsymbol{b}_n = \sum_{l=1}^{N} a'_{ln}(T)\Big(\sum_{m=1}^{N} a_{ml}(T)\boldsymbol{b}_m\Big) = \mathbf{0},$$

in E for each $n = 1, 2, \ldots, N$. That is, $\chi_T(T)$ is the zero endomorphism on E. This shows that $\chi_T(x)$ belongs to the the annihilator $\mathrm{Ann}(T)$. As the annihilator is a principal ideal generated by $\mu_T(x)$, the last assertion of the theorem is obvious.

Now assume that E is a field and so E/k is a finite extension of fields of degree N. Then each element β in E defines a k–linear endomorphism of E given by multiplication by β. That is, if β is in E then there exists a corresponding element T_β in $\mathrm{End}_k(E)$ such that

$$T_\beta(\gamma) = \beta\gamma \quad \text{for all} \quad \gamma \in E. \tag{1.7}$$

If $\beta \neq 0$ then T_β is in $\mathrm{Aut}_k(E)$. Clearly the map $\beta \to T_\beta$ is an embedding of the field E into the endomorphism ring $\mathrm{End}_k(E)$, and $\beta \to T_\beta$ is an injective homomorphism of the multiplicative group $k^\times$ into the group $\mathrm{Aut}_k(E)$. We define maps

$$\mathrm{Norm}_{E/k} : E^\times \to k^\times \quad \text{and} \quad \mathrm{Trace}_{E/k} : E \to k$$

by

$$\mathrm{Norm}_{E/k}(\beta) = \det(T_\beta) \quad \text{and} \quad \mathrm{Trace}_{E/k}(\beta) = \mathrm{trace}(T_\beta). \tag{1.8}$$

It follows that $\mathrm{Norm}_{E/k}$ is a homomorphism of multiplicative groups, and $\mathrm{Trace}_{E/k}$ is a homomorphism of additive groups.

As E/k is a finite and therefore algebraic extension, each element β in E is a root of a unique, monic, irreducible polynomial $f_\beta(x)$ in $k[x]$. The polynomial $f_\beta(x)$ is the *minimal polynomial* of β over k. Then $k \subseteq k(\beta) \subseteq E$ and the degree of the extension $k(\beta)/k$ is also the degree of the polynomial f_β. We write $[k(\beta) : k]$ for this degree, it is the dimension of $k(\beta)$ as a vector space over k.

Lemma 1.2. *Assume that E/k is a finite extension of fields and let β be an element of E. Write $f_\beta(x)$ for the minimal polynomial of β over k and let T_β be the unique element in* $\mathrm{End}_k(E)$ *that satisfies* (1.7)*. Then the minimal polynomial for T_β is given by*

$$\mu_{T_\beta}(x) = f_\beta(x), \tag{1.9}$$

and the characteristic polynomial of T_β is given by

$$\chi_{T_\beta}(x) = \det(x\mathbf{1}_N - T_\beta) = f_\beta(x)^R, \tag{1.10}$$

where $R = [E : k(\beta)]$.

Proof. We will prove (1.9) and leave the proof of (1.10) as an exercise. Because E is a field we have

$$\mathrm{Ann}(T_\beta) = \{g(x) \in k[x] : g(\beta)\gamma = 0 \text{ for all } \gamma \in E\} = \{g(x) \in k[x] : g(\beta) = 0\}.$$

Therefore $f_\beta(x)$ is a monic irreducible polynomial in $\mathrm{Ann}(T_\beta)$. As $\mathrm{Ann}(T_\beta)$ is a principal ideal generated by the monic polynomial $\mu_{T_\beta}(x)$, the identity (1.9) clearly follows.

LEMMA 1.3. *Assume that E/k is a finite extension of fields and let β be an element of E. Assume that the minimal polynomial $f_\beta(x)$ splits into linear factors in a field extension K/k, where $k \subseteq E \subseteq K$, as*

$$f_\beta(x) = \prod_{q=1}^{Q}(x - \beta_q).$$

Then we have

$$\mathrm{Norm}_{E/k}(\beta) = \Big\{\prod_{q=1}^{Q}\beta_q\Big\}^R = (-1)^{QR} f_\beta(0)^R, \tag{1.11}$$

and

$$\mathrm{Trace}_{E/k}(\beta) = R\sum_{q=1}^{Q}\beta_q, \tag{1.12}$$

where $R = [E : k(\beta)]$.

PROOF. Because $Q = [k(\beta) : k]$, it is obvious that $QR = [E : k] = N$. Using (1.4) and (1.10) we find that

$$\begin{aligned}\chi_{T_\beta}(x) &= x^N - \mathrm{Trace}_{E/k}(\beta)x^{N-1} + \cdots + (-1)^N\,\mathrm{Norm}_{E/k}(\beta)\\ &= f_\beta(x)^R\\ &= x^{QR} - \Big\{R\sum_{q=1}^{Q}\beta_q\Big\}x^{QR-1} + \cdots + (-1)^{QR}\Big\{\prod_{q=1}^{Q}\beta_q\Big\}^R.\end{aligned} \tag{1.13}$$

Both identities (1.11) and (1.12) follow from (1.13) be equating coefficients.

Exercises

1.1 Let T and U be elements of $\mathrm{End}_k(E)$. Prove that $\mathrm{trace}(T + U) = \mathrm{trace}\,T + \mathrm{trace}\,U$ and $\mathrm{trace}(T \circ U) = \mathrm{trace}(U \circ T)$.

1.2 Prove the identity (1.4).

1.3 Let $k = \mathbb{R}$ and $E = \mathbb{C}$. Find the matrix of an endomorphism T in $\mathrm{End}_{\mathbb{R}}(\mathbb{C})$ with respect to the basis $\{1, i\}$. If $\beta = \beta_1 + \beta_2 i$ is in $\mathbb{C}$, find the matrix of T_β with respect to the basis $\{1, i\}$. Compute both $\mathrm{Norm}_{\mathbb{C}/\mathbb{R}}(\beta)$ and $\mathrm{Trace}_{\mathbb{C}/\mathbb{R}}(\beta)$.

1.4 Prove the identity (1.10).

2. Norms on Vector Spaces over Complete Fields

We assume that K is a field with a nontrivial absolute value $|\ |$, that K is complete, and that E is a finite dimensional vector space over K. In this setting the absolute value on K can be extended to a vector space norm on E. More precisely, we say that a function $\|\ \| : E \to [0, \infty)$ defines a *norm* on E with respect to the absolute value $|\ |$ on K if it satisfies the following conditions:

(i) $\|\boldsymbol{x}\| = 0$ if and only if $\boldsymbol{x} = \mathbf{0}$ in E,

(ii) $\|\alpha\boldsymbol{x}\| = |\alpha|\|\boldsymbol{x}\|$ for scalars α in K and vectors $\boldsymbol{x}$ in E,

(iii) $\|\boldsymbol{x} + \boldsymbol{y}\| \le \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$ for all $\boldsymbol{x}$ and $\boldsymbol{y}$ in E.

Obviously a *norm* in this context is different from the map defined in (1.8).

When we work with only one absolute value on K then such a function $\|\ \|$ on E is called simply a norm. If $\|\ \|$ is a norm on E then it follows immediately from the definition that

$$(\boldsymbol{x}, \boldsymbol{y}) \to \|\boldsymbol{x} - \boldsymbol{y}\|$$

defines a metric. Thus $\|\ \|$ induces a metric topology in the vector space E.

THEOREM 2.1. *Suppose that both $\|\ \|_1$ and $\|\ \|_2$ are norms on E with respect to the nontrivial absolute value $|\ |$ on K. Then there exist positive constants C_1 and C_2 such that*

$$C_1\|\boldsymbol{x}\|_1 \le \|\boldsymbol{x}\|_2 \le C_2\|\boldsymbol{x}\|_1 \tag{2.1}$$

for all $\boldsymbol{x}$ in E. Moreover, the norms $\|\ \|_1$ and $\|\ \|_2$ induce the same metric topology in E, and E is a complete metric space.

