CHAPTER II

LOCAL FIELDS

1. Absolute Values

Let k be a field. An *absolute value* on k is a map $x \to |x|$ from k into the nonnegative real numbers that satisfies the following three conditions:

(i) $|x| = 0$ if and only if $x = 0$,

(ii) $|xy| = |x||y|$ for all x and y in k,

(iii) $|x + y| \leq |x| + |y|$ for all x and y in k.

The first results about a field with an absolute value are immediate consequences of the definition, and we organize them as a series of remarks.

Every field k has at least one absolute value which we denote here by $|\ |_0$. This is defined by

$$|x|_0 = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0. \end{cases}$$

The absolute value $|\ |_0$ is called the *trivial* or *improper* absolute value. Any other absolute values on k will be called *nontrivial* or *proper*. When working in a field k the trivial absolute value is usually not considered. However, there is at least one situation in which the trivial absolute value may appear quite naturally. Suppose that K is an extension of k and $|\ |$ is an absolute value on K. Then $|\ |$ restricted to k is obviously an absolute value on k. It may happen that $|\ |$ is a nontrivial absolute value on K, but the restriction $|\ |$ to k is trivial.

Let $k^\times$ denote the multiplicative group of nonzero elements in k. If $|\ |$ is an absolute value on k then the restriction of $|\ |$ to $k^\times$ is a homomorphism from the multiplicative group $k^\times$ into the multiplicative group of positive real numbers. It follows that $|1_k| = 1$ and more generally, if ζ is an nth root of unity in $k^\times$ then $|\zeta| = 1$. We also get

$$|-x| = |x| \quad \text{for all } x \in k, \quad \text{and} \quad |x^{-1}| = |x|^{-1} \quad \text{for all } x \in k^\times.$$

If x is in $k^\times$ and $|x| \neq 1$ then x must have infinite order in the multiplicative group $k^\times$. This shows that the only absolute value on a finite field is the trivial absolute value.

When verifying that a function $|\ | : k \to [0, \infty)$ is an absolute value, it is sometimes useful to be able to check an inequality that is weaker than the triangle inequality.

LEMMA 1.1. *Assume that k is a field and $|\ |: k \to [0,\infty)$ satisfies the three conditions*

(i) $|x| = 0$ *if and only if* $x = 0$,

(ii) $|xy| = |x||y|$ *for all* x *and* y *in* k,

(iv) $|x+y| \le 2\max\{|x|,|y|\}$ *for all* x *and* y *in* k.

Then $|\ |$ satisfies the triangle inequality (iii) *in the definition of an absolute value, and therefore $|\ |$ is an absolute value on k.*

PROOF. If $M = 2^m$ for some positive integer m, then it follows easily from (iv), by induction on m, that

$$|x_1 + x_2 + \cdots + x_M| \le 2^m \max\{|x_1|, |x_2|, \ldots, |x_M|\} \tag{1.1}$$

for all $x_1, x_2, \ldots, x_M$ in k. If N is a positive integer and $2^{m-1} < N \le 2^m$, then by selecting $x_{N+1} = x_{N+2} = \cdots = x_M = 0$ in (1.1), we find that

$$\begin{aligned} |x_1 + x_2 + \cdots + x_N| &\le 2^m \max\{|x_1|, |x_2|, \ldots, |x_N|\} \\ &\le 2N \max\{|x_1|, |x_2|, \ldots, |x_N|\} \end{aligned} \tag{1.2}$$

for all $x_1, x_2, \ldots, x_N$ in k. In particular, if $x_1 = x_2 = \cdots = x_N = 1$, then it follows that

$$|N| \le 2N. \tag{1.3}$$

Now let x and y be elements of k, and let L be a positive integer. Then using (1.2) and (1.3) we get

$$\begin{aligned} |x+y|^L &= |(x+y)^L| \\ &= \Big|\sum_{l=0}^{L} \binom{L}{l} x^l y^{L-l}\Big| \\ &\le 2(L+1)\max\left\{\Big|\binom{L}{l}\Big||x|^l|y|^{L-l} : 0 \le l \le L\right\} \\ &\le 4(L+1)\max\left\{\binom{L}{l}|x|^l|y|^{L-l} : 0 \le l \le L\right\} \\ &\le 4(L+1)\sum_{l=0}^{L}\binom{L}{l}|x|^l|y|^{L-l} \\ &= 4(L+1)\big(|x|+|y|\big)^L, \end{aligned}$$

and therefore

$$|x+y| \le \big(4(L+1)\big)^{1/L}\big(|x|+|y|\big). \tag{1.4}$$

The triangle inequality (iii) follows now by letting $L \to \infty$ in (1.4).

If $|\ |$ is an absolute value on k then the map $(x, y) \to |x - y|$ from $k \times k$ into $[0, \infty)$ is a metric, and therefore the absolute value induces a metric topology in k. The distance from x to y is $|x - y|$. Let $\mathcal{A}_k$ denote the set of absolute values on k. We say that two absolute values in $\mathcal{A}_k$ are *equivalent* if they induce the same metric topology. It is easy to verify that this is in fact an equivalence relation in $\mathcal{A}_k$. The trivial absolute value $|\ |_0$ clearly induces the discrete topology in k, and it is the unique absolute value in its equivalence class. We will show that an equivalence class determined by a nontrivial absolute value contains many distinct, nontrivial absolute values. An equivalence class determined by a nontrivial absolute value in $\mathcal{A}_k$ is called a *place* of k. Equivalent absolute values on k can be characterized in a simple way.

THEOREM 1.2. *Let $|\ |_1$ and $|\ |_2$ be absolute values on k. Then the following assertions are equivalent:*

(1) *$|\ |_1$ and $|\ |_2$ induce the same metric topology in k,*
(2) *$\{x \in k : |x|_1 < 1\} = \{x \in k : |x|_2 < 1\}$,*
(3) *there exists a positive number θ such that $|x|_1^\theta = |x|_2$ for all x in k.*

PROOF. Assume that (1) holds and let

$$U_j = \{x \in k : |x|_j < 1\}, \quad \text{for} \quad j = 1, 2.$$

If x belongs to U_1 then $\{x^n\}_{n=1}^\infty$ is a sequence that converges to 0 in k. As U_2 is an open neighborhood of 0 we must have x^N in U_2 for some sufficiently large integer N. But $|x^N|_2 < 1$ implies that $|x|_2^N < 1$, and therefore $|x|_2 < 1$. It follows that $U_1 \subseteq U_2$, and by symmetry $U_2 \subseteq U_1$. Thus condition (2) is satisfied.

Now assume that (2) holds. If either $|\ |_1$ or $|\ |_2$ is trivial then (3) follows immediately. Therefore we may assume that both $|\ |_1$ and $|\ |_2$ are nontrivial. Let y in k satisfy $|y|_1 \neq 0$ and $|y|_1 \neq 1$. By replacing y with y^{-1} if necessary, we may further assume that $0 < |y|_1 < 1$. From (2) we have $0 < |y|_2 < 1$. Hence

$$\theta = \frac{\log |y|_2}{\log |y|_1}$$

is a positive real number. We claim that $|x|_1^\theta = |x|_2$ for all x in k. If this claim is false then by replacing x with x^{-1} if necessary, there exists a point x in k with

$$|x|_1^\theta < |x|_2.$$

Now select a rational number r/s such that

$$|x|_1^\theta < |y|_1^{\theta r/s} = |y|_2^{r/s} < |x|_2.$$

This choice is possible because the image of the map $r/s \to |y|_2^{r/s}$ is dense in $(0,\infty)$. Then we have

$$|x^s|_1^\theta < |y^r|_1^\theta = |y^r|_2 < |x^s|_2,$$

and it follows that

$$|x^s y^{-r}|_1 < 1, \quad \text{and} \quad 1 < |x^s y^{-r}|_2.$$

This contradicts (2) and so verifies our claim. Thus (3) is satisfied.

Assume that (3) holds. Then the set of all open balls in the $|\ |_1$-topology is equal to the set of all open balls in the $|\ |_2$-topology. The assertion (1) follows.

Let $|\ |$ be an absolute value on k, and let $0 < \theta < 1$. It is obvious that $x \to |x|^\theta$ satisfies the conditions (i) and (ii) in the hypotheses of Lemma 1.1. Also, condition (iv) holds because

$$|x+y|^\theta \le \big(|x|+|y|\big)^\theta \le 2^\theta \max\big\{|x|^\theta, |y|^\theta\big\}.$$

It follows then from Lemma 1.1 that $|\ |^\theta$ is an absolute value on k. By Theorem 1.2, for each value of θ with $0 < \theta < 1$, the absolute value $|\ |^\theta$ is equivalent to $|\ |$. If we further assume that $|\ |$ is nontrivial, then $|z| \ne 1$ for some point z in $k^\times$, and we conclude that $|\ |^\theta$ and $|\ |$ are equivalent but not equal. In particular, this shows that the place determined by $|\ |$ in $\mathcal{A}_k$ contains many distinct but equivalent absolute values.

Let $|\ |$ be an absolute value on k. Then define

$$\Theta(|\ |) = \{\theta > 0 : x \to |x|^\theta \text{ is an absolute value in } \mathcal{A}_k\}.$$

It follows from the definition of an absolute value that $\Theta(|\ |)$ is a closed, nonempty subset of $(0,\infty)$. By our previous remarks, if τ is in $\Theta(|\ |)$ then $\theta\tau$ is in $\Theta(|\ |)$ for all θ such that $0 < \theta \le 1$. This shows that either $\Theta(|\ |) = (0,\infty)$, or $\Theta(|\ |) = (0,\tau]$ for some real number $\tau \ge 1$. We define a second function on absolute values in $\mathcal{A}_k$ by setting

$$\Phi(|\ |) = \sup\{|x+1| : x \in k \text{ and } |x| \le 1\}.$$

Obviously we have $1 \le \Phi(|\ |) \le 2$. Also, the inequality

$$|x+y| \le \Phi(|\ |)\max\{|x|,|y|\} \tag{1.5}$$

holds for all x and y in k. To verify (1.5) assume that $0 < |x| \le |y|$. Then we have

$$|x+y| = |(xy^{-1}+1)y| = |xy^{-1}+1||y| \le \Phi(|\ |)|y| = \Phi(|\ |)\max\{|x|,|y|\}.$$

Note that if $\Phi(|\ |) = 1$ then (1.5) is stronger than the triangle inequality (iii) in the definition of an absolute value.

THEOREM 1.3. *Let $|\ |$ be an absolute value on k. Then the following assertions are equivalent:*

(1) $\Theta(|\ |) = (0, \infty)$,
(2) $|x + y| \le \max\{|x|, |y|\}$ *for all x and y in k,*
(3) $\Phi(|\ |) = 1$.

Moreover, if $1 < \Phi(|\ |) \le 2$, then $\Theta(|\ |) = (0, \tau]$ for some real number $\tau \ge 1$, and

$$\Phi(|\ |)^\tau = 2. \tag{1.6}$$

PROOF. Assume that $\Theta(|\ |) = (0, \infty)$. Then the map $x \to |x|^n$ is an absolute value for all positive integers n. It follows that

$$|x + y| \le \left\{|x|^n + |y|^n\right\}^{1/n}$$

for all x and y in k. We let $n \to \infty$ and conclude that

$$|x + y| \le \max\{|x|, |y|\}.$$

This shows that (1) implies (2).

It is trivial that (2) implies (3).

Assume that $\Phi(|\ |) = 1$. In view of (1.5) we find that (2) is satisfied. Then we get

$$\begin{aligned} |x + y|^\theta &\le \big(\max\{|x|, |y|\}\big)^\theta \\ &= \max\{|x|^\theta, |y|^\theta\} \\ &\le |x|^\theta + |y|^\theta \end{aligned}$$

for all x and y in k and for all positive θ. This shows that the map $x \to |x|^\theta$ is an absolute value on k for all positive θ, and so verifies that $\Theta(|\ |) = (0, \infty)$. We have shown that (3) implies (1).