PROOF. We argue by induction on the dimension of E over K. The result is trivial for vector spaces of dimension 1 over K. Therefore we assume that the theorem holds for all vector spaces of dimension $N - 1$, and we assume that E has dimension N over K. Let $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_N$ be a basis for E as a vector space over K. Then define subspaces

$$E'_m = \operatorname{span}_K\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{m-1}, \boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_N\} \quad \text{for} \quad m = 1, 2, \ldots, N.$$

It follows that $E'_m \subseteq E$ is an $N - 1$ dimensional subspace for each $m = 1, 2, \ldots, N$. Define a map $\|\ \|_\infty : E \to [0, \infty)$ by

$$\Big\| \sum_{n=1}^{N} x_n \boldsymbol{b}_n \Big\|_\infty = \max\{|x_n| : n = 1, 2, \ldots, N\}.$$

Then $\|\ \|_\infty$ is clearly a norm on E with respect to the absolute value $|\ |$ on K. Of course $\|\ \|_\infty$, $\|\ \|_1$ and $\|\ \|_2$ are also norms when restricted to one of the subspaces E'_m. By

the inductive hypothesis, each subspace E'_m is complete in the common metric topology induced by $\| \|_\infty$, $\| \|_1$ and $\| \|_2$. In particular, each subspace $E'_m \subseteq E$ is a closed subset of E when E is given the metric topology induced by $\| \|_1$. The translate $E'_m + \boldsymbol{b}_m$ is also closed in E and does not contain the vector $\mathbf{0}$. Hence there exists a positive real number δ_m such that

$$(E'_m + \boldsymbol{b}_m) \cap \{\boldsymbol{x} \in E : \|\boldsymbol{x}\|_1 < \delta_m\}$$

is empty.

Now define positive real numbers

$$A_1 = \min\{\delta_m : m = 1, 2, \ldots, N\} \quad \text{and} \quad B_1 = \sum_{n=1}^{N} \|\boldsymbol{b}_n\|_1.$$

We note that A_1 and B_1 depend on $\| \|_1$ and on the choice of basis. If

$$\boldsymbol{x} = \sum_{n=1} x_n \boldsymbol{b}_n \neq \mathbf{0}$$

we select m so that $\|\boldsymbol{x}\|_\infty = |x_m|$. Then the vector $x_m^{-1}\boldsymbol{x}$ belongs to $E'_m + \boldsymbol{b}_m$ and we have

$$A_1 \leq \delta_m \leq \|x_m^{-1}\boldsymbol{x}\|_1 = |x_m|^{-1}\|\boldsymbol{x}\|_1. \tag{2.2}$$

From (2.2) we conclude that

$$\begin{aligned} A_1\|\boldsymbol{x}\|_\infty &= A_1|x_m| \leq \|\boldsymbol{x}\|_1 \\ &= \Big\| \sum_{n=1}^{N} x_n \boldsymbol{b}_n \Big\|_1 \\ &\leq \sum_{n=1}^{N} |x_n| \|\boldsymbol{x}_n\|_1 \leq B_1\|\boldsymbol{x}\|_\infty. \end{aligned} \tag{2.3}$$

Of course (2.3) is trivial if $\boldsymbol{x} = \mathbf{0}$. In a similar manner we find that there exist positive real numbers A_2 and B_2 such that

$$A_2\|\boldsymbol{x}\|_\infty \leq \|\boldsymbol{x}\|_2 \leq B_2\|\boldsymbol{x}\|_\infty \tag{2.4}$$

for all $\boldsymbol{x}$ in E. We set $C_1 = A_2 B_1^{-1}$ and $C_2 = A_1^{-1} B_2$. Then (2.1) follows easily from (2.3) and (2.4).

Let $U \subseteq E$ be a nonempty open set in the $\| \|_1$–topology. Then for each point $\boldsymbol{\xi}$ in U there exists a positive real number ϵ such that

$$\{\boldsymbol{x} \in E : \|\boldsymbol{\xi} - \boldsymbol{x}\|_1 < \epsilon\} \subseteq U.$$

Using (2.1) we find that

$$\{\boldsymbol{x} \in E : \|\boldsymbol{\xi} - \boldsymbol{x}\|_2 < C_2^{-1}\epsilon\} \subseteq U.$$

Hence U is also an open set in the $\| \ \|_2$–topology. By symmetry the two metric topologies are the same.

Finally, we must show that E is a complete metric space. From what we have already established it suffices to show that E is complete with respect to the metric topology induced by $\| \ \|_\infty$. Let $\{\boldsymbol{x}_m\}_{m=1}^\infty$ be a $\| \ \|_\infty$–Cauchy sequence and write

$$\boldsymbol{x}_m = \sum_{n=1}^N x_{mn}\boldsymbol{b}_n.$$

Then for each n we have

$$|x_{mn} - x_{ln}| \leq \|\boldsymbol{x}_m - \boldsymbol{x}_l\|_\infty.$$

It follows that for each n the sequence $\{x_{mn}\}_{m=1}^\infty$ is $| \ |$–Cauchy in K. As K is complete, each of the limits

$$\lim_{m\to\infty} x_{mn} = y_n$$

exists in K. It follows that

$$\lim_{m\to\infty} \boldsymbol{x}_m = \lim_{m\to\infty} \sum_{n=1}^N x_{mn}\boldsymbol{b}_n = \sum_{n=1}^N y_n\boldsymbol{b}_n$$

in E. This proves the theorem.

Now suppose that E is a field and $\| \ \|$ on E extends the absolute value $| \ |$ on K. It follows that $\| \ \|$ is also a norm on the vector space E over K. In this special case the conclusion (2.1) can be improved.

Corollary 2.2. *Assume that E is a field and so E/K is a finite extension of fields of degree N. If $\| \ \|_1$ and $\| \ \|_2$ are both absolute values on E that extend the absolute value $| \ |$ on K, then*

$$\|\beta\|_1 = \|\beta\|_2 \quad \textit{for all} \quad \beta \in E.$$

Proof. By Theorem 2.1 the absolute values $\| \ \|_1$ and $\| \ \|_2$ induce the same topology in E. By Theorem 1.1 of Chapter 2, there exists a positive constant θ such that

$$\|\beta\|_1^\theta = \|\beta\|_2 \quad \text{for all} \quad \beta \in E.$$

As $\|\beta\|_1 = \|\beta\|_2 = |\beta|$ for β in K, and $| \ |$ is not trivial on K, we conclude that $\theta = 1$.

3. Hensel's Lemma Revisited

In this section we assume that K is a field with a nontrivial, non-archimedean absolute value $|\ |$ and we assume that $(K, |\ |)$ is complete. We write

$$O_K = \{\alpha \in K : |\alpha| \leq 1\}$$

for the associated local ring, and

$$M_K = \{\alpha \in K : |\alpha| < 1\}$$

for its maximal ideal. Then we extend the absolute value $|\ |$ on K to the polynomial ring $K[x]$ as follows. If

$$f(x) = a_0 x^N + a_{N-1} x^{N-1} + \cdots + a_N$$

is a polynomial in $K[x]$ we define

$$|f| = \max\{|a_0|, |a_1|, \ldots, |a_N|\}. \tag{3.1}$$

It will be convenient to write $\varphi : O_K \to O_K/M_K$ for the canonical homomorphism. This extends to a homomorphism $\varphi : O_K[x] \to (O_K/M_K)[x]$ by

$$\varphi\big(a_0 x^N + a_{N-1} x^{N-1} + \cdots + a_N\big) = \varphi(a_0) x^N + \varphi(a_1) x^{N-1} + \cdots + \varphi(a_N).$$

We note that f in $O_K[x]$ is in the kernel of φ if and only if $|f| < 1$. Our objective in this section is to establish the following algebraic form of Hensel's Lemma.

THEOREM 3.1 (HENSEL'S LEMMA). *Let f be a polynomial in $O_K[x]$ such that $|f| = 1$. Suppose that $\gamma(x)$ and $\eta(x)$ are relatively prime polynomials in $(O_K/M_K)[x]$, $\gamma(x)$ is a monic polynomial, and*

$$\varphi(f)(x) = \gamma(x)\eta(x). \tag{3.2}$$

Then there exist polynomials $g(x)$ and $h(x)$ in $O_K[x]$ such that

(1) $f(x) = g(x)h(x)$,
(2) $\varphi(g)(x) = \gamma(x)$ *and* $\varphi(h)(x) = \eta(x)$,
(3) $\deg g = \deg \gamma$ *and* $g(x)$ *is monic.*

PROOF. Select polynomials $g_1(x)$ and $h_1(x)$ in $O_K[x]$ so that

$$\varphi(g_1)(x) = \gamma(x), \quad \deg g_1 = \deg \gamma, \quad \varphi(h_1)(x) = \eta(x), \quad \text{and} \quad \deg h_1 = \deg \eta. \tag{3.3}$$

As $\gamma(x)$ is monic in $(O_K/M_K)[x]$ and has the same degree as $g_1(x)$, it is obvious that $g_1(x)$ is a monic polynomial. Because $\gamma(x)$ and $\eta(x)$ are relatively prime in $(O_K/M_K)[x]$, there exist polynomials $r(x)$ and $s(x)$ in $O_K[x]$ such that

$$\varphi(r)(x)\gamma(x) + \varphi(s)(x)\eta(x) = 1 \quad \text{in } (O_K/M_K)[x].$$

It follows that the polynomials

$$f(x) - g_1(x)h_1(x) \quad \text{and} \quad r(x)g_1(x) + s(x)h_1(x) - 1$$

have coefficients in M_K, and therefore

$$\delta = \max\{|f - g_1h_1|, |rg_1 + sh_1 - 1|\} < 1. \tag{3.4}$$

If $\delta = 0$ then $f(x) = g_1(x)h_1(x)$ and the theorem is proved. Therefore we assume throughout the remainder of the proof that $0 < \delta < 1$.

Next we construct two sequences of polynomials $\{g_n(x)\}_{n=1}^{\infty}$ and $\{h_n(x)\}_{n=1}^{\infty}$ in the ring $O_K[x]$ such that

$$|f - g_nh_n| \le \delta^n \quad \text{for each} \quad n = 1, 2, \ldots, \tag{3.5}$$

$$|g_n - g_{n-1}| \le \delta^{n-1} \quad \text{and} \quad |h_n - h_{n-1}| \le \delta^{n-1} \quad \text{for each} \quad n = 2, 3, \ldots, \tag{3.6}$$

$$\varphi(g_n) = \gamma \quad \text{and} \quad \varphi(h_n) = \eta \quad \text{for each} \quad n = 1, 2, \ldots, \tag{3.7}$$

$$\deg g_n = \deg \gamma \quad \text{and} \quad \deg g_n + \deg h_n \le \deg f \quad \text{for each} \quad n = 1, 2, \ldots. \tag{3.8}$$

As $g_1(x)$ and $h_1(x)$ are already determined, we assume that $g_m(x)$ and $h_m(x)$ have been defined for $m = 1, 2, \ldots, n-1$ and satisfy the conditions (3.5), (3.6), (3.7) and (3.8). Then we define $g_n(x)$ and $h_n(x)$ inductively in terms of $g_{n-1}(x)$ and $h_{n-1}(x)$. Toward this end we select ϵ in M_K so that $|\epsilon| = \delta$. Then we set

$$g_n(x) = g_{n-1}(x) + \epsilon^{n-1}t_{n-1}(x) \quad \text{and} \quad h_n(x) = h_{n-1}(x) + \epsilon^{n-1}u_{n-1}(x), \tag{3.9}$$

where $t_{n-1}(x)$ and $u_{n-1}(x)$ are polynomials in $O_K[x]$ to be determined. We note that (3.9) and the inductive hypothesis already imply that (3.6) and (3.7) hold. Then from (3.6) and the strong triangle inequality we get

$$|g_1 - g_{n-1}| \le \delta \quad \text{and} \quad |h_1 - h_{n-1}| \le \delta \quad \text{for each} \quad n = 2, 3, \ldots, \tag{3.10}$$

Also, by the inductive hypothesis the polynomial $p_{n-1}(x)$, defined by

$$f(x) - g_{n-1}(x)h_{n-1}(x) = \epsilon^{n-1}p_{n-1}(x),$$

belongs to $O_K[x]$ and satisfies

$$\deg p_{n-1} \leq \deg f.$$

Using the division algorithm and the fact that $g_1(x)$ is monic, there exist polynomials $q_{n-1}(x)$ and $t_{n-1}(x)$ in $O_K[x]$ such that

$$p_{n-1}(x)s(x) = q_{n-1}(x)g_1(x) + t_{n-1}(x) \quad \text{and} \quad \deg t_{n-1} < \deg g_1.$$

Now write

$$p_{n-1}(x)r(x) + q_{n-1}(x)h_1(x) = c_0x^M + c_1x^{M-1} + \cdots + c_M,$$

so that $|c_m| \leq 1$ for each $m = 0, 1, \ldots, M$. We define

$$u_{n-1}(x) = \tilde{c}_0x^M + \tilde{c}_1x^{M-1} + \cdots + \tilde{c}_M,$$

where

$$\tilde{c}_m = \begin{cases} c_m & \text{if } \delta < |c_m|, \\ 0 & \text{if } |c_m| \leq \delta. \end{cases} \tag{3.11}$$

It follows that

$$|p_{n-1}r + q_{n-1}h_1 - u_{n-1}| \leq \delta,$$

and therefore

$$\begin{aligned} &\big|p_{n-1}(rg_1 + sh_1) - g_1u_{n-1} - h_1t_{n-1}\big| \\ &\qquad = \big|p_{n-1}rg_1 + q_{n-1}g_1h_1 + h_1t_{n-1} - g_1u_{n-1} - h_1t_{n-1}\big| \\ &\qquad = \big|(p_{n-1}r + q_{n-1}h_1 - u_{n-1})g_1\big| \\ &\qquad \leq \delta. \end{aligned} \tag{3.12}$$

Combining (3.4) and (3.12) we get the inequality

$$\begin{aligned} &\big|p_{n-1} - g_1u_{n-1} - h_1t_{n-1}\big| \\ &\qquad \leq \max\big\{|p_{n-1}(1 - rg_1 - sh_1)|, |p_{n-1}(rg_1 + sh_1) - g_1u_{n-1} - h_1t_{n-1}\big|\big\} \\ &\qquad \leq \delta. \end{aligned} \tag{3.13}$$

Using (3.9) and (3.13) we obtain the bound

$$|p_{n-1} - g_{n-1}u_{n-1} - h_{n-1}t_{n-1}| \le \delta. \tag{3.14}$$

In order to verify (3.5) we use (3.14) and get

$$\begin{aligned}
|f - g_n h_n| &= \left|f - g_{n-1}h_{n-1} - \epsilon^{n-1}(g_{n-1}u_{n-1} + h_{n-1}t_{n-1}) - \epsilon^{2n-2}t_{n-1}u_{n-1}\right| \\
&= \left|\epsilon^{n-1}\big(p_{n-1} - g_{n-1}u_{n-1} - h_{n-1}t_{n-1}\big) - \epsilon^{2n-2}t_{n-1}u_{n-1}\right| \\
&\le \max\left\{\delta^{n-1}|p_{n-1} - g_{n-1}u_{n-1} - h_{n-1}t_{n-1}|, \delta^{2n-2}\right\} \\
&\le \delta^n.
\end{aligned}$$

Finally, we must show that $g_n(x)$ and $h_n(x)$ satisfy (3.8). We have $\deg g_{n-1} = \deg \gamma$ by the inductive hypothesis, and $\deg g_n = \deg g_{n-1}$ holds because $\deg t_{n-1} < \deg g_1 = \deg \gamma$. If follows then that $\deg g_n = \deg \gamma$. Now assume that $\deg h_n > \deg f - \deg g_n$. From (3.9) and the inductive hypothesis we get $\deg u_{n-1} > \deg f - \deg g_n$. Hence we also have

$$\deg p_{n-1} \le \deg f, \quad \deg f < \deg g_{n-1} + \deg u_{n-1} \quad \text{and} \quad \deg h_{n-1} + \deg t_{n-1} < \deg f.$$

As $g_{n-1}(x)$ is monic, it follows that the leading coefficient of the polynomial

$$p_{n-1}(x) - g_{n-1}(x)u_{n-1}(x) - h_{n-1}(x)t_{n-1}(x)$$

is also the leading coefficient of $-u_{n-1}(x)$. Because the leading coefficient of $-u_{n-1}(x)$ has absolute value greater than δ, this plainly contradicts the inequality (3.14). We have shown that $\deg h_n \le \deg f - \deg g_n$, and so we have verified (3.8).

Now write

$$g_n(x) = \sum_{l=0}^{L} a_l^{(n)} x^{L-l} \quad \text{and} \quad h_n(x) = \sum_{m=0}^{M} b_m^{(n)} x^{M-m},$$

where $a_0^{(n)} = 1$ for each $n = 1, 2, \ldots$. It follows from (3.6) that for each l, $0 \le l \le L$, the sequence $\{a_l^{(n)}\}_{n=1}^{\infty}$ is Cauchy. As K is complete, we define

$$\lim_{n\to\infty} a_l^{(n)} = A_l \quad \text{and} \quad g(x) = \sum_{l=0}^{L} A_l x^{L-l}.$$

We find that $g(x)$ is a monic polynomial in $O_K[x]$, $\deg g = \deg \gamma$, and $\varphi(g)(x) = \gamma(x)$. In a similar manner we define

$$\lim_{n\to\infty} b_m^{(n)} = B_m \quad \text{and} \quad h(x) = \sum_{m=0}^{M} B_m x^{M-m},$$

so that $h(x)$ is a polynomial in $O_K[x]$ and $\varphi(h)(x) = \eta(x)$. Then (3.5) implies that $f(x) = g(x)h(x)$, and this completes the proof.