Assume that $1 < \Phi(|\ |) \le 2$. By our previous remarks we have $\Theta(|\ |) = (0, \tau]$ for some real number $\tau \ge 1$. Because $|\ |^\tau$ is an absolute value, we find that

$$\begin{aligned} \Phi(|\ |)^\tau &= \Phi\big(|\ |^\tau\big) \\ &= \sup\{|x + 1|^\tau : x \in k \text{ and } |x|^\tau \le 1\} \\ &\le 2. \end{aligned}$$

If in fact $\Phi(|\ |)^\tau < 2$, then there exists $\theta > \tau$ such that

$$\Phi\big(|\ |^\theta\big) = \Phi(|\ |)^\theta \le 2.$$

It follows from (1.5) that

$$|x+y|^\theta \le 2\max\{|x|^\theta, |y|^\theta\} \tag{1.7}$$

for all x and y in k. From Lemma 1.1 and (1.7) we conclude that $x \to |x|^\theta$ is an absolute value on k. As $\theta > \tau$, this contradicts the definition of $\Theta(|\ |)$. We have shown that if $1 < \Phi(|\ |) \le 2$, then (1.6) holds.

We are now in position to distinguish between different types of absolute values. If $|\ |$ is an absolute value on k then by Theorem 1.3, $\Phi(|\ |) = 1$ if and only if the absolute value satisfies the inequality

$$|x+y| \le \max\{|x|, |y|\} \tag{1.8}$$

for all x and y in k. An absolute value that satisfies (1.8) is said to be a *non-archimedean* absolute value or to be an *ultrametric* absolute value. Then (1.8) is called the *strong triangle* inequality or the *ultrametric* inequality. If $|\ |$ is a non-archimedean absolute value then the equivalence class it represents in $\mathcal{A}_k$ is the set

$$\{|\ |^\theta : 0 < \theta < \infty\}.$$

Each absolute value in this equivalence class is also non-archimedean and so we may refer to it as a non-archimedean equivalence class. We note that the trivial absolute value $|\ |_0$ is non-archimedean and it is the only absolute value in its equivalence class.

If $1 < \Phi(|\ |) \le 2$ then by Theorem 1.3 we know that (1.8) does not hold, but $|\ |$ does satisfy the ordinary triangle inequality (iii) in the definition of an absolute value. In this case we say that $|\ |$ is an *archimedean* absolute value. The equivalence class it represents is

$$\{|\ |^\theta : 0 < \theta \le \tau\}, \qquad \text{where } \tau = \frac{\log 2}{\log \Phi(|\ |)}.$$

Obviously all the absolute values in this equivalence class are archimedean and so we may refer to it as an archimedean equivalence class.

If the absolute value $|\ |$ is nontrivial then the equivalence class it represents is a place of k, and we may speak of non-archimedean places or archimedean places.

We now establish a basic result due to K. Mahler that demonstrates how inequivalent absolute values behave independently. We require the following lemma.

LEMMA 1.4. *Let k be a field and let $\{|\ |_n : 1 \le n \le N\}$ be a finite collection of inequivalent, nontrivial, absolute values on k. Then there exists a point α in k such that $|\alpha|_1 > 1$, and $|\alpha|_n < 1$ for $2 \le n \le N$.*

PROOF. Suppose that $N = 2$. As $|\ |_1$ and $|\ |_2$ are inequivalent, by Theorem 1.2 there exists β in k with

$$|\beta|_1 < 1 \quad \text{and} \quad 1 \le |\beta|_2,$$

and there exists γ in k with

$$1 \le |\gamma|_1 \quad \text{and} \quad |\gamma|_2 < 1.$$

In this case we take $\alpha_1 = \gamma\beta^{-1}$.

We continue now using induction on N. By the inductive hypothesis there exists β in k with

$$|\beta|_1 > 1 \quad \text{and} \quad |\beta|_n < 1 \text{ for } 2 \le n \le N-1,$$

and γ in k with

$$1 \le |\gamma|_1 \quad \text{and} \quad |\gamma|_N < 1.$$

There are three cases to consider:

(i) if $|\beta|_N < 1$ we take $\alpha = \beta$,

(ii) if $|\beta|_N = 1$ we take $\alpha = \beta^l\gamma$ with a large positive integer l,

(iii) if $|\beta|_N > 1$ we take $\alpha = \beta^l\gamma(1+\beta^l)^{-1}$ with a large positive integer l.

In each case it is easy to check that α satisfies the requirements of the lemma when l is sufficiently large.

THEOREM 1.5 (THE WEAK APPROXIMATION THEOREM). *Let k be a field, let $\{|\ |_n : 1 \le n \le N\}$ be a finite collection of inequivalent, nontrivial, absolute values on k and $\{x_n : 1 \le n \le N\}$ a collection of points in k. Then for every $\epsilon > 0$ there exists a point y in k such that*

$$|x_n - y|_n < \epsilon \quad \textit{for each } n = 1, 2, \ldots, N.$$

PROOF. For each integer n with $1 \le n \le N$ we apply Lemma 1.4 but with $|\ |_n$ in place of $|\ |_1$. In this way we determine a collection of points $\alpha_1, \alpha_2, \ldots, \alpha_N$ in k such that

$$|\alpha_m|_n > 1 \text{ if } m = n, \text{ and } |\alpha_m|_n < 1 \text{ if } m \ne n.$$

Then we find that

$$\lim_{l\to\infty} \frac{\alpha_m^l}{1+\alpha_m^l} = 1 \quad \text{in the } |\ |_n\text{-metric if } m = n,$$

and

$$\lim_{l\to\infty} \frac{\alpha_m^l}{1+\alpha_m^l} = 0 \quad \text{in the } |\ |_n\text{-metric if } m \ne n.$$

It follows that for each n, $1 \le n \le N$, we have

$$\lim_{l\to\infty} \sum_{m=1}^{N} \frac{x_m\alpha_m^l}{1+\alpha_m^l} = x_n \quad \text{in the } |\ |_n\text{-metric.}$$

Hence we may take

$$y = \sum_{m=1}^{N} \frac{x_m \alpha_m^l}{1 + \alpha_m^l}$$

with l a sufficiently large positive integer that depends on ϵ.

Given a field k it is an interesting problem to determine all the nontrivial absolute values on k. The following result is useful when the field k is the field of fractions of an integral domain.

LEMMA 1.6. *Let R be in integral domain and let k be its field of fractions. Assume that $x \to \|x\|$ is a map from R to $[0, \infty)$ that satisfies the three conditions*

(1) $\|x\| = 0$ *if and only if* $x = 0$,
(2) $\|xy\| = \|x\|\|y\|$ *for all x and y in R,*
(3) $\|x + y\| \le \|x\| + \|y\|$ *for all x and y in R.*

Then there exists a unique absolute value $|\ | : k \to [0, \infty)$ such that $|x| = \|x\|$ for all x in R. If $\|\ \|$ on R satisfies the strong triangle inequality

(4) $\|x + y\| \le \max\{\|x\|, \|y\|\}$ *for all x and y in R,*

then $|\ |$ on k is a non-archimedean absolute value. Moreover, if a and $b \neq 0$ are in R, and a/b is a point in k, then these maps satisfy the identity

$$\Big|\frac{a}{b}\Big| = \frac{\|a\|}{\|b\|}. \tag{1.9}$$

PROOF. Suppose that $a/b = c/d$ in k. That is, a, $b \neq 0$, c and $d \neq 0$ belong to R and $ad = bc$. It follows that $\|a\|\|d\| = \|b\|\|c\|$ and

$$\frac{\|a\|}{\|b\|} = \frac{\|c\|}{\|d\|}$$

in $[0, \infty)$. Therefore we define a map $|\ | : k \to [0, \infty)$ by

$$\Big|\frac{a}{b}\Big| = \frac{\|a\|}{\|b\|}.$$

Our previous remarks show that this is well defined. Using (1), (2) and (3) it is easy to verify that $|\ |$ on k satisfies the corresponding conditions required of an absolute value. For example, if a, $b \neq 0$, c and $d \neq 0$ belong to R, then

$$\begin{aligned}\Big|\frac{a}{b} + \frac{c}{d}\Big| = \Big|\frac{ad + bc}{bd}\Big| &= \frac{\|ad + bc\|}{\|bd\|} \\ &\le \frac{\|ad\| + \|bc\|}{\|bd\|} = \frac{\|a\|}{\|b\|} + \frac{\|c\|}{\|d\|} = \Big|\frac{a}{b}\Big| + \Big|\frac{c}{d}\Big|.\end{aligned}$$

If (4) holds this calculation becomes

$$\Big|\frac{a}{b}+\frac{c}{d}\Big| = \Big|\frac{ad+bc}{bd}\Big| = \frac{\|ad+bc\|}{\|bd\|}$$
$$\leq \frac{\max\big\{\|ad\|,\|bc\|\big\}}{\|bd\|} = \max\left\{\frac{\|a\|}{\|b\|},\frac{\|c\|}{\|d\|}\right\} = \max\Big\{\Big|\frac{a}{b}\Big|,\Big|\frac{c}{d}\Big|\Big\},$$

and we conclude that the absolute value $|\ |$ is non-archimedean.

We note that (2) implies that $\|y\| = \|1y\| = \|1\|\|y\|$ and therefore $\|1\| = 1$. Now if a belongs to R then

$$|a| = \Big|\frac{a}{1}\Big| = \frac{\|a\|}{\|1\|} = \|a\|,$$

and this shows that $|\ |$ on k is an extension of $\|\ \|$ on R. If $|\ |_1$ and $|\ |_2$ are both absolute values on k that extend the map $\|\ \|$ on R, then we have

$$\Big|\frac{a}{b}\Big|_1 = \frac{|a|_1}{|b|_1} = \frac{\|a\|}{\|b\|} = \frac{|a|_2}{|b|_2} = \Big|\frac{a}{b}\Big|_2.$$

This shows that in fact $|\ |_1$ and $|\ |_2$ are equal on k. Thus the absolute value defined by (1.9) is the unique extension of $\|\ \|$ on R.

Exercises

1.1 Let $|\ |$ be an absolute value on the field k. Prove that $|\ |$ is non-archimedean if and only if $|n1_k| \leq 1$ for all integers n, where 1_k is the multiplicative identity element in k.

1.2 Let k be a field of positive characteristic. Prove that every absolute value on k is non-archimedean.

1.3 Assume that $|\ |_1$ and $|\ |_2$ are nontrivial absolute values on a field k that satisfy the condition

$$\{x \in k : |x|_1 < 1\} \subseteq \{x \in k : |x|_2 < 1\}. \tag{1.10}$$

Prove that $|\ |_1$ and $|\ |_2$ are equivalent.

1.4 Assume that $|\ |$ is an absolute value on a field k, and let

$$\Theta(|\ |) = \{\theta > 0 : x \to |x|^\theta \text{ is an absolute value in } \mathcal{A}_k\}.$$

Prove that $\Theta(|\ |)$ is a closed subset of $(0,\infty)$.

1.5 Assume that $|\ |$ is a non-archimedean absolute value on a field k, $x_1, x_2, \ldots, x_N$ are point in k, and

$$x_1 + x_2 + \cdots + x_N = 0.$$

Prove that there exist integers m and n such that $1 \leq m < n \leq N$ such that

$$|x_m| = |x_n| = \max\{|x_1|, |x_2|, \ldots, |x_N|\}.$$

1.6 Let k be a field with a nontrivial absolute value $|\ |$. Prove that each polynomial f in $k[x_1, x_2, \ldots, x_N]$ defines a continuous function $f : k^N \to k^N$, where k^N has the product topology. Then prove that $x \to x^{-1}$ defines a continuous function from $k^\times$ onto $k^\times$. Formulate a result about the continuity of a rational function F in $k(x_1, x_2, \ldots, x_N)$.

2. Completions

Let k be a field and $|\ |$ an absolute value on k. We say that k is *complete* if k is a complete metric space with respect to the metric topology induced by $|\ |$. That is, k is *complete* if every Cauchy sequence in k converges to a point in k. We note that completeness is a property of the metric topology; it does not depend on the particular absolute value in the place determined by $|\ |$. If $|\ |_1$ and $|\ |_2$ are equivalent absolute values on k, then k is complete with respect to $|\ |_1$ if and only if it is complete with respect to $|\ |_2$.