COROLLARY 3.2. *Suppose that $f(x)$ is an irreducible polynomial of degree N in $K[x]$ and*

$$f(x) = a_0 x^N + a_{N-1} x^{N-1} + \cdots + a_N.$$

Then we have

$$|f| = \max\{|a_0|, |a_1|, \ldots, |a_N|\} = \max\{|a_0|, |a_N|\}. \tag{3.15}$$

PROOF. If (3.15) is false then there exists a smallest positive integer m such that

$$|f| = |a_m| > \max\{|a_0|, |a_N|\} \quad \text{where} \quad 1 \le m \le N-1.$$

It follows that $a_m^{-1} f(x)$ belongs to $O_K[x]$ and satisfies $|a_m^{-1} f| = 1$. Write $\gamma(x) = \varphi(a_m^{-1} f)(x)$ and $\eta(x) = 1$. Then $\gamma(x)$ is monic, $\deg \gamma = m$ and

$$\varphi(a_m^{-1} f)(x) = \gamma(x)\eta(x) \quad \text{in } (O_K/M_K)[x].$$

By the theorem $a_m^{-1} f(x)$ factors in $O_K[x]$ as

$$a_m^{-1} f(x) = g(x)h(x) \quad \text{with} \quad \deg g = m.$$

This contradicts the assumption that $f(x)$ is irreducible in $K[x]$ and the statement of the corollary follows.

COROLLARY 3.3. *Suppose that $f(x)$ is a monic, irreducible polynomial in $O_K[x]$. Then $\varphi(f)(x)$ is a positive integer power of an irreducible polynomial in $(O_K/M_K)[x]$.*

PROOF. Because $f(x)$ is monic the polynomial $\varphi(f)(x)$ is also monic and has positive degree. Let

$$\varphi(f)(x) = \prod_{l=1}^{L} \psi_l(x)^{m_l}$$

be the factorization of $\varphi(f)(x)$ in $(O_K/M_K)[x]$. That is, $m_1, m_2, \ldots, m_L$ are positive integers, and $\psi_1(x), \psi_2(x), \ldots, \psi_L(x)$ are distinct, monic, irreducible polynomials in $(O_K/N_K)[x]$ having positive degree. If $2 \le L$ write

$$\gamma(x) = \psi_1(x)^{m_1} \quad \text{and} \quad \eta(x) = \prod_{l=2}^{L} \psi_l(x)^{m_l}.$$

Then we have the nontrivial factorization $\varphi(f)(x) = \gamma(x)\eta(x)$ in $(O_K/M_K)[x]$. By the theorem there is a nontrivial factorization $f(x) = g(x)h(x)$ in $O_K[x]$ with $1 \le \deg g = \deg \gamma < \deg f$. This contradicts the assumption that $f(x)$ is irreducible and shows that $L = 1$.

COROLLARY 3.4. *Suppose that $f(x)$ is a polynomial in $O_K[x]$ such that $\varphi(f)(x)$ has a simple root at the point α in O_K/M_K. Then there exists a point β in O_K such that $f(\beta) = 0$ and $\varphi(\beta) = \alpha$.*

PROOF. By hypothesis the polynomial $\varphi(f)(x)$ factors in $(O_K/M_K)[x]$ as

$$\varphi(f)(x) = (x - \alpha)\eta(x)$$

where $(x - \alpha)$ and $\eta(x)$ are relatively prime. By the theorem there exist polynomials $g(x)$ and $h(x)$ in $O_K[x]$ such that $f(x) = g(x)h(x)$, $g(x)$ is monic, linear, and $\varphi(g)(x) = (x - \alpha)$. Writing $g(x) = (x - \beta)$ we must have $f(\beta) = 0$ and $\varphi(\beta) = \alpha$.

Exercises

3.1 Let p be a prime number. Prove that the polynomial $x^{p-1} - 1$ splits into linear factors in the field $\mathbb{Q}_p$, and show that the roots of $x^{p-1} - 1$ in $\mathbb{Q}_p^\times$ form a cyclic subgroup of order $p - 1$.

3.2 Let $\mu_{p-1} \subseteq \mathbb{Q}_p^\times$ denote the set of roots of the polynomial $x^{p-1} - 1$ in $\mathbb{Q}_p^\times$. Prove that the set $\{0\} \cup \mu_{p-1}$ forms a complete set of distinct representatives for the residue class field $\mathbb{Z}_p/M_p$, where $M_p \subseteq \mathbb{Z}_p$ is the unique maximal ideal.

3.3 Let $\mu_{p-1} \subseteq \mathbb{Q}_p^\times$ be as in Exercise 1.2. Write $\psi : \mathbb{Z}_p \to \mathbb{Z}_p/M_p$ for the canonical homomorphism. Prove that the restriction of ψ to the subgroup μ_{p-1} is a group isomorphism from μ_{p-1} onto the cyclic group $(\mathbb{Z}_p/M_p)^\times$.

3.4 Prove that if α is in the ring $\mathbb{Z}_p$, then the limit

$$\lim_{m\to\infty} \alpha^{p^m} = T_p(\alpha) \tag{3.16}$$

exists, and so defines a map $T_p : \mathbb{Z}_p \to \mathbb{Z}_p$.

3.5 Let $\mu_{p-1} \subseteq \mathbb{Q}_p^\times$ be as in Exercise 1.2, and let $T_p : \mathbb{Z}_p \to \mathbb{Z}_p$ be the map defined by (3.16). Prove that T_p takes values in the subset $\{0\} \cup \mu_{p-1}$, and the restriction of T_p to the subset $\{0\} \cup \mu_{p-1}$ is the identity map.

3.6 Assume that K is a field with a nontrivial, non-archimedean absolute value $|\ |$ and assume that $(K, |\ |)$ is complete. Let $|\ |$ be extended to the polynomial ring $K[x]$ by (3.1). Prove that $f \to |f|$ is a map from $K[x]$ to $[0, \infty)$ that satisfies the three conditions

(1) $|f| = 0$ if and only if $f = 0$,
(2) $|fg| = |f||g|$ for all f and g in $K[x]$,
(3) $|f + g| \le \max\{|f|, |g|\}$ for all f and g in $K[x]$.

Conclude using Lemma 1.6 of Chapter 2 that $f \to |f|$ has a unique extension to a non-archimedean absolute value on the field of rational functions $K(x)$. Note that the restriction of this absolute value to the subfield K is not trivial.

4. Extensions of Absolute Values on Complete Fields

In this section we assume that K is a field with a nontrivial absolute value $|\ |$, that $(K, |\ |)$ is complete, and that L/K is a finite extension of fields. Then we define a map $\|\ \| : L \to [0, \infty)$ by

$$\|\beta\| = |\operatorname{Norm}_{L/K}(\beta)|^{1/N}, \quad \text{where} \quad N = [L : K]. \tag{4.1}$$

If β is in K then (1.11) implies that $\|\beta\| = |\beta|$. Thus $\beta \to \|\beta\|$ extends the absolute value $|\ |$ on K to a map on L.

THEOREM 4.1. *The map* (4.1) *defines an absolute value* $\|\ \|$ *on* L *that extends the absolute value* $|\ |$ *on* K*. Moreover,* $\|\ \|$ *is the unique absolute value on* L *that extends* $|\ |$ *on* K*, and* L *is complete in the metric topology induced by* $\|\ \|$*.*

PROOF. We may assume that $N = [L : K] > 1$. If $|\ |$ is archimedean then by Theorem 2.2 of Chapter 2, $(K, |\ |)$ is isometrically isomorphic to either $(\mathbb{R}, |\ |_\infty^\theta)$ or $(\mathbb{C}, |\ |_\infty^\theta)$ with $0 < \theta \le 1$. However, $\mathbb{C}$ is algebraically closed and does not have nontrivial finite extensions. We conclude that $(K, |\ |)$ is isometrically isomorphic to $(\mathbb{R}, |\ |_\infty^\theta)$. As $[\mathbb{C} : \mathbb{R}] = 2$ we also conclude that $N = 2$ and L is isomorphic to $\mathbb{C}$. A basis for $\mathbb{C}$ over $\mathbb{R}$ is given by $\{1, i\}$. If β in $\mathbb{C}$ is written with respect this basis as $\beta = \beta_1 + i\beta_2$, with β_1 and β_2 in $\mathbb{R}$, we find that

$$\operatorname{Norm}_{\mathbb{C}/\mathbb{R}}(\beta) = \beta_1^2 + \beta_2^2.$$

It follows from (4.1) that

$$\|\beta\| = |\beta|_\infty^\theta,$$

where $|\ |_\infty$ is the usual Hermitian absolute value on $\mathbb{C}$. By Corollary 2.2 this extension to an absolute value on $\mathbb{C}$ is unique and Theorem 2.1 shows that $\mathbb{C}$ is complete in the resulting metric topology. Of course these results about $\mathbb{R}$ and $\mathbb{C}$ are well known.