Let k be a field with an absolute value $|\ |_k$, and l a field with an absolute value $|\ |_l$. A map $\sigma : k \to l$ is an *isometric isomorphism* if σ is an isomorphism of k onto l and $|x|_k = |\sigma(x)|_l$ for all x in k. In this case it is obvious that $\sigma^{-1} : l \to k$ is also an isometric isomorphism and we say that the pair $(k, |\ |_k)$ and the pair $(l, |\ |_l)$ are *isometrically isomorphic*. A map $\sigma : k \to l$ is an *isometric embedding* if σ is an isomorphism of k onto a subfield of l and $|x|_k = |\sigma(x)|_l$ for all x in k.

A pair $(K, |\ |_K)$, consisting of a field K and an absolute value $|\ |_K$, is a *completion* of the pair $(k, |\ |_k)$ if

(i) K is complete with respect to the metric topology induced by $|\ |_K$, and

(ii) there exists an isometric embedding σ of k onto a dense subfield of K.

Completions always exist and are unique up to an isometric isomorphism. The precise result is as follows.

THEOREM 2.1. *Let $(k, |\ |_k)$ be a pair consisting of a field k and an absolute value $|\ |_k$. Then there exists a pair $(K, |\ |_K)$ that is a completion of $(k, |\ |_k)$. Moreover, if $(K, |\ |_K)$ and $(L, |\ |_L)$ are both completions of $(k, |\ |_k)$, if $\sigma_K : k \to K$ and $\sigma_L : k \to L$ are the corresponding isometric embeddings, then there exists a unique isometric isomorphism $\tau : K \to L$ such that $\tau \circ \sigma_K = \sigma_L$.*

SKETCH OF THE PROOF. Let $C(k)$ be the set of all maps $a : \{1, 2, \dots\} \to k$ such that $\{a(n)\}_{n=1}^{\infty}$ is a Cauchy sequence in k. Then $C(k)$ is obviously a commutative ring with respect to the operations

$$\{a + b\}(n) = a(n) + b(n) \quad \text{and} \quad \{ab\}(n) = a(n)b(n).$$

Let $M(k) \subseteq C(k)$ be the subset of Cauchy sequences that converge to 0 in k. Then $M(k)$ is a maximal ideal and therefore the quotient ring

$$K = C(k)/M(k)$$

is a field.

Next we define an absolute value $|\ |_K$ on K. If $\{a(n)\}_{n=1}^{\infty}$ is a Cauchy sequence then the inequality

$$-|a(m) - a(n)|_k \leq |a(m)|_k - |a(n)|_k \leq |a(m) - a(n)|_k$$

shows that $\{|a(n)|_k\}_{n=1}^{\infty}$ is a Cauchy sequence in $[0, \infty)$. If $\{b(n)\}_{n=1}^{\infty}$ represents the same coset in K as $\{a(n)\}_{n=1}^{\infty}$ then

$$\lim_{n\to\infty} |a(n) - b(n)|_k = 0$$

and therefore

$$\lim_{n\to\infty} |a(n)|_k = \lim_{n\to\infty} |b(n)|_k.$$

This shows that the map

$$\{a(n)\}_{n=1}^{\infty} \to |\{a(n)\}_{n=1}^{\infty}|_K = \lim_{n\to\infty} |a(n)|_k,$$

from $C(k)$ into $[0, \infty)$, is well defined on the field K. It follows easily that $|\ |_K$ is an absolute value on K.

If α belongs to k let $\sigma(\alpha) : \{1, 2, \dots\} \to k$ be the constant sequence defined by $\sigma(\alpha)(n) = \alpha$ for all $n = 1, 2, \dots$. Obviously this sequence is Cauchy and so determines a coset in K. The map $\sigma : k \to K$ is an embedding, an isometry with respect to the metrics induced by $|\ |_k$ and $|\ |_K$, and its image is dense in K. Thus the pair $(K, |\ |_K)$ satisfies the requirements of a completion.

Finally, let $\sigma_K : k \to K$ and $\sigma_L : k \to L$ be isometric embeddings. Then define $\tau : \sigma_K(k) \to \sigma_L(k)$ by $\tau(x) = \sigma_L \circ \sigma_K^{-1}(x)$. It follows that $\tau^{-1}(y) = \sigma_K \circ \sigma_L^{-1}(y)$, and it can be shown that τ and τ^{-1} are both continuous. Because $\sigma_K(k)$ and $\sigma_L(k)$ are dense in K and L, respectively, both τ and τ^{-1} have unique extensions to continuous maps

$$\tau : K \to L \quad \text{and} \quad \tau^{-1} : L \to K.$$

Continuity can now be used to show that the extended maps are isometric isomorphisms.

In the notation of Theorem 2.1, k is isomorphic to its image $\sigma(k)$ in the completion K. Thus we may identify k and $\sigma(k)$ and so regard k as a dense subfield of K. Then it is obvious that $|\ |_K$ on K is an extension of $|\ |_k$ on the dense subfield k, and therefore $\Phi(|\ |_k) = \Phi(|\ |_K)$. In particular, $|\ |_k$ and $|\ |_K$ are either both archimedean, or they are both non-archimedean.

Let $|\ |_\infty$ denote the usual archimedean absolute value on the fields $\mathbb{R}$ and $\mathbb{C}$. Then $(\mathbb{R}, |\ |_\infty)$ and $(\mathbb{C}, |\ |_\infty)$ are both complete. It is a result of Ostrowski [6] (see also, [8], Chapter 1, Theorem S) that these are essentially the only examples of complete archimedean fields.

THEOREM 2.2. *Let K be a field that is complete with respect to an archimedean absolute value $|\ |_K$. Then there exists θ, $0 < \theta \le 1$, such that $(K, |\ |_K)$ is isometrically isomorphic to either $(\mathbb{R}, |\ |_\infty^\theta)$ or $(\mathbb{C}, |\ |_\infty^\theta)$.*

For the remainder of this section we assume that k is a field with a nontrivial, non-archimedean absolute value $|\ |$. We write K for a completion of k and then we continue to use $|\ |$ for the extended absolute value on K. We also identify k with its image in K and so speak of k as a dense subfield of K. Because $|\ |$ satisfies the strong triangle inequality (1.8), some aspects of elementary analysis in K are simpler than in the case of an archimedean absolute value. Suppose, for example, that α and β are in K and $|\alpha| < |\beta|$. Then we have

$$\begin{aligned} |\beta| &= |\alpha + \beta - \alpha| \\ &\le \max\{|\alpha + \beta|, |\alpha|\} \\ &= |\alpha + \beta| \qquad \text{(since the maximum cannot occur at } |\alpha|) \\ &\le \max\{|\alpha|, |\beta|\} \\ &= |\beta|, \end{aligned}$$

and therefore

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

More generally, if $\alpha_1, \alpha_2, \ldots \alpha_N$ are in K, if $|\alpha_n| < |\alpha_N|$ for $1 \le n < N$, then

$$|\alpha_1 + \alpha_2 + \cdots + \alpha_N| = |\alpha_N|. \tag{2.1}$$

We often refer to (2.1) as the case of equality in the strong triangle inequality. Of course the hypothesis $|\alpha_n| < |\alpha_N|$ is a sufficient condition for (2.1) to hold, but it is not a necessary condition. If $\alpha_1, \alpha_2, \ldots$ is an infinite series in K then the strong triangle inequality implies that

$$\lim_{N\to\infty} \sum_{n=1}^{N} \alpha_n \quad \text{exists if and only if} \quad \lim_{N\to\infty} \alpha_N = 0. \tag{2.2}$$

Next we define

$$O_k = \{\alpha \in k : |\alpha| \leq 1\}, \qquad O_K = \{\alpha \in K : |\alpha| \leq 1\},$$

$$U_k = \{\alpha \in k : |\alpha| = 1\}, \qquad U_K = \{\alpha \in K : |\alpha| = 1\},$$

$$M_k = \{\alpha \in k : |\alpha| < 1\}, \qquad M_K = \{\alpha \in K : |\alpha| < 1\}.$$

Because $|\ |$ is non-archimedean, it is easy to check that the closed unit ball O_k is an integral domain. Then U_k is exactly the multiplicative group of invertible elements in O_k, and M_k is the unique maximal ideal in O_k. Plainly these sets depend on the equivalence class determined by $|\ |$ and not on the particular choice of absolute value in the equivalence class. As M_k is a maximal ideal, the quotient ring O_k/M_k is a field, called the *residue class field* of k. As the ring O_k has a unique maximal ideal M_k, it is an example of a *local ring*. Of course these remarks also apply to the sets O_K, U_K and M_K.

An element α in O_k obviously determines a coset $\alpha + M_k$ in the residue class field O_k/M_k. When α in O_k is regarded as an element of O_K it determines a coset $\alpha + M_K$ in the residue class field O_K/M_K. Thus there is a map

$$\psi : O_k/M_k \to O_K/M_K \quad \text{given by} \quad \psi\{\alpha + M_k\} = \alpha + M_K,$$

and it is trivial to check that it is well defined and an isomorphism of O_k/M_k onto a subfield of O_K/M_K. In fact, we will show that this map is surjective.

LEMMA 2.3. *The map $\psi : O_k/M_k \to O_K/M_K$ is an isomorphism of O_k/M_k onto O_K/M_K*

PROOF. Let $\beta + M_K$ be a coset in O_K/M_K. Because k is dense in K there exists α in k such that $|\alpha - \beta| < 1$. Then $|\alpha| \leq \max\{|\alpha - \beta|, |\beta|\} \leq 1$, and it follows that α is in O_k and $\alpha - \beta$ is in M_K. That is,

$$\psi\{\alpha + M_k\} = \alpha + M_K = \beta + M_K,$$

and the lemma follows.

As $|\ |$ is a homomorphism from the multiplicative group $k^\times$ into the multiplicative group $(0, \infty)$ of positive real numbers, its image

$$|k^\times| = \{|\alpha| : \alpha \in k^\times\}$$

is a nontrivial subgroup. This subgroup is called the *multiplicative value group* of $(k, |\ |)$. We recall that a nontrivial subgroup $G \subseteq (0, \infty)$ is either discrete or dense in $(0, \infty)$, and G is a discrete, nontrivial subgroup if and only if it is an infinite cyclic subgroup. That

is, G is a discrete, nontrivial subgroup if and only if it has the form $G = \{t^n : n \in \mathbb{Z}\}$ for some real number t, $0 < t < 1$. We say that $|\ |$ is a *discrete* absolute value on k if its value group is a discrete, nontrivial subgroup of $(0, \infty)$. It is clear that $|\ |$ is discrete if and only if all the absolute values in the equivalence class it determines are discrete. Also, if $|\ |$ is a discrete absolute value on k then its extension to the completion K is also discrete and has the same multiplicative value group. We note that a nontrivial absolute value on k, or on its completion K, does *not* induce the discrete topology in either k or K. Only the trivial absolute value induces the discrete topology. A discrete absolute value has a discrete multiplicative value group, but it does *not* induce the discrete topology in k or K.

LEMMA 2.4. *A nontrivial, non-archimedean absolute value on k is discrete if and only if M_k is a principal, maximal ideal in the ring O_k.*

PROOF. It is evident from the definition of a discrete absolute value and from the definition of M_k, that $|\ |$ is discrete if and only if

$$\sup\{|\alpha| : \alpha \in M_k\} < 1.$$

Assume that M_k is principal and so generated by an element π. That is,

$$M_k = (\pi) = \{\beta\pi : \beta \in O_k\}.$$

Then we have

$$\sup\{|\alpha| : \alpha \in M_k\} = \sup\{|\beta\pi| : \beta \in O_k\} = |\pi|,$$

and $|\pi| < 1$ because π is in M_k. This shows that the multiplicative value group of $|\ |$ is discrete.

Now assume that $|\ |$ is discrete and so the multiplicative value group has the form

$$\{t^n : n \in \mathbb{Z}\} \quad \text{for some } t,\ 0 < t < 1.$$

Let π in M_k satisfy $|\pi| = t$. If α belongs to M_k let $\beta = \alpha\pi^{-1}$. Then $|\beta| = |\alpha||\pi|^{-1} \leq 1$ and therefore β is an element of O_k. Because $\alpha = \beta\pi$ this shows that $M_k \subseteq (\pi)$. As M_k is a maximal ideal we have $M_k = (\pi)$. We have shown that M_k is principal and this completes the proof.