We assume throughout the remainder of the proof that $|\ |$ is nontrivial and nonarchimedean. The function $\operatorname{Norm}_{L/K} : L^\times \to K^\times$ is a homomorphism of multiplicative groups. From this observation we conclude that

$$\|\beta\| = 0 \quad \text{if and only if} \quad \beta = 0,$$

and

$$\|\alpha\beta\| = \|\alpha\|\|\beta\|.$$

It remains then to demonstrate that $\beta \to \|\beta\|$ satisfies the strong triangle inequality. To accomplish this we will show that

$$\sup\{\|1 + \beta\| : \beta \in L,\ \|\beta\| \le 1\} = 1. \tag{4.2}$$

Let β be in L, $\|\beta\| \le 1$, and let

$$f_\beta(x) = x^Q + a_l x^{Q-1} + \cdots + a_Q, \quad \text{where} \quad Q = [K(\beta) : K],$$

be the minimal polynomial for β over K. As in (1.11) we have

$$\operatorname{Norm}_{L/K}(\beta) = (-1)^{QR} f_\beta(0)^R, \quad \text{where} \quad R = [L : K(\beta)],$$

and therefore

$$|a_Q| = |f_\beta(0)| = |\operatorname{Norm}_{L/K}(\beta)|^{Q/N} = \|\beta\|^Q \le 1. \tag{4.3}$$

As $f_\beta(x)$ is a monic, irreducible polynomial in $K[x]$, Corollary 3.2 and (4.3) imply that $f_\beta(x)$ is in $O_K[x]$. Plainly the minimal polynomial for $1+\beta$ is $f_\beta(x-1)$. Applying (1.11) again we get

$$\operatorname{Norm}_{L/K}(1+\beta) = (-1)^{QR} f_\beta(-1)^R,$$

and then

$$\begin{aligned}
\|1+\beta\| &= |\operatorname{Norm}_{L/K}(1+\beta)|^{1/N} \\
&= |f_\beta(-1)|^{R/N} \\
&= \left|(-1)^Q + a_1(-1)^{Q-1} + \cdots + a_Q\right|^{1/Q} \\
&\le \max\left\{1, |a_1|, |a_2|, \ldots, |a_Q|\right\}^{1/Q} \\
&= 1.
\end{aligned}$$

This verifies (4.2). Now if α and β are in L, if $\|\beta\| \le \|\alpha\|$ then we have

$$\|\alpha+\beta\| = \|\alpha\|\|1+\alpha^{-1}\beta\| \le \|\alpha\| = \max\{\|\alpha\|, \|\beta\|\}.$$

We have shown that (4.1) defines an absolute value on L that extends the absolute value $|\ |$ on K. It follows from Corollary 2.2 that this is the unique extension of $|\ |$ on K to an absolute value on L. By Theorem 2.1 L is complete in the induced metric topology.

It is not difficult to see that the extended absolute value defined by (4.1) depends on β but not otherwise on the finite extension L. To make this more precise, let $\overline{K}$ be an algebraic closure of K and then let L_1 and L_2 be finite extensions of K such that

$$K \subseteq L_1 \subseteq \overline{K} \quad \text{and} \quad K \subseteq L_2 \subseteq \overline{K}.$$

Write $N_1 = [L_1 : K]$ and $N_2 = [L_2 : K]$, so that

$$\|\alpha\|_1 = |\operatorname{Norm}_{L_1/K}(\alpha)|^{1/N_1} \quad \text{and} \quad \|\beta\|_2 = |\operatorname{Norm}_{L_2/K}(\beta)|^{1/N_2}$$

are the unique extensions of $|\ |$ on K to L_1 and L_2, respectively. Now assume that β belongs to $L_1 \cap L_2$. Let f_β be the minimal polynomial for β over K and assume that f_β has degree Q. Using (1.11) we find that

$$\mathrm{Norm}_{L_1/K}(\beta) = (-1)^{QR_1} f_\beta(0)^{R_1} \quad \text{and} \quad \mathrm{Norm}_{L_2/K}(\beta) = (-1)^{QR_2} f_\beta(0)^{R_2},$$

where $R_1 = [L_1 : K(\beta)]$ and $R_2 = [L_2 : K(\beta)]$. It follows that $N_1 = QR_1$, $N_2 = QR_2$, and therefore

$$\|\beta\|_1 = |f_\beta(0)|^{R_1/N_1} = |f_\beta(0)|^{R_2/N_2} = \|\beta\|_2. \tag{4.4}$$

This shows that the absolute value $|\ |$ on K extends to a map $|\ | : \overline{K} \to [0, \infty)$ as follows: if β is in $\overline{K}$, select a finite extension L/K such that β is in L and $K \subseteq L \subseteq \overline{K}$. Then define the absolute value of β by (4.1). In view of the identity (4.4) this is well defined. Therefore we will write simply

$$|\beta| = |\,\mathrm{Norm}_{L/K}(\beta)|^{1/N}, \quad \text{where} \quad N = [L : K], \tag{4.5}$$

for the extended function $|\ | : \overline{K} \to [0, \infty)$. By Theorem 4.1 the restriction of $|\ |$ to a finite extension L/K is an absolute value on L. We now show that (4.5) defines the unique extension of $|\ |$ on K to an absolute value on $\overline{K}$.

THEOREM 4.2. *Assume that K is a field with a nontrivial absolute value $|\ |$, that $(K, |\ |)$ is complete, and that $\overline{K}$ is an algebraic closure of K. Then $|\ |$ has a unique extension to $\overline{K}$. If β is a point in $\overline{K}$, if $K \subseteq L \subseteq \overline{K}$ and L/K is a finite extension with β in L, then the extended absolute value of β is given by* (4.5).

PROOF. Let α and β be elements of $\overline{K}$. Let $L = K(\alpha, \beta)$ so that L/K is a finite extension of fields. By our previous remarks, the restriction of $|\ |$ on $\overline{K}$ to the subfield L is an absolute value on L. Hence the three conditions

(i) $|\alpha| = 0$ if and only if $\alpha = 0$,

(ii) $|\alpha\beta| = |\alpha||\beta|$,

(iii) $|\alpha + \beta| \leq |\alpha| + |\beta|$,

required of an absolute value are satisfied. We have shown that (4.5) defines an absolute value on $\overline{K}$. The uniqueness of $|\ |$ as an absolute value on $\overline{K}$ follows because the restriction of $|\ |$ to each finite extension of K is unique. This proves the theorem.

COROLLARY 4.3. *Assume that K is a field with a nontrivial absolute value $|\ |$, that $(K, |\ |)$ is complete, and that $\overline{K}$ is an algebraic closure of K. If L/K is a finite extension of fields, and $\|\ \|$ on L extends the absolute value $|\ |$ on K, then there exists an isometric*

embedding $\sigma : L \to \overline{K}$ that fixes K, and satisfies the identity $\|\beta\| = |\sigma(\beta)|$ for all β in L.

PROOF. Because L/K is an algebraic extension of fields, and $\overline{K}$ is an algebraic closure of K, there exists a field embedding $\sigma : L \to \overline{K}$ that fixes K. It follows that the map $\beta \to |\sigma(\beta)|$ defines an absolute value on L, and this absolute value extends $|\ |$ on K. By Theorem 4.1 an extension of $|\ |$ on K to an absolute value on L is unique, and therefore we have $\|\beta\| = |\sigma(\beta)|$ for all β in L.

We recall that two points β_1 and β_2 in $\overline{K}$ are *conjugate* over K if they have the same minimal polynomial over K. In this case, if $f_{\beta_1}(x) = f_{\beta_2}(x)$ is the common minimal polynomial with degree N, we have

$$|\beta_1| = |f_{\beta_1}(0)|^{1/N} = |f_{\beta_2}(0)|^{1/N} = |\beta_2|. \tag{4.6}$$

We now prove a useful generalization of (4.6).