The proof of Lemma 2.4 provides the following characterization of the elements that generate the maximal ideal M_k.

COROLLARY 2.5. *Let $|\ |$ be a discrete absolute value on k and let π be an element of the maximal ideal M_k. Then the following assertions are equivalent:*

(1) $M_k = (\pi) = \{\beta\pi : \beta \in O_k\}$,
(2) $\sup\{|\alpha| : \alpha \in M_k\} = |\pi|$,
(3) *the multiplicative value group of $(k, |\ |)$ is $\{|\pi|^n : n \in \mathbb{Z}\}$.*

An element π in M_k that satisfies one, and therefore all, of the three conditions in the statement of Corollary 2.5 is called a *prime element* of k. Obviously a prime element of k is also a prime element in the completion K.

We can use prime elements in the complete field K to make certain infinite series expansions. Let $R_K \subseteq O_K$ be a complete set of distinct coset representatives for the residue class field O_K/M_K and let π in M_K be a prime element. For each infinite sequence $\{a(n)\}_{n=0}^{\infty}$ of points in R_K the infinite series

$$\sum_{n=0}^{\infty} a(n)\pi^n = \lim_{N\to\infty} \sum_{n=0}^{N} a(n)\pi^n$$

plainly converges by (2.2) to a point in O_K. We will show that every point in O_K has an expansion of this sort.

THEOREM 2.6. *Let α be a point in O_K. Then there exists a unique sequence*

$$a(0), a(1), a(2), \ldots$$

of points in R_K such that

$$\alpha = \sum_{n=0}^{\infty} a(n)\pi^n. \tag{2.3}$$

PROOF. There is a unique point $a(0)$ in R_K so that $|\alpha - a(0)| < 1$. Hence we can write

$$\alpha = a(0) + b(1)\pi, \quad \text{with } b(1) \in O_K.$$

Then there is a unique point $a(1)$ in R_K so that $|b(1) - a(1)| < 1$. Therefore we get

$$\alpha = a(0) + a(1)\pi + b(2)\pi^2, \quad \text{with } b(2) \in O_K.$$

Continuing in this manner we determine two infinite sequences $\{a(n)\}_{n=0}^{\infty}$ and $\{b(n)\}_{n=1}^{\infty}$ such that each term $a(n)$ is in R_K, each term $b(n)$ is in O_K, and

$$\alpha = a(0) + a(1)\pi + a(2)\pi^2 + a(3)\pi^3 + \cdots + a(N-1)\pi^{N-1} + b(N)\pi^N$$

for each $N = 1, 2, 3, \ldots$. As

$$\lim_{N\to\infty} |b(N)\pi^N| = 0,$$

we find that (2.3) is satisfied.

Assume that $\{a'(n)\}_{n=0}^{\infty}$ is another sequence of points in R_K satisfying (2.3). Then we have

$$0 = \sum_{n=0}^{\infty} \{a(n) - a'(n)\}\pi^n. \tag{2.4}$$

For each nonnegative integer n, either $a(n) - a'(n) = 0$ or $|a(n) - a'(n)| = 1$. It follows, using (2.4) and the case of equality in the strong triangle inequality, that $a(n) - a'(n) = 0$ for all n. Thus the expansion (2.3) is unique.

In applications of Theorem 2.6 it is often useful to assume that the coset M_K is represented in R_K by 0. Then 0 is represented by the series in which $a(n) = 0$ for each n. Also, if (2.3) is the expansion of α in O_K, if $a(0) = a(1) = a(2) = \dots a(N-1) = 0$ and $a(N) \neq 0$, then by the case of equality in the strong triangle inequality we have $|\alpha| = |\pi|^N$. More generally, we get a similar expansion at each point of $K^\times$.

COROLLARY 2.7. *Let α be a point in $K^\times$ with $|\alpha| = |\pi|^L$ for some L in $\mathbb{Z}$. Assume that the coset M_K is represented in R_K by 0. Then there exists a unique sequence $\{a(n)\}_{n=L}^{\infty}$ of points in R_K such that*

$$\alpha = \sum_{n=L}^{\infty} a(n)\pi^n \quad \textit{and} \quad a(L) \neq 0. \tag{2.5}$$

PROOF. Apply the theorem to $\alpha\pi^{-L}$, then use the case of equality in the strong triangle inequality.

Exercises

2.1 Prove the equivalence asserted in (2.2).

2.2 Prove that a nontrivial subgroup $G \subseteq (0, \infty)$ is either discrete or dense in $(0, \infty)$, and G is a discrete, nontrivial subgroup if and only if it is an infinite cyclic subgroup.

2.3 Let k be a field, and let $\{|\ |_n : 1 \leq n \leq N\}$ be a finite collection of inequivalent, nontrivial, absolute values on k. Assume that $(K_n, |\ |_n)$ is a completion of $(k, |\ |_n)$ for each $1 \leq n \leq N$. Write

$$J = \prod_{n=1}^{N} K_n,$$

and give J the product topology. Let $\delta : k \to J$ be the diagonal map that sends a point α in k to the point $(\alpha, \alpha, \dots, \alpha)$ in J. Prove that the image $\delta(k)$ is dense in J.

2.4 Let L be a field with an absolute value $|\ |$, assume that L is complete and let $k \subseteq L$ be a subfield. Write K' for the closure of k in L. Prove that K' is a subfield of L, and show that $(K', |\ |)$ is a completion of $(k, |\ |)$.

3. Hensel's Lemma

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 continue to write

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

If k is a dense subfield of K then obviously $(K, |\ |)$ is a completion of $(k, |\ |)$. However, the dense subfield k would play no role in the results of this section. Therefore we begin more simply with the pair $(K, |\ |)$ and the integral domain O_K. In this setting one form of Hensel's lemma provides information about roots of certain polynomials in $O_K[x]$.

THEOREM 3.1 (HENSEL'S LEMMA). *Let $f(x)$ be a polynomial in $O_K[x]$ with positive degree. Assume that ξ_1 in O_K satisfies*

$$|f(\xi_1)| < |f'(\xi_1)|^2. \tag{3.1}$$

Then there exists a unique point α in the closed ball

$$B(f, \xi_1) = \Big\{x \in O_K : |x - \xi_1| \leq \frac{|f(\xi_1)|}{|f'(\xi_1)|}\Big\} \tag{3.2}$$

such that $f(\alpha) = 0$. Moreover, we have $f'(\alpha) \neq 0$, so that α is a simple zero of f.

This result asserts the existence of a root α for the polynomial f. However, the proof also provides a useful numerical method for calculating α.

For f in $O_K(x)$ we define

$$\mathcal{D}_f = \{x \in O_K : |f(x)| < |f'(x)|^2\}, \tag{3.3}$$

and we assume that $\mathcal{D}_f$ is not empty. Next we define a map $\psi : \mathcal{D}_f \to K$ by

$$\psi(x) = x - \frac{f(x)}{f'(x)}. \tag{3.4}$$

Clearly ψ is the restriction to $\mathcal{D}_f$ of a rational function having no poles in $\mathcal{D}_f$. Thus $\psi : \mathcal{D}_f \to K$ is certainly continuous.

LEMMA 3.2. *Let f be a polynomial in $O_K[x]$ with positive degree such that the set $\mathcal{D}_f$ defined by* (3.3) *is not empty. Let ψ be the rational function defined by* (3.4). *Then the image $\psi(\mathcal{D}_f)$ is contained in $\mathcal{D}_f$. Moreover, if β belongs to $\mathcal{D}_f$ then*

$$\big|f\big(\psi(\beta)\big)\big| \leq \Big|\frac{f(\beta)}{f'(\beta)}\Big|^2 < |f(\beta)|, \tag{3.5}$$

and

$$\big|f'\big(\psi(\beta)\big)\big| = |f'(\beta)|. \tag{3.6}$$

Proof. Write

$$f(x) = f_0(x) = \sum_{n=0}^{N} a_n x^n, \quad f'(x) = f_1(x) = \sum_{n=1}^{N} a_n \binom{n}{1} x^{n-1},$$

and

$$f_m(x) = \sum_{n=m}^{N} a_N \binom{n}{m} x^{n-m} \quad \text{for} \quad m = 2, 3, \ldots, N.$$

Because f is in $O_K[x]$ and $|\ |$ is non-archimedean, each of the polynomials f_m belongs to $O_K[x]$ and therefore

$$\sup\{|f_m(x)| : x \in O_K\} \le 1. \tag{3.7}$$

Let x and y be independent indeterminants. Using the binomial expansion we find that

$$\begin{aligned} f(x) &= \sum_{n=0}^{N} a_n \big(y + (x-y)\big)^n \\ &= \sum_{m=0}^{N} \Big\{ \sum_{n=m}^{N} a_n \binom{n}{m} y^{n-m} \Big\} (x-y)^m \\ &= f(y) + f'(y)(x-y) + \sum_{m=2}^{N} f_m(y)(x-y)^m. \end{aligned} \tag{3.8}$$

Let β be a point in $\mathcal{D}_f$. We apply (3.8) with $x = \psi(\beta)$ and $y = \beta$. Using (3.4) we obtain the identity

$$\begin{aligned} f\big(\psi(\beta)\big) &= f(\beta) + f'(\beta)\big(\psi(\beta) - \beta\big) + \sum_{m=2}^{N} f_m(\beta)\big(\psi(\beta) - \beta\big)^m \\ &= \sum_{m=2}^{N} f_m(\beta)\big(\psi(\beta) - \beta\big)^m. \end{aligned}$$

Then using the strong triangle inequality we find that

$$\begin{aligned} \big|f\big(\psi(\beta)\big)\big| &\le \max\big\{\big|f_m(\beta)\big(\psi(\beta) - \beta\big)^m\big| : 2 \le m \le N\big\} \\ &\le \max\Big\{\Big|\frac{f(\beta)}{f'(\beta)}\Big|^m : 2 \le m \le N\Big\} \\ &= \Big|\frac{f(\beta)}{f'(\beta)}\Big|^2 \\ &< |f(\beta)|, \end{aligned}$$

and this establishes (3.5).

Now let $g(x) = f'(x)$, so that g is a polynomial in $O_K[x]$ and write

$$g(x) = g_0(y) + \sum_{m=1}^{N-1} g_m(y)(x-y)^m. \tag{3.9}$$

Again we find that each polynomial g_m belongs to $O_k[x]$ and therefore

$$\sup\{|g_m(x)| : x \in O_K\} \le 1.$$

Let β be a point in $\mathcal{D}_f$. We apply (3.9) with $x = \psi(\beta)$ and $y = \beta$ and find that

$$\begin{aligned}
\big|f'\big(\psi(\beta)\big) - f'(\beta)\big| &= \big|g\big(\psi(\beta)\big) - g(\beta)\big| \\
&= \Big|\sum_{m=1}^{N-1} g_m(\beta)\big(\psi(\beta)-\beta\big)^m\Big| \\
&\le \max\big\{|\psi(\beta)-\beta|^m : 1 \le m \le N-1\big\} \\
&= \Big|\frac{f(\beta)}{f'(\beta)}\Big| \\
&< |f'(\beta)|.
\end{aligned}$$

By the case of equality in the strong triangle inequality we have

$$\big|f'\big(\psi(\beta)\big)\big| = |f'(\beta)|$$

and this verifies (3.6). Combining (3.5) and (3.6) leads to the inequality

$$\big|f\big(\psi(\beta)\big)\big| < |f(\beta)| < |f'(\beta)|^2 = \big|f'\big(\psi(\beta)\big)\big|^2,$$

and this shows that $\psi : \mathcal{D}_f \to \mathcal{D}_f$.