LEMMA 4.4 (KRASNER'S LEMMA). *Assume that K is a field with a nontrivial, nonarchimedean absolute value $|\ |$, that $(K, |\ |)$ is complete, and that $\overline{K}$ is an algebraic closure of K. Suppose that β_1 and β_2 are in $\overline{K}$ and conjugate over K. Then each point γ in K satisfies*

$$|\beta_1 - \beta_2| \le |\beta_1 - \gamma| = |\beta_2 - \gamma|. \tag{4.7}$$

PROOF. We have

$$|\beta_1 - \beta_2| = \big|(\beta_1 - \gamma) + (\gamma - \beta_2)\big| \le \max\{|\beta_1 - \gamma|, |\beta_2 - \gamma|\}.$$

Now $\beta_1 - \gamma$ and $\beta_2 - \gamma$ are both roots of the monic irreducible polynomial $f_{\beta_1}(x+\gamma) = f_{\beta_2}(x+\gamma)$ in $K[x]$. Hence $\beta_1 - \gamma$ and $\beta_2 - \gamma$ are conjugate over K. Then (4.6) implies that

$$|\beta_1 - \gamma| = |\beta_2 - \gamma|,$$

and this verifies (4.7).

We note that Lemma 4.4 has an obvious archimedean analogue. If β_1 and β_2 are complex numbers, conjugate over $\mathbb{R}$, and γ is in $\mathbb{R}$, then

$$\tfrac{1}{2}|\beta_1 - \beta_2|_\infty \le |\beta_1 - \gamma|_\infty = |\beta_2 - \gamma|_\infty. \tag{4.8}$$

5. Extensions of Absolute Values on Incomplete Fields

We assume that l/k is a finite, separable extension of fields, and $|\ |$ is a nontrivial absolute value on k. In this section we do not assume that k is complete. Our objective is to determine how $|\ |$ on k can be extended to an absolute value on l.

Let $(K, |\ |)$ be a completion of $(k, |\ |)$, and write $\overline{K}$ for an algebraic closure of K. Because l/k is a finite extension and $\overline{K}$ is an algebraically closed field containing k, there exist N distinct field embeddings $\sigma_n : l \to \overline{K}$ that fix k, where $n = 1, 2, \ldots, N$, and $N = [l : k]$. To determine these embeddings let α in l generate l as a simple extension of k, and let $f_\alpha(x)$ in $k[x]$ be the minimal polynomial of α. Write $\beta_1, \beta_2, \ldots, \beta_N$ for the roots of f_α in $\overline{K}$. As l/k is a separable extension, the polynomial f_α has N distinct roots in $\overline{K}$. Each root β_n determines an embedding $\sigma_n : l \to \overline{K}$ that fixes k by $\sigma_n(\alpha) = \beta_n$, and in general by

$$\begin{aligned}\sigma_n\big(b_{N-1}\alpha^{N-1} + b_{N-2}\alpha^{N-2} + \cdots + b_0\big)& \\ = b_{N-1}\beta_n^{N-1} + b_{N-2}\beta_n^{N-2} + \cdots + b_0,&\end{aligned} \tag{5.1}$$

where $b_0, b_1, \ldots, b_{N-1}$ are elements of k. Then each map $\gamma \to |\sigma_n(\gamma)|$ determines an absolute value on l that extends $|\ |$ on k. In this section we will show that every absolute value on l that extends $|\ |$ on k has this form. We will also show that the maps $\gamma \to |\sigma_m(\gamma)|$ and $\gamma \to |\sigma_n(\gamma)|$ determine exactly the same absolute value on l if and only if β_m and β_n are are conjugate over K. In particular, suppose that f_α factors in $K[x]$ as

$$f_\alpha(x) = \prod_{r=1}^{R} \varphi_r(x), \tag{5.2}$$

where each factor φ_r is a monic irreducible polynomial in $K[x]$ with positive degree. Then β_m and β_n are conjugate over K if and only if they are both roots of the same irreducible factor. Thus there are exactly R different extensions of the absolute value $|\ |$ on k to an absolute value on l.

Lemma 5.1. *Assume that l/k is a finite, separable extension of fields, and $|\ |$ is a nontrivial absolute value on k. Let $(K, |\ |)$ be a completion of $(k, |\ |)$, and write $\overline{K}$ for an algebraic closure of K. For $n = 1, 2, \ldots, N$ let $\sigma_n : l \to \overline{K}$ be the embedding defined by* (5.1). *Then the maps $\gamma \to |\sigma_m(\gamma)|$ and $\gamma \to |\sigma_n(\gamma)|$ determine the same absolute value on l if and only if β_m and β_n are conjugate over K.*

Proof. Suppose that β_m and β_n are conjugate over K, and let

$$\gamma = b_{N-1}\alpha^{N-1} + b_{N-2}\alpha^{N-2} + \cdots + b_0$$

be an element of l, where $b_0, b_1, \ldots, b_{N-1}$ are elements of k. Then

$$b_{N-1}\beta_m^{N-1} + b_{N-2}\beta_m^{N-2} + \cdots + b_0 \quad \text{and} \quad b_{N-1}\beta_n^{N-1} + b_{N-2}\beta_n^{N-2} + \cdots + b_0$$

are conjugate over K. It follows using (4.6) that

$$\begin{aligned} |\sigma_m(\gamma)| &= |b_{N-1}\beta_m^{N-1} + b_{N-2}\beta_m^{N-2} + \cdots + b_0| \\ &= |b_{N-1}\beta_n^{N-1} + b_{N-2}\beta_n^{N-2} + \cdots + b_0| \\ &= |\sigma_n(\gamma)|. \end{aligned}$$

Now assume that β_m and β_n are not conjugate over K, and let

$$\varphi(x) = x^J + c_1 x^{J-1} + \cdots + c_J$$

be the minimal polynomial for β_m in $K[x]$. Then we have $\varphi(\beta_n) \neq 0$. Select $\delta > 0$ so that

$$\delta \max\{1, |\beta_m|\}^{J-1} < |\varphi(\beta_n)| - \delta \max\{1, |\beta_n|\}^{J-1}. \tag{5.3}$$

Because k is dense in K, there exist $a_1, a_2, \ldots, a_J$ in k such that

$$\sum_{j=1}^{J} |a_j - c_j| < \delta. \tag{5.4}$$

Then let

$$\psi(x) = x^J + a_1 x^{J-1} + \cdots + a_J$$

be the corresponding polynomial in $k[x]$. It follows using (5.4) that

$$\begin{aligned} |\psi(\beta_m)| &= |\psi(\beta_m) - \varphi(\beta_m)| \\ &\leq \sum_{j=1}^{J} |a_j - c_j| \max\{1, |\beta_m|\}^{J-j} \\ &\leq \delta \max\{1, |\beta_m|\}^{J-1}, \end{aligned} \tag{5.5}$$

and similarly,

$$\begin{aligned} |\varphi(\beta_n)| &\leq |\varphi(\beta_n) - \psi(\beta_n)| + |\psi(\beta_n)| \\ &\leq \delta \max\{1, \beta_n|\}^{J-1} + |\psi(\beta_n)|. \end{aligned} \tag{5.6}$$

Combining (5.3), (5.5) and (5.6) leads to the inequality

$$|\psi(\beta_m)| < |\psi(\beta_n)|.$$

It follows that if η in l is given by

$$\eta = \alpha^J + a_1\alpha^{J-1} + \cdots + a_J,$$

then

$$|\sigma_m(\eta)| = |\psi(\beta_m)| < |\psi(\beta_n)| = |\sigma_n(\eta)|.$$

This proves the lemma.

It will be convenient now to index the roots $\beta_1, \beta_2, \ldots, \beta_N$ of f_α in $\overline{K}$ so that β_r is a root of the irreducible factor $\varphi_r(x)$ for $r = 1, 2, \ldots, R$. Then each of the maps

$$\gamma \to |\gamma|_r = |\sigma_r(\gamma)|, \quad \text{where} \quad r = 1, 2, \ldots, R, \tag{5.7}$$

defines an absolute on l that extends the absolute value $|\ |$ on k. By Lemma 5.1, the absolute values $|\ |_r$ are distinct for $r = 1, 2, \ldots, R$, and account for all the absolute values on l that are defined by the maps $\gamma \to |\sigma_n(\gamma)|$ for $n = 1, 2, \ldots, N$.