Proof of Theorem 3.1. By hypothesis the set $\mathcal{D}_f$ contains the point ξ_1. We define a sequence of points $\xi_1, \xi_2, \xi_3, \dots$ by iterating the map ψ defined in (3.4). That is, for $n = 1, 2, 3, \dots$ we set

$$\xi_{n+1} = \psi(\xi_n).$$

By Lemma 3.2 each point in the sequence $\xi_1, \xi_2, \xi_3 \dots$ belongs to $\mathcal{D}_f$. Using (3.5) we have

$$|f(\xi_1)| > |f(\xi_2)| > |f(\xi_3)| > \cdots. \tag{3.10}$$

From (3.6) we conclude that

$$\big|f'(\xi_1)\big| = \big|f'(\xi_2)\big| = \big|f'(\xi_3)\big| = \cdots . \tag{3.11}$$

We will also show that

$$|f(\xi_n)| \le |f'(\xi_1)|^2 \left\{ \frac{|f(\xi_1)|}{|f'(\xi_1)|^2} \right\}^{2^{n-1}} \tag{3.12}$$

for each integer $n = 1, 2, \ldots$. If $n = 1$ then (3.12) is trivial. Assume that (3.12) holds for some positive integer n. Using (3.5) and the inductive hypothesis (3.12) we get

$$\begin{aligned} |f(\xi_{n+1})| &\le \Big| \frac{f(\xi_n)}{f'(\xi_n)} \Big|^2 \\ &\le |f'(\xi_1)|^{-2} \left(|f'(\xi_1)|^2 \left\{ \frac{|f(\xi_1)|}{|f'(\xi_1)|^2} \right\}^{2^{n-1}} \right)^2 \\ &= |f'(\xi_1)|^2 \left\{ \frac{|f(\xi_1)|}{|f'(\xi_1)|^2} \right\}^{2^n}, \end{aligned}$$

as required. It follows now from the hypothesis (3.1) and (3.12) that

$$\lim_{n\to\infty} |f(\xi_n)| = 0. \tag{3.13}$$

From (3.11) we obtain the identity

$$|\xi_{n+1} - \xi_n| = \Big| \frac{f(\xi_n)}{f'(\xi_n)} \Big| = \frac{|f(\xi_n)|}{|f'(\xi_1)|}, \tag{3.14}$$

and therefore

$$\lim_{n\to\infty} |\xi_{n+1} - \xi_n| = 0. \tag{3.15}$$

If follows from (3.15) and the strong triangle inequality that $\{\xi_n\}_{n=1}^{\infty}$ is a Cauchy sequence in the closed set O_K. Hence there exists a point α in O_K such that

$$\lim_{n\to\infty} \xi_n = \alpha. \tag{3.16}$$

As the polynomial map $f : O_K \to O_K$ is continuous, (3.13) and (3.16) imply that

$$f(\alpha) = 0.$$

Of course the derivative of f is also continuous and so (3.11) and (3.16) imply that

$$|f'(\xi_1)| = |f'(\alpha)| > 0. \tag{3.17}$$

This shows that α is a simple zero of f.

Let the integer m be so large that

$$|\alpha - \xi_m| < \frac{|f(\xi_1)|}{|f'(\xi_1)|}.$$

Then using (3.10) and (3.14) we get

$$\begin{aligned} |\alpha - \xi_1| &= |\alpha - \xi_m + \xi_m - \xi_{m-1} + \xi_{m-1} - \xi_{m-2} + \cdots + \xi_2 - \xi_1| \\ &\le \max\big\{|\alpha - \xi_m|, \max\{|\xi_{l+1} - \xi_l| : 1 \le l \le m-1\}\big\} \\ &\le \max\Big\{|\alpha - \xi_m|, \max\big\{\frac{|f(\xi_l)|}{|f'(\xi_1)|} : 1 \le l \le m-1\big\}\Big\} \\ &\le \frac{|f(\xi_1)|}{|f'(\xi_1)|}. \end{aligned} \tag{3.18}$$

Now suppose that γ is a point in O_K such that

$$\gamma \neq \alpha, \quad |\gamma - \xi_1| \le \frac{|f(\xi_1)|}{|f'(\xi_1)|} \quad \text{and} \quad f(\gamma) = 0.$$

From the identity (3.8) we have

$$0 = f(\gamma) - f(\alpha) = \sum_{m=1}^{N} f_m(\alpha)(\gamma - \alpha)^m. \tag{3.19}$$

But for $2 \le m \le N$ we get

$$\begin{aligned} \big|f_m(\alpha)(\gamma - \alpha)^m\big| &\le |\gamma - \alpha|^2 \\ &\le \max\{|\gamma - \xi_1|, |\xi_1 - \alpha|\}|\gamma - \alpha| \\ &\le \frac{|f(\xi_1)|}{|f'(\xi_1)|}|\gamma - \alpha| \\ &< |f'(\xi_1)||\gamma - \alpha| \\ &= |f_1(\alpha)(\gamma - \alpha)|, \end{aligned} \tag{3.20}$$

where we have used (3.17) at the last step. By the case of equality in the strong triangle inequality, the identity (3.19) and the strict inequality (3.20) are impossible. We have

shown that α is the unique zero of f in the closed ball $B(f, \xi_1)$ defined by (3.2). This completes the proof of Hensel's lemma.

In Chapter 3, section 3, we will state and prove a more algebraic form of Hensel's lemma.

Exercises

3.1 Assume that K is a field with a nontrivial, non-archimedean absolute value $|\ |$, and assume that $(K, |\ |)$ is complete. Let

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

be a polynomial in $O_K[x]$ of positive degree. Assume that there exists a point α in O_K such that

$$|f(\alpha)| < |\operatorname{Disc}(f)|^2,$$

where $\operatorname{Disc}(f)$ is the discriminant of f. Prove that f has a root in O_K.

4. Local Fields

Let K be a field with an absolute value $|\ |$. If $|\ |$ is the trivial absolute value then it induces the discrete topology in K, and so K is locally compact. For the remainder of this section we assume that $|\ |$ is nontrivial, and so the metric topology induced in K is not discrete. We say that K is a *local field* if the metric topology induced by $|\ |$ in K is locally compact and not discrete. Clearly a local field is also complete because a locally compact metric space is complete. As $\mathbb{R}$ and $\mathbb{C}$ are both locally compact, it follows from Theorem 2.2 that every archimedean local field is isometrically isomorphic to either $(\mathbb{R}, |\ |_\infty^\theta)$ or $(\mathbb{C}, |\ |_\infty^\theta)$ for some θ, $0 < \theta \leq 1$. As the archimedean local fields are determined (and familiar), our objective in this section is to characterize the non-archimedean local fields.

THEOREM 4.1. *Let K be a field and $|\ |$ a nontrivial, non-archimedean absolute value on K. Then the following conditions are equivalent:*

(1) *K is complete, $|\ |$ is discrete, and the residue class field O_K/M_K is finite,*
(2) *O_K is compact,*
(3) *K is locally compact.*

PROOF. Assume that (1) holds and let $\{\alpha_l\}_{l=1}^\infty$ be a sequence in O_K. As in the statement of Corollary 2.7, let R_K be a complete set of distinct coset representatives for the finite residue class field O_K/M_K and let π in M_K be a prime element. Then each point α_l has a unique expansion

$$\alpha_l = \sum_{n=0}^{\infty} a(l,n)\pi^n, \quad \text{with } a(l,n) \in R_K.$$

We now define a nested sequence of infinite subsets

$$\{1, 2, 3, \dots\} \supseteq S_0 \supseteq S_1 \supseteq S_2 \supseteq \dots$$

as follows. Because R_K is finite there exists $b(0)$ in R_K such that $a(l, 0) = b(0)$ for all integers l in an infinite subset $S_0 \subseteq \{1, 2, 3, \dots\}$. Then the finiteness of R_K implies that there exists $b(1)$ in R_K such that $a(l, 1) = b(1)$ for all integers l in an infinite subset $S_1 \subseteq S_0$. Again the finiteness of R_K implies that there exists $b(2)$ in R_K such that $a(l, 2) = b(2)$ for all integers l in an infinite subset $S_2 \subseteq S_1$. Continuing in this manner we determine a sequence of points $\{b(n)\}_{n=0}^{\infty}$ in R_K such that for every nonnegative integer N we have

$$a(l, n) = b(n) \quad \text{for } n = 0, 1, 2, \dots, N, \quad \text{and } l \in S_N.$$

As K is complete the point

$$\beta = \sum_{n=0}^{\infty} b(n)\pi^n$$

belongs to O_K. Let $L_0 < L_1 < L_2 < \dots$ be an increasing sequence of positive integers such that L_N is in S_N for each nonnegative integer N. Then we have

$$\sum_{n=0}^{N} a(L_N, n)\pi^n = \sum_{n=0}^{N} b(n)\pi^n$$

for each nonnegative integer N. It follows that

$$\begin{aligned} |\alpha_{L_N} - \beta| &= |\sum_{n=0}^{\infty} a(L_N, n)\pi^n - \sum_{n=0}^{\infty} b(n)\pi^n| \\ &= |\sum_{n=N+1}^{\infty} \{a(L_N, n) - b(n)\}\pi^n| \\ &\leq \max\{|\pi|^n : N + 1 \leq n\} \\ &= |\pi|^{N+1}. \end{aligned}$$

This shows that an arbitrary sequence in O_K has a convergent subsequence. Hence O_K is compact.

Assume that (2) holds. Every closed ball in K with positive radius has the form

$$B_K(\beta, \gamma) = \{\alpha \in K : |\alpha - \beta| \leq |\gamma|\}$$

for some β in K and γ in $K^\times$. The map $x \to \gamma x + \beta$ is obviously continuous and maps O_K onto $B_K(\beta, \gamma)$. Thus $B_K(\beta, \gamma)$ is compact. As every closed ball of positive radius in K is compact, it follows that K is locally compact.

Assume that (3) holds. Then K is complete and every closed ball of positive radius is compact. In particular the set O_K is compact. Now suppose that

$$\sup\{|\alpha| : \alpha \in M_K\} = 1. \tag{4.1}$$

Let $\{\alpha_n\}_{n=1}^\infty$ be a sequence of points in M_K such that

$$0 < |\alpha_1| < |\alpha_2| < |\alpha_3| < \dots, \quad \text{and} \quad \lim_{n\to\infty} |\alpha_n| = 1.$$

By the compactness of O_K the sequence $\{\alpha_n\}_{n=1}^\infty$ must have a convergent subsequence. By the case of equality in the strong triangle inequality we have

$$|\alpha_m - \alpha_n| = \max\{|\alpha_m|, |\alpha_n|\} \geq |\alpha_1| > 0$$

whenever $m \neq n$. This shows that $\{\alpha_n\}_{n=1}^\infty$ has no Cauchy subsequence and therefore no convergent subsequence. Hence the assumption (4.1) is false and so $|\ |$ is a discrete absolute value. Finally, we suppose that R_K is a complete set of distinct coset representatives for the residue class field O_K/M_K. If R_K is infinite then by the compactness of O_K it must have a limit point in O_K. But if a and b are distinct elements of R_K then $|a - b| = 1$. The contradiction shows that R_K is finite and therefore O_K/M_K is a finite field.

If $(K, |\ |)$ is a non-archimedean local field then the residue class field O_K/M_K is a finite field and so $|O_K/M_K|$, the number of elements in O_K/M_K, is a prime power, say, $q = p^m$ where p is a prime number and m is a positive integer. Also, M_K is a principal, maximal ideal in the ring O_K generated by a prime element π, $|\pi| < 1$, and the multiplicative value group of $(K, |\ |)$ is the subset

$$\{|\pi|^n : n \in \mathbb{Z}\}.$$

Of course $|\ |^\theta$ is an equivalent absolute value for every positive real θ. Therefore we can always select an equivalent absolute value $|\ |^\theta$ in such a way that $|\pi|^\theta = q^{-1}$. We say that the resulting choice of an absolute value is *normalized*. Later we will see other convenient ways to select a normalized absolute value on a local field.

5. Absolute Values on $\mathbb{Q}$

We will describe all the nontrivial absolute values on the field $\mathbb{Q}$ of rational numbers. First of all there is the usual archimedean absolute value on $\mathbb{Q}$. In situations such as this, where we need to refer to several different absolute values on $\mathbb{Q}$, we will write $|\ |_\infty$

for the usual archimedean absolute value. It is trivial that $\Phi(|\ |_\infty) = 2$, and therefore $\Theta(|\ |_\infty) = (0, 1]$. Thus the usual absolute value $|\ |_\infty$ is the unique absolute value in its place that satisfies $|2|_\infty = 2$.

Next, for each prime number p there is the usual p-adic absolute value $|\ |_p$. This is defined on $\mathbb{Q}$ as follows. If β is a nonzero rational number then by the fundamental theorem of arithmetic we can write

$$\beta = \pm 2^{w_2(\beta)} 3^{w_3(\beta)} 5^{w_5(\beta)} 7^{w_7(\beta)} \dots, \tag{5.1}$$

where $\{w_q(\beta)\}$ is a sequence of integers indexed by the set of prime numbers q and $w_q(\beta) = 0$ for all but finitely many q. In particular there is no question of convergence with respect to this product because all but finitely many terms are equal to 1. Then the usual p-adic absolute value of β is defined by

$$|\beta|_p = p^{-w_p(\beta)}. \tag{5.2}$$

Of course we also have $|0|_p = 0$. In this case we find that $\Phi(|\ |_p) = 1$, $\Theta(|\ |_p) = (0, \infty)$, and therefore $|\ |_p$ is a non-archimedean absolute value on $\mathbb{Q}$. The usual p-adic absolute value $|\ |_p$ is the unique absolute value in its place that satisfies $|p|_p = p^{-1}$.

Clearly the multiplicative value group associated to $|\ |_p$ is

$$\{p^{-m} : m \in \mathbb{Z}\},$$

and $|\ |_p$ is a discrete absolute value on $\mathbb{Q}$. Then

$$\{\beta \in \mathbb{Q} : |\beta|_p \le 1\} = \{a/b \in \mathbb{Q} : p \nmid b\}$$

is an integral domain, and

$$\{\beta \in \mathbb{Q} : |\beta|_p < 1\} = \{a/b \in \mathbb{Q} : p|a, \text{ and } p \nmid b\} \tag{5.3}$$

is its unique maximal ideal. If a/b is in $\mathbb{Q}$ and $p \nmid b$ then $a\bar{b}$ is a well defined element of $\mathbb{Z}/p\mathbb{Z}$, where $\bar{b}$ denotes the inverse of b in $\mathbb{Z}/p\mathbb{Z}$. Moreover, it is easy to check that the map $a/b \to a\bar{b}$ is a surjective homomorphism. As the kernel of this homomorphism is clearly the maximal ideal (5.3), it follows that the residue class field is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and $\{0, 1, 2, \dots, p-1\}$ is a complete set of distinct coset representatives.

Using Theorem 1.2 we find that any two distinct absolute values in the set

$$\{|\ |_\infty,\ |\ |_2,\ |\ |_3,\ |\ |_5,\ |\ |_7,\ \dots\} \tag{5.4}$$

are not equivalent, and so the places they determine are distinct. It is a basic result of Ostrowski [7] that this accounts for all the nontrivial absolute values on $\mathbb{Q}$.

THEOREM 5.1. *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to exactly one of the absolute values in the set* (5.4).

PROOF. Suppose that $|\ |:\mathbb{Q}\to[0,\infty)$ is a nontrivial absolute valued on $\mathbb{Q}$. Let $a>1$ and $b>1$ be integers. Write a in the base b, so that

$$a=d_0+d_1b+d_2b^2+\cdots+d_Mb^M,$$

where

$$M=\left[\frac{\log a}{\log b}\right]$$

is a nonnegative integer, and

$$d_m\in\{0,1,2,\dots,b-1\}\quad\text{for}\quad m=0,1,2,\dots,M.$$

Then we have

$$\begin{aligned}|a|&\le|d_0|+|d_1||b|+|d_2||b|^2+\cdots+|d_M||b|^M\\&\le(M+1)\max\{|1|,|2|,\dots,|b-1|\}\max\{1,|b|\}^M.\end{aligned}\tag{5.5}$$

Next we apply (5.5) with a replaced by a^N, we take Nth roots of both sides of (5.5) and then let $N\to\infty$. In this way we establish the inequality

$$|a|^{\log b}\le\max\{1,|b|\}^{\log a}.\tag{5.6}$$

We now consider two cases. First assume that a can be selected so that $1<|a|$. Then (5.6) implies that $1<|b|$ for all integers $b>1$. By interchanging a and b in (5.6) we find that

$$|a|^{\log b}\le\max\{1,|b|\}^{\log a}=|b|^{\log a}\le\max\{1,|a|\}^{\log b}=|a|^{\log b}.$$

That is, $(\log b)\log|a|=(\log a)\log|b|$, or

$$\det\begin{pmatrix}\log|a| & \log a\\ \log|b| & \log b\end{pmatrix}=0.$$

Thus there exists a constant $\theta\neq0$ such that

$$\theta\log|a|=\log a\quad\text{and}\quad\theta\log|b|=\log b.$$

Obviously θ is positive and it follows that $|\ |^\theta$ is the usual absolute value on $\mathbb{Z}$. From Lemma 1.5 we conclude that $|\ |^\theta$ is the usual absolute value on $\mathbb{Q}$.

Finally, we assume that $|a| \leq 1$ for all integers $a > 1$. If $|a| = 1$ for all integers $a > 1$ then it is clear that $|\ |$ is trivial. Thus there exists a smallest positive integer p such that $|p| < 1$. If $p = ab$ with $a > 1$ and $b > 1$ then $|p| = |a||b| < 1$, which is impossible. This shows that p is a prime number. Now let q be an integer such that $p \nmid q$. Then there exist integers r and s such that $1 = pr + qs$. It follows that

$$1 = |pr + qs| \leq |p| + |q|.$$

Replacing q with q^N we get

$$1 - |p| \leq |q|^N. \tag{5.7}$$

Letting $N \to \infty$ in (5.7) shows that $|q| = 1$. If $a > 1$ is an integer then we can write $a = p^m q$ where $m \geq 0$ is an integer and q is an integer such that $p \nmid q$. Then the value of $|a|$ is given by

$$|a| = |p|^m |q| = |p|^m. \tag{5.8}$$

Finally, we select a positive constant θ so that $|p|^\theta = p^{-1}$. From (5.8) we conclude that $|\ |^\theta$ is equal to the p-adic absolute value on $\mathbb{Z}$. And Lemma 6.1 implies that $|\ |^\theta$ is the p-adic absolute value on $\mathbb{Q}$.

In sympathy with the notation used to denote the nontrivial absolute values on $\mathbb{Q}$, we write $\mathbb{Q}_\infty$ for the completion of $(\mathbb{Q}, |\ |_\infty)$, and at each prime number p we write $\mathbb{Q}_p$ for the completion of $(\mathbb{Q}, |\ |_p)$. We often speak of $\mathbb{Q}_\infty$ as the completion of $\mathbb{Q}$ at the place ∞, or at the *infinite place*, and speak of $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ at the place p, or at a *finite place*. In these cases we continue to write $|\ |_\infty$ or $|\ |_p$ for the absolute value extended to the completion, and we identify $\mathbb{Q}$ with its image in each completion. Of course $(\mathbb{Q}_\infty, |\ |_\infty)$ is isometrically isomorphic to $(\mathbb{R}, |\ |_\infty)$, and we use $\mathbb{Q}_\infty$ as a convenient, alternative notation for $\mathbb{R}$.

For each prime number p the field $\mathbb{Q}_p$ is the field of *p-adic numbers*. The multiplicative value group is clearly

$$\{p^{-m} : m \in \mathbb{Z}\},$$

and therefore $|\ |_p$ is a discrete absolute value on $\mathbb{Q}_p$. We will also use the standard notation

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\}$$

for the ring of *p-adic integers*. The ring $\mathbb{Z}_p$ is an integral domain, $\mathbb{Q}_p$ is its field of fractions, and

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

is the unique maximal ideal in $\mathbb{Z}_p$. We note that M_p is the principal ideal $M_p = p\mathbb{Z}_p$. It follows from Lemma 2.3 that $\mathbb{Z}_p/M_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and $\{0, 1, 2, \ldots, p-1\}$

is a complete set of distinct coset representatives for $\mathbb{Z}_p/M_p$. If $\alpha \neq 0$ is a point in $\mathbb{Q}_p$, if $|\alpha|_p = |p|_p^L = p^{-L}$, then by Corollary 2.7 there exists a unique sequence $\{a(n)\}_{n=L}^{\infty}$ of points in $\{0, 1, 2, \ldots, p-1\}$ such that

$$\alpha = \sum_{n=L}^{\infty} a(n)p^n \quad \text{and} \quad a(L) \neq 0. \tag{5.9}$$

Thus the points of $\mathbb{Q}_p^{\times}$ are in bijective correspondence with expansions of the form (5.9).

As an illustration of the use of Hensel's lemma, we consider the problem of determining a root in $\mathbb{Q}_7$ of the polynomial $f(x) = x^3 - x + 1$. Clearly this polynomial has no roots in $\mathbb{Q}$ and, by the case of equality in the strong triangle inequality, a root in $\mathbb{Q}_7$ must occur in $\mathbb{Z}_7$. If α in $\mathbb{Z}_7$ is a root of f then the image of α in the residue class field $\mathbb{Z}/7\mathbb{Z}$ is a root of the congruence $x^3 - x + 1 \equiv 0 \bmod 7$. It is easy to check that the only root of this congruence is $x \equiv 2 \bmod 7$. Therefore a root α in $\mathbb{Z}_7$ of the polynomial $f(x) = x^3 - x + 1$ must satisfy

$$|\alpha - 2|_7 \leq 7^{-1}. \tag{5.10}$$

Of course this does not yet establish that such a root exists. However, we have $|f'(2)|_7 = 1$, and therefore the inequality (3.1) in the statement of Hensel's lemma is satisfied with $\xi_1 = 2$. It follows that $f(x) = x^3 - x + 1$ does have a unique root α in the closed ball (5.10). Moreover, the proof of Hensel's lemma provides a sequence of rational numbers that converge rapidly to α. Let $\varphi(x)$ be the rational function

$$\varphi(x) = x - \frac{f(x)}{f'(x)} = \frac{2x^3 - 1}{3x^2 - 1}.$$

Then define a sequence of rational numbers $\xi_1 = 2, \xi_2, \xi_3, \ldots$ by setting

$$\xi_{n+1} = \varphi(\xi_n) \quad \text{for} \quad n = 1, 2, 3, \ldots.$$

We find that

$$\xi_1 = 2, \quad \xi_2 = \frac{15}{11}, \quad \xi_3 = \frac{5419}{6094}, \quad \text{and} \quad \xi_4 = \frac{45976035767}{155274653809}.$$

Using the estimate given in (3.12) we get

$$|f(\xi_n)|_7 \leq 7^{-2^{n-1}},$$

and (3.14) implies that

$$|\xi_{n+1} - \xi_n|_7 \leq |f(\xi_n)|_7 \leq 7^{-2^{n-1}} \quad \text{for} \quad n = 1, 2, 3, \ldots. \tag{5.11}$$

It follows from (5.11) and the strong triangle inequality that

$$|\alpha - \xi_n|_7 \leq |f(\xi_n)|_7 \leq 7^{-2^{n-1}} \quad \text{for} \quad n = 1, 2, 3, \ldots.$$

This confirms our remark that the sequence of rational numbers $\{\xi_n\}_{n=1}^{\infty}$ converges rapidly to the root α in $\mathbb{Z}_7$.

The collection of absolute values in the set (5.4) satisfies the following basic identity.

THEOREM 5.2 (THE PRODUCT FORMULA). *If β is a nonzero rational number then*

$$|\beta|_\infty \prod_p |\beta|_p = 1, \tag{5.12}$$

where the product on the left of (5.12) *runs over all prime numbers p.*

PROOF. This is essentially trivial. For if β has the factorization (5.1) then

$$\prod_p |\beta|_p = \prod_p p^{-w_p(\beta)} = |\beta|_\infty^{-1}.$$

6. Valuations

Let k be a field. A *valuation* on k is a map $x \to v(x)$ from k into the set $\mathbb{R} \cup \{\infty\}$ that satisfies the following three conditions:

(i) $v(x) = \infty$ if and only if $x = 0$,

(ii) $v(xy) = v(x) + v(y)$ for all x and y in k,

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all x and y in k.