Lemma 5.2. *Assume that l/k is a finite, separable extension of fields, and $|\ |$ is a nontrivial absolute value on k. Let $(K, |\ |)$ be a completion of $(k, |\ |)$, and write $\overline{K}$ for an algebraic closure of K. Let $\|\ \|$ be an absolute value on l that extends the absolute value $|\ |$ on k, and write $(L, \|\ \|)$ for a completion of $(l, \|\ \|)$. Then there exists an isometric embedding $\tau : L \to \overline{K}$ that fixes k, and satisfies the identity $\|\gamma\| = |\tau(\gamma)|$ for all γ in L.*

Proof. Let K' be the closure of k in L. By Exercise 2.4 in Chapter 2, the set K' is a subfield of L and $(K', \|\ \|)$ is a completion of $(k, \|\ \|) = (k, |\ |)$. Because l/k is a finite, separable extension, there exists α in l such that $l = k(\alpha)$. Obviously α is algebraic over k, and therefore α is algebraic over K'. It follows from Theorem 4.1 that $K'(\alpha)$ is complete. As

$$l \subseteq K'(\alpha) \subseteq L,$$

we conclude that $K'(\alpha) = L$.

Since $(K', \|\ \|)$ and $(K, |\ |)$ are both completions of $(k, \|\ \|) = (k, |\ |)$, it follows from Theorem 2.1 that there exists a unique isometric isomorphism $\tau : K' \to K$ such that $\tau \circ \sigma_{K'} = \sigma_K$, where $\sigma_{K'} : k \to K'$ and $\sigma_K : k \to K$ are isometric embeddings. As $k \subseteq K'$ and $k \subseteq K$, we find that τ fixes k. Obviously τ extends to a ring isomorphism $\tau : K'[x] \to K[x]$ by letting τ act on the coefficients of polynomials. In particular, let

$$g_\alpha(x) = x^Q + a_1x^{Q-1} + \cdots + a_Q$$

be the minimal polynomial of α in $K'[x]$. Write

$$\tau(g_\alpha)(x) = x^Q + \tau(a_1)x^{Q-1} + \cdots + \tau(a_Q)$$

for the image of g_α in $K[x]$. Clearly, $\tau(g_\alpha)$ is a monic, irreducible polynomial in $K[x]$. Let β be a root of $\tau\big(g_\alpha\big)$ in $\overline{K}$. Then $\tau : K' \to K$ extends to an isomorphism

$$\tau : K'(\alpha) \to K(\beta)$$

given by

$$\begin{aligned}\tau\big(c_{Q-1}\alpha^{Q-1} + c_{Q-2}\alpha^{Q-2} + \cdots + c_0\big)& \\ = \tau(c_{Q-1})\beta^{Q-1} + \tau(c_{Q-2})\beta^{Q-2} + \cdots + \tau(c_0).&\end{aligned}$$

It follows that the map $\gamma \to |\tau(\gamma)|$ determines an absolute value on $K'(\alpha)$ that extends the absolute value $\| \ \|$ on K'. By Theorem 4.1 the extension of $\| \ \|$ on K' to an absolute value on $K'(\alpha)$ is unique, and therefore we have $\|\gamma\| = |\tau(\gamma)|$ for all γ in $K'(\alpha) = L$.

We are now in position to combine Lemma 5.1 and Lemma 5.2 and so determine all absolute values on l that extend $| \ |$ on k.

THEOREM 5.3. *Assume that l/k is a finite, separable extension of fields, and $| \ |$ is a nontrivial absolute value on k. Let α in l generate l as a simple extension of k, and let $f_\alpha(x)$ in $k[x]$ be the minimal polynomial of α. Assume that f_α factors into monic, irreducible factors in $K[x]$ as in* (5.2)*, and let $| \ |_r$, for $r = 1, 2, \ldots, R$, be the distinct absolute values on l defined by* (5.7)*.*

(1) *If $\| \ \|$ is an absolute value on l that extends the absolute value $| \ |$ on k, then $\| \ \| = | \ |_r$ for some r.*
(2) *If $(L_r, | \ |_r)$ is a completion of $(l, | \ |_r)$, and K_r is the closure of k in L_r, then $(K_r, | \ |_r)$ is a completion of $(k, | \ |_r) = (k, | \ |)$.*
(3) *For each $r = 1, 2, \ldots, R$, we have $[L_r : K_r] = \deg \varphi_r$, and therefore*

$$\sum_{r=1}^{R} [L_r : K_r] = [l : k]. \tag{5.8}$$

PROOF. Let $(K, | \ |)$ be a completion of $(k, | \ |)$, write $\overline{K}$ for an algebraic closure of K, and write $(L, \| \ \|)$ for a completion of $(l, \| \ \|)$. By Lemma 5.2 there exists an isometric embedding $\tau : L \to \overline{K}$ that fixes k, and satisfies the identity $\|\gamma\| = |\tau(\gamma)|$ for all γ in L. Hence the restriction of τ to l maps the generator α to one of the roots β_n in $\overline{K}$.

That is, τ restricted to l is one of the maps $\sigma_n : l \to \overline{K}$ defined by (5.1). Select r in $\{1, 2, \ldots, R\}$ so that β_n and β_r are conjugate over K. By Lemma 5.1 we have

$$\|\gamma\| = |\tau(\gamma)| = |\sigma_n(\gamma)| = |\sigma_r(\gamma)| = |\gamma|_r$$

for each γ in l. This verifies (1).

The assertion (2) follows from Exercise 2.4 in Chapter 2.

For each r in $\{1, 2, \ldots, R\}$ we apply Lemma 5.2 to the absolute value $|\ |_r$ on l. Thus there exists an isometric embedding $\tau_r : L_r \to K$ such that $|\gamma|_r = |\tau_r(\gamma)|$ for all γ in L_r. By Theorem 2.1 the restriction of τ_r to K_r is an isometric isomorphism from K_r onto K. It follows that

$$[L_r : K_r] = [K(\beta_r) : K] = \deg \varphi_r$$

for each r, and then

$$\sum_{r=1}^{R} [L_r : K_r] = \sum_{r=1}^{R} \deg \varphi_r = \deg f_\alpha = [l : k].$$

This proves (3).

THEOREM 5.4. *Assume that l/k is a purely inseparable extension of fields, and $|\ |$ is a nontrivial absolute value on k. Then $|\ |$ has a unique extension to an absolute value on l.*

PROOF. Clearly we may assume that k is a field of characteristic $p > 0$ and therefore $|\ |$ is a non-archimedean absolute value on k. It will be convenient to use a corresponding nontrivial valuation $v : k \to \mathbb{R} \cup \{\infty\}$, which we define by $v(a) = -\log |a|$ for all a in k. Thus we must show that v has a unique extension to a valuation on l.

If $\alpha \neq 0$ is in l then there exists a nonnegative integer m such that $\alpha^{p^m} = a$ is in k. Suppose that n is also a positive integer such that $\alpha^{p^n} = b$ is in k. We may assume that $1 \leq m < n$ and then conclude that

$$b = \alpha^{p^n} = \left(\alpha^{p^m}\right)^{p^{n-m}} = a^{p^{n-m}}. \tag{5.9}$$

Now (5.9) implies that

$$p^{-m} v(a) = p^{-n} v(b). \tag{5.10}$$

Therefore we extend v to a map $w : l \to \mathbb{R} \cup \{\infty\}$ by setting $w(0) = \infty$ and

$$w(\alpha) = p^{-m} v(a). \tag{5.11}$$

The identity (5.10) shows that the extended map w is well defined. If α is in k then we may use (5.11) with $m = 0$. It follows that w on l extends the map v on k.

Suppose that $\alpha \neq 0$ and $\beta \neq 0$ belong to l. Let m and n be nonnegative integers such that both $\alpha^{p^m} = a$ and $\beta^{p^n} = b$ belong to k. If $0 \leq m \leq n$ then we have

$$(\alpha\beta)^{p^n} = \left(\alpha^{p^m}\right)^{p^{n-m}} (\beta)^{p^n} = a^{p^{n-m}} b. \tag{5.12}$$

Using (5.12) we get

$$w(\alpha\beta) = p^{-n} v\left(a^{p^{n-m}} b\right) = p^{-m} v(a) + p^{-n} v(b) = w(\alpha) + w(\beta). \tag{5.13}$$

As l has characteristic p we also have

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = a^{p^{n-m}} + b,$$

and therefore

$$\begin{aligned} w(\alpha + \beta) &= p^{-n} v\left(a^{p^{n-m}} + b\right) \\ &\geq p^{-n} \min\left\{p^{n-m} v(a), v(b)\right\} \\ &= \min\left\{p^{-m} v(a), p^{-n} v(b)\right\} \\ &= \min\{w(\alpha), w(\beta)\}. \end{aligned} \tag{5.14}$$

Then it follows from (5.13) and (5.14) that w defines a valuation on l.

Finally, we assume that $\widehat{w}$ is also an extension of v to a valuation on l. If $\alpha \neq 0$ is in l and m is a nonnegative integer such that $\alpha^{p^m} = a$ is in k, then we have

$$w(\alpha) = p^{-m} v(a) = p^{-m} \widehat{w}\left(\alpha^{p^m}\right) = \widehat{w}(\alpha).$$

This shows that w is the unique extension of v to a valuation on k.