The concept of a valuation and that of a non-archimedean absolute value differ only in notation. Suppose that v is a valuation on k. Then for every positive real number θ the map $x \to \exp\{-\theta v(x)\}$ defines a non-archimedean absolute value on k. Suppose that $|\ |$ is a non-archimedean absolute value on k. Then for every positive real number θ the map $x \to -\theta \log |x|$ defines a valuation on k. We note, however, that there is no correspondence of this sort between archimedean absolute values and valuations. When working with fields that have archimedean places we will generally use absolute values. In the case of some function fields where we would use only non-archimedean absolute values, it may be more convenient to use valuations.

In view of these remarks all concepts that apply to non-archimedean absolute values can also be applied to valuations. For example, if v is a valuation on k then the map $(x, y) \to \exp\{\theta v(x-y)\}$ from $k \times k$ into $[0, \infty)$ is a metric and induces a metric topology in k. We say that two valuations v_1 and v_2 on k are equivalent if they induce the same metric topology. Then Theorem 1.2 shows that v_1 and v_2 are equivalent if and only if

$$\{x \in k : v_1(x) \geq 0\} = \{x \in k : v_2(x) \geq 0\}.$$

If v is a nontrivial valuation on k then $v : k^\times \to \mathbb{R}$ is a homomorphism from the multiplicative group $k^\times$ into the additive group of real numbers. Its image

$$v(k^\times) = \{v(\alpha) : \alpha \in k^\times\}$$

is a nontrivial subgroup. This subgroup is called the *additive value group* of (k, v). Then v is said to be a *discrete valuation* if its additive value group is a discrete subgroup. Obviously v is a discrete valuation if and only if there exists a positive constant θ such that the equivalent valuation $x \to \theta v(x)$ has additive value group equal to $\mathbb{Z}$.

As an example, suppose that β is a nonzero rational number given, as in (5.1), by

$$\beta = \pm 2^{w_2(\beta)} 3^{w_3(\beta)} 5^{w_5(\beta)} 7^{w_7(\beta)} \dots .$$

Then the usual p-adic absolute value of β is

$$|\beta|_p = p^{-w_p(\beta)}.$$

If we extend the map $w_p : \mathbb{Q}^\times \to \mathbb{Z}$ by setting $w_p(0) = \infty$, then $\beta \to w_p(\beta)$ is a valuation on $\mathbb{Q}$.

7. Valuations on $k(x)$

Let k be a field. In this section we will describe all the nontrivial valuations on the rational function field $k(x)$, that are trivial on the subfield k, and have $\mathbb{Z}$ as additive value group. That is, we will describe all the surjective maps

$$v : k(x) \to \mathbb{Z} \cup \{\infty\}$$

such that

(i) $v(F) = \infty$ if and only if $F = 0$ in $k(x)$,
(ii) $v(FG) = v(F) + v(G)$ for all F and G in $k(x)$,
(iii) $v(F + G) \geq \min\{v(F), v(G)\}$ for all F and G in $k(x)$,
(iv) $v(F) = 0$ whenever F is a nonzero constant in $k(x)$.

We note that such valuations are nontrivial because their additive value group is $\mathbb{Z}$.

Let $\mathcal{F}_k \subseteq k[x]$ be the subset of all monic, irreducible polynomials. It turns out that the collection of all surjective maps satisfying (i), (ii), (iii) and (iv), is conveniently indexed by the set $\mathcal{F}_k \cup \{\infty\}$. If $F \neq 0$ is in $k(x)$ then we have the factorization

$$F(x) = a \prod_{j=1}^{J} q_j(x)^{m_j}, \tag{7.1}$$

where a is a nonzero constant in k, $q_1, q_2, \dots, q_J$ are distinct, monic, irreducible polynomials in $k[x]$, and $m_1, m_2, \dots, m_J$ are nonzero integers. For each monic, irreducible polynomial $p(x)$ in $k[x]$ we define the map

$$\mathrm{ord}_{p(x)} : k[x] \to \mathbb{Z} \cup \{\infty\}$$

by

$$\mathrm{ord}_{p(x)}(F) = \begin{cases} m_j & \text{if } p(x) = q_j(x) \text{ for some integer } j, \\ 0 & \text{if } p(x) \neq q_j(x) \text{ for each integer } j. \end{cases}$$

Of course we set $\mathrm{ord}_{p(x)}(0) = \infty$. Then it is easy to check that $\mathrm{ord}_{p(x)}$ is surjective and satisfies the conditions (i), (ii), (iii) and (iv). Thus each map $\mathrm{ord}_{p(x)}$ is a valuation on $k(x)$ with additive value group $\mathbb{Z}$, and the restriction of this valuation to the subfield k is trivial. If p_1 and p_2 are distinct elements of $\mathcal{F}_k$ then the corresponding valuations satisfy

$$\mathrm{ord}_{p_1(x)}(p_1) = \mathrm{ord}_{p_2(x)}(p_2) = 1 \quad \text{and} \quad \mathrm{ord}_{p_1(x)}(p_2) = \mathrm{ord}_{p_2(x)}(p_1) = 0.$$

It follows using Theorem 1.2 that $\mathrm{ord}_{p_1(x)}$ and $\mathrm{ord}_{p_2(x)}$ are not equivalent.

There is one further valuation that we denote by

$$\mathrm{ord}_\infty : k[x] \to \mathbb{Z} \cup \{\infty\}.$$

If $F \neq 0$ is in $k(x)$, write $F(x) = f(x)/g(x)$, where $f(x)$ and $g(x) \neq 0$ are relatively prime polynomials in $k[x]$. Then we define

$$\mathrm{ord}_\infty(F) = \deg g - \deg f.$$

Again we find that ord_∞ is surjective and satisfies the conditions (i), (ii), (iii) and (iv). Clearly ord_∞ is not equivalent to any valuation $\mathrm{ord}_{p(x)}$ for $p(x)$ in $\mathcal{F}_k$.

The following result is an analogue of Theorem 5.1.

THEOREM 7.1. *Let $v : k(x) \to \mathbb{Z} \cup \{\infty\}$ be a valuation with additive value group $\mathbb{Z}$ and assume that the restriction of v to k is trivial. If v is nonnegative on the polynomial ring $k[x]$, then there exists a monic irreducible polynomial $p(x)$ in $k[x]$ such that v is $\mathrm{ord}_{p(x)}$. If v takes a negative value on $k[x]$, then v is ord_∞.*

PROOF. Assume that v is nonnegative on $k[x]$. If v is identically 0 on $k[x]$, then v is identically 0 on $k(x)$. In fact v is nontrivial and so there exists a polynomial $p(x)$ of minimal degree such that $v(p) > 0$. Because v is trivial on k we may assume that $p(x)$ is monic. If $p(x)$ factors in $k[x]$ as $p(x) = f(x)g(x)$, where f and g have positive degree, then $v(p) = v(f) + v(g) > 0$, which is impossible. Hence the monic polynomial $p(x)$ is irreducible. Now suppose that $q(x)$ is in $k[x]$ and is not divisible by $p(x)$. By the division algorithm there exist nonzero polynomials $r(x)$ and $s(x)$ in $k[x]$ such that

$$q(x) = p(x)r(x) + s(x) \quad \text{and} \quad 0 \leq \deg s < \deg p.$$

It follows that $v(s) = 0$, and therefore

$$0 = v(q - pr) \geq \min\{v(q), v(p) + v(r)\} \geq \min\{v(q), v(p)\} = v(q).$$

In particular we have $v(q) = 0$ whenever q is in $\mathcal{F}_k$ and $q \neq p$. If $F(x) \neq 0$ in $k(x)$ has the factorization (7.1), then we find that

$$v(F) = \begin{cases} m_j v(p) & \text{if } p(x) = q_j(x) \text{ for some integer } j, \\ 0 & \text{if } p(x) \neq q_j(x) \text{ for each integer } j. \end{cases}$$

As the additive value group is $\mathbb{Z}$ we must have $v(p) = 1$. We have shown that v is equal to $\operatorname{ord}_{p(x)}$.

Now assume that v takes some negative value on $k[x]$. As before, there exists a monic polynomial $p(x)$ of minimal degree such that $v(p) < 0$. Write

$$p(x) = x^M + c_1 x^{M-1} + c_2 x^{M-2} + \cdots + c_M = x^M + q(x),$$

where $1 \leq M$ and $v(q) = 0$. Then we have

$$0 > v(p) \geq \min\{v(x^M), v(q)\} = M v(x),$$

and therefore $0 > v(x)$. Suppose that $f(x) \neq 0$ is an arbitrarily polynomial in $k[x]$, $\deg f = N$, and

$$f(x) = d_0 x^N + d_1 x^{N-1} + d_2 x^{N-2} + \cdots + d_N \quad \text{where} \quad d_0 \neq 0.$$

Then we have

$$v(d_0 x^N) = N v(x), \quad \text{and} \quad v(d_n x^{N-n}) \geq (N-n) v(x) \quad \text{for} \quad n = 1, 2, \ldots, N.$$

From the case of equality in the strong triangle inequality we conclude that

$$v(f) = N v(x) = (\deg f) v(x). \tag{7.2}$$

More generally, if $f(x)$ and $g(x) \neq 0$ are relatively prime polynomials in $k[x]$ then (7.2) implies that

$$v(f/g) = (\deg f - \deg g) v(x).$$

Because the additive value group is $\mathbb{Z}$ we must have $v(x) = -1$. We have shown that v is equal to $\operatorname{ord}_\infty$.

If $F \neq 0$ is in $k(x)$ and has the factorization (7.1), then we have the identity

$$\operatorname{ord}_\infty(F) = -\sum_{j=1}^{J} m_j \deg q_j. \tag{7.3}$$

This is plainly an analogue of Theorem 5.2. It is usually reformulated as follows, with a sum over all the absolute values identified in Theorem 7.1.

THEOREM 7.2. *If F is a nonzero element of the field $k(x)$ then*

$$\operatorname{ord}_\infty(F) + \sum_{p(x)\in\mathcal{F}_k} \operatorname{ord}_{p(x)}(F)\deg p = 0, \tag{7.4}$$

where only finitely many terms in the sum are not equal to zero.

In this setting (7.4) is known as the *sum formula*.

If $k = \overline{k}$ is algebraically closed then

$$\mathcal{F}_k = \{(x-\alpha) : \alpha \in k\}.$$

Thus the valuations on $k(x)$ that are trivial on k and have $\mathbb{Z}$ as additive value group, are conveniently indexed by the elements of the set $k \cup \infty$. In this special case we will simplify our notation and write $\operatorname{ord}_\alpha(F)$ rather than $\operatorname{ord}_{(x-\alpha)}(F)$. If $F \neq 0$ is in $k(x)$ and $k = \overline{k}$ is algebraically closed, then the sum formula becomes

$$\operatorname{ord}_\infty(F) + \sum_{\alpha\in k} \operatorname{ord}_\alpha(F) = 0. \tag{7.5}$$

As an application of (7.5) we prove the *ABC*-inequality for polynomials. Assume that $k = \overline{k}$ is an algebraically closed field of characteristic zero. Then let

$$\varphi_0(x), \varphi_1(x), \ldots, \varphi_N(x)$$

be polynomials in $k[x]$ that have no common zero in k. We assume that $\varphi_0, \varphi_1, \ldots, \varphi_N$ span a vector space of dimension N over k, and satisfy the identity

$$\varphi_0(x) + \varphi_1(x) + \cdots + \varphi_N(x) = 0. \tag{7.6}$$

Then we define the set of common zeros

$$\mathcal{Z} = \{\alpha \in k : \prod_{n=0}^{N} \varphi_n(\alpha) = 0\}. \tag{7.7}$$

It is obvious that the cardinality of $\mathcal{Z}$ is bounded from above by

$$|\mathcal{Z}| \leq \sum_{n=0}^{N} \deg \varphi_n.$$

In this setting the *ABC*-inequality of Stothers [9] and Mason, (see [2], Lemma, p. 222, [3], Lemma 2, p. 14, or [4], Lemma, p. 152,) provides a nontrivial lower bound for $|\mathcal{Z}|$.

THEOREM 7.3. *Let $k = \overline{k}$ be an algebraically closed field of characteristic zero. Let $\varphi_0, \varphi_1, \dots, \varphi_N$ be polynomials in $k[x]$ that span a vector space of dimension N over k, and satisfy the linear equation* (7.6). *Assume that the polynomials have no common zero in k and let $\mathcal{Z}$ be defined by* (7.7). *Then we have*

$$\max\{\deg \varphi_n : 0 \le n \le N\} \le \binom{N}{2}\{|\mathcal{Z}| - 1\}. \tag{7.8}$$

PROOF. Among the polynomials $\varphi_0, \varphi_1, \dots, \varphi_N$, we may assume that φ_0 has the maximum degree. For each nonnegative integer l we define the differential operator

$$D^{(l)} = \frac{1}{l!}\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^l.$$

Using these operators we define the Wronskian

$$W_m(x) = \det\bigl(D^{(l-1)}\varphi_n(x)\bigr),$$

where $l = 1, 2, \dots, N$ indexes rows and $n = 0, 1, 2, \dots, m-1, m+1, \dots, N$ indexes columns. By hypothesis the polynomials $\varphi_0, \varphi_1, \dots, \varphi_{m-1}, \varphi_{m+1}, \dots, \varphi_N$ are K-linearly independent, and therefore the Wronskian $W_m(x)$ is not identically zero. Using (7.6) we find that

$$(-1)^m W_m(x) = (-1)^n W_n(x) \quad \text{for} \quad 0 \le m < n \le N. \tag{7.9}$$

From the sum formula (7.5) we have

$$\begin{aligned} 0 &= \operatorname{ord}_\infty\{W_0\} + \sum_{\alpha \in K} \operatorname{ord}_\alpha\{W_0\} \\ &\ge \operatorname{ord}_\infty\{W_0\} + \sum_{\alpha \in \mathcal{Z}} \operatorname{ord}_\alpha\{W_0\}. \end{aligned} \tag{7.10}$$

Next we use the two basic inequalities:

$$\operatorname{ord}_\infty\{W_0\} \ge \sum_{n=1}^{N} \operatorname{ord}_\infty\{\varphi_n\} + \binom{N}{2}, \tag{7.11}$$

and

$$\operatorname{ord}_\alpha\{W_0\} \ge \sum_{n=1}^{N} \operatorname{ord}_\alpha\{\varphi_n\} - \binom{N}{2}. \tag{7.12}$$

In fact the inequality (7.12) can be slightly improved. If α is in $\mathcal{Z}$ then there exists an integer $m = m(\alpha)$ such that $\operatorname{ord}_\alpha\{\varphi_m\} = 0$. In view of (7.9) we have

$$\begin{aligned} \operatorname{ord}_\alpha\{W_0\} &= \operatorname{ord}_\alpha\{W_m\} \\ &\geq \sum_{\substack{n=0 \\ n\neq m}}^{N} \operatorname{ord}_\alpha\{\varphi_n\} - \binom{N}{2} \\ &= \sum_{n=0}^{N} \operatorname{ord}_\alpha\{\varphi_n\} - \binom{N}{2}. \end{aligned} \tag{7.13}$$

It follows now using (7.10), (7.11) and (7.13) that

$$\begin{aligned} 0 &\geq \sum_{n=1}^{N} \operatorname{ord}_\infty\{\varphi_n\} + \binom{N}{2} + \sum_{\alpha\in\mathcal{Z}} \Big\{ \sum_{n=0}^{N} \operatorname{ord}_\alpha\{\varphi_n\} - \binom{N}{2} \Big\} \\ &= \sum_{n=1}^{N} \operatorname{ord}_\infty\{\varphi_n\} + \binom{N}{2} + \Big\{ \sum_{n=0}^{N} \sum_{\alpha\in\mathcal{Z}} \operatorname{ord}_\alpha\{\varphi_n\} \Big\} - \binom{N}{2}|\mathcal{Z}| \\ &= \sum_{n=1}^{N} \operatorname{ord}_\infty\{\varphi_n\} - \sum_{n=0}^{N} \operatorname{ord}_\infty\{\varphi_n\} - \binom{N}{2}\big\{|\mathcal{Z}| - 1\big\}, \end{aligned}$$

and therefore

$$0 \geq \deg\varphi_0 - \binom{N}{2}\big\{|\mathcal{Z}| - 1\big\}. \tag{7.14}$$

Exercises

7.1 Prove the inequalities (7.11) and (7.12) in the proof of Theorem 7.3.

7.2 Let $k = \overline{k}$ be an algebraically closed field of characteristic zero. Suppose that $A(x)$, $B(x)$, and $C(x)$ are polynomials in the ring $k[x]$ with no common zero, and positive degrees. Prove that these polynomials cannot satisfy the Fermat equation

$$A(x)^N + B(x)^N = C(x)^N, \quad \text{where} \quad 3 \leq N.$$

7.3 Let $k = \overline{k}$ be an algebraically closed field of characteristic zero. Suppose that $A(x)$, $B(x)$, and $C(x)$ are polynomials in the ring $k[x]$ with no common zero, and positive degrees. Prove that these polynomials cannot satisfy the generalized Fermat equation

$$A(x)^L + B(x)^M = C(x)^N, \quad \text{where} \quad L^{-1} + M^{-1} + N^{-1} \leq 1.$$

8. Invariant Measures

Let G be a locally compact abelian group, written additively. That is, G is an abelian group, G is a topological space, and the map from $G \times G$ to G given by $(x, y) \to x - y$ is continuous. We recall that the collection $\mathcal{B}_G$ of Borel sets in G is the σ-algebra generated by the open sets in G. If E is a Borel set in G then the translation

$$x + E = \{x + y : y \in E\}$$

is also a Borel set for each point x in G. Moreover, there exists a measure μ on the $\mathcal{B}_G$ such that

(i) $\mu(C) < \infty$ if $C \subseteq G$ is compact,

(ii) $0 < \mu(E)$ if $E \subseteq G$ is open and not empty,

(iii) $\mu(E) = \mu(x + E)$ for all Borel sets E and all points x in G.

Such a measure μ is called a *Haar measure*. Haar measure is unique up to a positive multiplicative constant. That is, if μ_1 and μ_2 are both Haar measures on the the σ-algebra of Borel subsets of G, then there exists a positive constant λ such that $\mu_1(E) = \lambda\mu_2(E)$ for all Borel sets E.

By an *automorphism* of G we understand a map $\eta : G \to G$ that is both a group isomorphism and a topological homeomorphism. It is clear that the collection of all automorphisms of G is a group with respect to composition of maps. If η is an automorphism, then it follows that the map

$$E \to \eta(E) = \{\eta(y) : y \in E\}$$

is a bijective map from $\mathcal{B}_G$ onto $\mathcal{B}_G$. If μ is a Haar measure on $\mathcal{B}_G$, then the composite map

$$E \to \mu\big(\eta(E)\big)$$

is also a Haar measure on $\mathcal{B}_G$. By our previous remarks, there exists a positive constant, which we denote by $\mathrm{mod}_G(\eta)$, such that

$$\mu\big(\eta(E)\big) = \mathrm{mod}_G(\eta)\mu(E) \quad \text{for all } E \text{ in } \mathcal{B}_G. \tag{8.1}$$

Alternatively, (8.1) can be written as

$$\int_G \chi_E\big(\eta^{-1}(x)\big)\, \mathrm{d}\mu(x) = \mathrm{mod}_G(\eta) \int_G \chi_E(x)\, \mathrm{d}\mu(x). \tag{8.2}$$

where χ_E denotes the characteristic function of the Borel set E. Now suppose that $f : G \to [0, \infty]$ is a Borel measurable function and η is an automorphism of G. By

approximating f from below by nonnegative simple functions, we find that (8.2) leads to the identity

$$\int_G f\big(\eta^{-1}(x)\big)\ \mathrm{d}\mu(x) = \mathrm{mod}_G(\eta) \int_G f(x)\ \mathrm{d}\mu(x). \tag{8.3}$$

Then it is obvious that (8.3) also holds for functions $f : G \to \mathbb{C}$ that are integrable with respect to the Haar measure μ. The positive number $\mathrm{mod}_G(\eta)$ is called the *modulus* of the automorphism η.

If η and θ are both automorphisms of the group G, then it follows from the definition of mod_G that

$$\mathrm{mod}_G(\eta\theta) = \mathrm{mod}_G(\eta)\,\mathrm{mod}_G(\theta).$$

Thus the map $\eta \to \mathrm{mod}_G(\eta)$ is a homomorphism from the group of all automorphisms of G into the multiplicative group of positive real numbers.

Now let K be a local field, either archimedean or non-archimedean. Then the additive group of K is a locally compact abelian group, and we may apply the previous discussion to K. We write $\mathcal{B}_K$ for the σ-algebra of Borel subsets of K, and we write μ for a Haar measure on $\mathcal{B}_K$. If α belongs to the multiplicative group $K^\times$, then the map $x \to \alpha x$ is plainly an automorphism of the additive group of K. Hence we define $\mathrm{mod}_K : K^\times \to (0, \infty)$ by

$$\mu(\alpha E) = \mathrm{mod}_K(\alpha)\mu(E) \quad \text{for all Borel sets } E \subseteq K. \tag{8.4}$$

Alternatively, (8.4) can be written as

$$\int_K f(\alpha^{-1}x)\ \mathrm{d}\mu(x) = \mathrm{mod}_K(\alpha) \int_K f(x)\ \mathrm{d}\mu(x), \tag{8.5}$$

where f is a nonnegative Borel measureable function on K, or f is a complex valued integrable function on K.

From our previous remarks it is clear that

$$\mathrm{mod}_K(\alpha\beta) = \mathrm{mod}_K(\alpha)\,\mathrm{mod}_K(\beta)$$

for all α and β in $K^\times$. Thus $\alpha \to \mathrm{mod}_K(\alpha)$ defines a homomorphism from $K^\times$ into the multiplicative group of positive real numbers. It will be convenient to set $\mathrm{mod}_K(0) = 0$. Again the function mod_K is called the *modulus* of K. We note that it does not depend on the initial choice of Haar measure μ, but is an intrinsic function defined on every local field. In particular, if $K = \mathbb{R}$ then $\mathrm{mod}_{\mathbb{R}}(\alpha) = |\alpha|_\infty$, where $|\ |_\infty$ is the usual absolute value on $\mathbb{R}$. If $K = \mathbb{C}$ then $\mathrm{mod}_{\mathbb{C}}(\alpha) = |\alpha|_\infty^2$, where $|\ |_\infty$ is the usual absolute value on $\mathbb{C}$. And if $K = \mathbb{Q}_p$ then $\mathrm{mod}_{\mathbb{Q}_p}(\alpha) = |\alpha|_p$, where $|\ |_p$ is the usual p-adic absolute value on $\mathbb{Q}_p$. Later we will determine mod_K for other local fields.

Exercises

8.1 Prove the identity $\mathrm{mod}_{\mathbb{Q}_p}(\alpha) = |\alpha|_p$ for each prime number p.

References for Chapter 2

1. J. W. S. Cassels, *Local Fields*, London Math. Soc. Student Texts 3, Cambridge University Press, 1986.
2. R. C. Mason, *The hyperelliptic equation over function fields,*, Math. Proc. Cambridge Philos. Soc. **93** (1983), 219–230.
3. R. C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge University Press, 1984.
4. R. C. Mason, *Equations over Function Fields,*, Lecture Notes in Mathematics, vol. 1068, Springer-Verlag, New York, 1984, pp. 149–157.
5. R. C. Mason, *Norm form equations, I*, J. Number Theory **22** (1986), 190–207.
6. A. M. Ostrowski, *Über einige Lösungen der Funktionalgleichung* $\phi(x)\phi(y) = \phi(xy)$, Acta Math. **41** (1918), 271–284.
7. A. M. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper*, Math. Zeit. **39** (1934), 269–404.
8. P. Ribenboim, *The Theory of Classical Valuations*, Springer-Verlag, New York, 1999.
9. W. W. Stothers,, *Polynomial identities and Hauptmoduln*, Quart. J. Math., Oxford Ser. (2) **32** (1981), 349–370.
5. A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1974.

1227, September 17, 2007