Exercises

5.1 Assume that l/k is a finite extension of fields, and let $|\ |_0$ denote the trivial absolute value on k. Prove that the only absolute value on l that extends $|\ |_0$ on k is the trivial absolute value on l. (Recall that we showed in section 7 of Chapter 2 that there exist nontrivial absolute values on $k(x)$ that extend the trivial absolute value on k.)

6. Absolute Values on Algebraic Number Fields

By an *algebraic number field* we understand a finite extension k of the rational field $\mathbb{Q}$. If $\| \ \|$ is a nontrivial absolute value on k, then by Exercise 5.1 the restriction of $\| \ \|$ to an absolute value on $\mathbb{Q}$ is also nontrivial. Hence the restriction of $\| \ \|$ to an absolute value on $\mathbb{Q}$ is equivalent to exactly one of the absolute values in the set

$$\big\{| \ |_\infty,\ | \ |_2,\ | \ |_3,\ | \ |_5,\ | \ |_7,\ \dots\big\},$$

as discussed in Theorem 5.1 of Chapter 2. Then Theorem 5.3 of the present chapter enables us to determine all the absolute values on k that extend one of the nontrivial absolute values on $\mathbb{Q}$.

It will be convenient to reformulate these observations in terms of the places of k and $\mathbb{Q}$. Let v denote a place of k, and write k_v for the completion of k at the place v. If the restriction of an absolute value from the place v to the subfield $\mathbb{Q}$ is equivalent to $| \ |_\infty$, then v is an archimedean place and we write $v|\infty$. In this case the completion k_v is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, and so the *local degree* $[k_v : \mathbb{Q}_\infty]$ is either 1 or 2. If the restriction of an absolute value from the place v to the subfield $\mathbb{Q}$ is equivalent to $| \ |_p$ for some prime number p, then v is a non-archimedean place and we write $v|p$. In this case the *local degree* $[k_v : \mathbb{Q}_p]$ is finite. By (5.8) the local degrees and the *global degree* $[k : \mathbb{Q}]$ are related by the basic identities

$$\sum_{v|\infty} [k_v : \mathbb{Q}_\infty] = [k : \mathbb{Q}] \quad \text{and} \quad \sum_{v|p} [k_v : \mathbb{Q}_p] = [k : \mathbb{Q}], \tag{6.1}$$

where the sums run over the (finite) set of all places v of k such that $v|\infty$ and $v|p$, respectively.

Exercises

6.1 Prove that for each positive integer N and prime number p the ring $\mathbb{Z}[x]$ contains a polynomial of degree N that is irreducible in $\mathbb{Q}_p[x]$.

7. The field Ω_p

Let p be a prime number and $\mathbb{Q}_p$ the field of p-adic numbers. By Theorem 4.2 the p-adic absolute value $| \ |_p$ on $\mathbb{Q}_p$ has a unique extension to an algebraic closure $\overline{\mathbb{Q}_p}$. Then by Theorem 2.1 of Chapter 2, $| \ |_p$ has a further extension to a completion of $\overline{\mathbb{Q}_p}$. Let Ω_p denote the completion of $\overline{\mathbb{Q}_p}$ with respect to $| \ |_p$. Obviously $(\Omega_p, | \ |_p)$ is a complete metric space. Evidently we can now form an algebraic closure of Ω_p, but in fact we will show that Ω_p is already algebraically closed. This is the p-adic analogue of the fundamental theorem of algebra, which asserts that the field $\mathbb{C}$ is algebraically closed.

THEOREM 7.1. *Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{Q}_p$, and let Ω_p be the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\ |_p$. Then the field Ω_p is algebraically closed.*

PROOF. Write

$$O_p = \{\alpha \in \Omega_p : |\alpha|_p \leq 1\}$$

for the local ring in Ω_p. Then let

$$f(x) = x^N + a_1 x^{N-1} + a_2 x^{N-2} + \cdots + a_N \tag{7.1}$$

be a monic, irreducible polynomial in $O_p[x]$. Write $\operatorname{Disc}(f)$ for the discriminant of $f(x)$. Because Ω_p has characteristic zero and the coefficients of $f(x)$ belong to O_p, we find that

$$0 < |\operatorname{Disc}(f)|_p \leq 1.$$

Let

$$g(x) = x^N + b_1 x^{N-1} + b_2 x^{N-2} + \cdots + b_N$$

be a monic polynomial in $\overline{\mathbb{Q}_p}[x]$. Because $\overline{\mathbb{Q}_p}$ is dense in Ω_p we can select the coefficients $b_1, \ldots, b_N$ so that

$$|a_n - b_n|_p < |\operatorname{Disc}(f)|_p^2 \quad \text{for each} \quad n = 1, 2, \ldots, N.$$

As $\overline{\mathbb{Q}_p}$ is algebraically closed there exists a point β in $\overline{\mathbb{Q}_p}$ such that $g(\beta) = 0$. Clearly we must have $|b_n|_p \leq 1$ and therefore $|\beta|_p \leq 1$. It follows that

$$\begin{aligned} |f(\beta)|_p &= |f(\beta) - g(\beta)|_p \\ &= \big|(a_1 - b_1)\beta^{N-1} + (a_2 - b_2)\beta^{N-2} + \cdots + (a_N - b_N)\big|_p \\ &\leq \max\{|a_1 - b_1|_p, |a_2 - b_2|_p, \ldots, |a_N - b_N|_p\} \\ &< |\operatorname{Disc}(f)|_p^2. \end{aligned} \tag{7.2}$$

Using the fact that the discriminant of $f(x)$ can be expressed as the resultant of $f(x)$ and $f'(x)$, we find (see [2], Theorem 2, section 7.4, or [3], Exercise 30, section 14.6) that there exist polynomials $r(x)$ and $s(x)$ in $O_p[x]$ such that

$$r(x)f(x) + s(x)f'(x) = \operatorname{Disc}(f).$$

As

$$|r(\beta)f(\beta)|_p \leq |f(\beta)|_p < |\operatorname{Disc}(f)|_p^2 \leq |\operatorname{Disc}(f)|_p,$$

we conclude that

$$|\operatorname{Disc}(f)|_p = |s(\beta)f'(\beta)|_p \leq |f'(\beta)|_p. \tag{7.3}$$

Combining (7.2) and (7.3) leads to the inequality

$$|f(\beta)|_p < |f'(\beta)|^2.$$

Thus we may apply Theorem 3.1 of Chapter 2, and conclude that $f(\alpha) = 0$ at some point α in O_p. We have shown that the monic, irreducible polynomial $f(x)$ in $O_p[x]$ must be linear.

Now suppose that $f(x)$ is a monic irreducible polynomial in $\Omega_p[x]$ given by (7.1). For nonnegative integers m define

$$F_m(x) = p^{mN} f(p^{-m}x) = x^N + a_1 p^m x^{N-1} + a_2 p^{2m} x^{N-2} + \cdots + a_N p^{Nm}.$$

If m is sufficiently large then $F_m(x)$ is a monic polynomial in $O_p[x]$. We also have

$$f(x) = p^{-mN} F_m(p^m x).$$

Thus $F_m(x)$ is irreducible in $\Omega_p[x]$ because $f(x)$ is irreducible in $\Omega_p[x]$. By the case already considered $F_m(x)$ is linear, and therefore $f(x)$ is also linear. This shows that Ω_p is algebraically closed.

Exercises

1.1 Let p be a prime number. Write O_p for the local ring in Ω_p and

$$M_p = \{\alpha \in \Omega_p : |\alpha|_p < 1\}$$

for its unique maximal ideal. Let $\mathbb{F}_p$ denote the finite field with p elements and write $\overline{\mathbb{F}_p}$ for an algebraic closure of $\mathbb{F}_p$. Prove that the residue class field O_p/M_p is isomorphic to $\overline{\mathbb{F}_p}$.

References for Chapter 3

1. J. W. S. Cassels, *Local Fields*, London Math. Soc. Student Texts 3, Cambridge University Press, 1986.
2. P. M. Cohn, *Classic Algebra*, Wiley, Chichester, England, 2000.
3. D. S. Dummit and R. F. Foote, *Abstract Algebra*, second edition, Prentice Hall, Saddle River, New Jersey, 1999.
4. S. Lang, *Algebra*, third edition, Addison Wesley, New York.
5. P. Ribenboim, *The Theory of Classical Valuations*, Springer-Verlag, New York, 1999.
6. A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1974.

1227, September 17, 2007