Fourier Analysis on Number Fields

March 19, 2004

Chapter 1

Locally Compact Topological Fields

1.1 Topological Fields

1.1.1 Definition. A field K is called a topological field, if K is provided with a Hausdorff topology such that $(K,+)$ and $(K^\times,\cdot)$ are both is topological groups and such that the multiplication is even continuous as a mapping from $K\times K\to K$. Hereby we have set $K^\times = K\setminus\{0\}$.

K is called a locally compact field, if it is a topological field whose topology is locally compact.

The most prominent examples for locally compact fields are $\mathbb{R}$ and $\mathbb{C}$.

Particularly interesting topological fields are those whose topology is induced by a metric similarly as it is done for $\mathbb{R}$ with the natural absolute value.

1.1.2 Definition. Let K be a field. An absolute value ν on K is a real-valued function $x\mapsto |x|_\nu$ on K satisfing the following three properties

AV1 $|x|_\nu \geq 0,\ \forall x\in K$ and $|x|_\nu = 0$ if and only if $x=0$.

AV2 $|xy|_\nu = |x|_\nu|y|_\nu,\ \forall x,y\in K$.

AV3 $|x+y|_\nu \leq |x|_\nu + |y|_\nu,\ \forall x,y\in K$.

If in addition the following stronger condition

AV4 $|x+y|_\nu \leq \max(|x|_\nu,|y|_\nu),\ \forall x,y\in K,$

is valid, then ν is called non-archimedean.

An absolute value is called discrete, if $|K^\times|$ is a discrete subgroup of $\mathbb{R}_+^\times$.

If we do not distinguish different absolute values, we will often write $|x|$ instead of $|x|_\nu$. If $|x| = 1, \forall x \in K^\times$, then $|.|$ is called trivial. Observe also that in any field K with absolute value $|.|$ we have $|1| = |1^2| = |(-1)^2| = |1|^2$, and therefore $|1| = |-1| = 1$. Also note that $|-x| = |-1||x| = |x|$ and that by AV2 $|x^{-1}| = |x|^{-1},\ x \neq 0$.

Every absolute value $|.|$ defines a metric $d(x, y) = |x - y|$ as one can easily verify. Moreover, the operations $+, -, \cdot, .^{-1}$ are continuous. This can be verified in the same manner as for $\mathbb{R}$ and the natural absolute value on $\mathbb{R}$. An absolute value $|.|$ is called complete, if (K, d) is a complete metric space. From general topology we know that any locally compact metric space is complete.

We mentioned above that $|.|$ defines a topology on K. It is remarkable that this topology determines the absolute value almost uniquely.

1.1.3 Proposition. *Let $|.|_1$ and $|.|_2$ be two non-trivial absolute values on K. They induce the same topology if and only if $|x|_1 < 1$ implies $|x|_2 < 1$. In this case there exists a number $c > 0$ such that $|.|_1 = |.|_2^c$.*

Proof. Note first that by AV2 $\{x \in K : |x|_j < 1\}$ is just the set of all $x \in K$ such that $x^n \to 0$ as $n \to \infty$ with respect to the topology induced by $|.|_j$, $j = 1, 2$.

Consequently, the fact that $|.|_1$ and $|.|_2$ induce the same topology, implies $\{x \in K : |x|_1 < 1\} = \{x \in K : |x|_2 < 1\}$ which clearly implies our condition.

Conversely, assume that our condition holds. Then $|x|_1 > 1$ implies $|x|_2 > 1$ because $|x^{-1}|_1 < 1$. Since $|.|_1$ is non-trivial, we can find an $x_0 \in K$ such that $|x_0|_1 > 1$. Let

$$c = \frac{\ln |x_0|_2}{\ln |x_0|_1}.$$

If $x \in K^\times$, then $|x|_1 = |x_0|_1^d$ for some $d > 0$. With $m, n \in \mathbb{N},\ n > 0$ such that $\frac{m}{n} > d$ we have

$$|x|_1 < |x_0|_1^{\frac{m}{n}},$$

and hence

$$\left|\frac{x^n}{x_0^m}\right|_1 < 1.$$

By assumption this yields

$$\left|\frac{x^n}{x_0^m}\right|_2 < 1,$$

and further $|x|_2 < |x_0|_2^{\frac{m}{n}}$. As there exists a sequence of rational numbers converging from above to d we obtain

$$|x|_2 \leq |x_0|_2^d.$$

In the same manner we show that $|x|_2 \geq |x_0|_2^d$, and consequently $|x|_2 = |x_0|_2^d$. Thus

$$|x|_2 = |x_0|_2^d = |x_0|_1^{cd} = |x|_1^c,$$

for all $x \in K$. It is now elementary to see that the respective metrices induce the same topology. □

Let us consider some examples of absolute values.

1. As already mentioned $\mathbb{R}$ provided with the classical absolute value satisfies the axioms AV1 - AV3 in Definition 1.1.2. The same ist true for $\mathbb{C}$ provided with $|z| = \sqrt{z\bar{z}}$. Let us mention that $\mathbb{R}$ and $\mathbb{C}$ are complete with respect to the metric induced by $|.|$. Moreover, $\mathbb{R}$ and $\mathbb{C}$ are locally compact if they are provided with the topology induced by $|.|$.

2. Denoting now by $|.|$ the classical absolute value on $\mathbb{Q}$ this function is also an absolute value in the above sense on $\mathbb{Q}$.

3. There are other absolute values on $\mathbb{Q}$. In fact, for every prime number p we define a function $|.|_p$ on $\mathbb{Q}$ as follows: Let $q \in \mathbb{Q}$ and write it in in the form
$$q = p^r \frac{m}{n},$$
where $r \in \mathbb{Z}$ and p is relatively prime to both numbers $m, n \in \mathbb{N}$. Now set
$$|q|_p = p^{-r}. \tag{1.1.1}$$
It is elementary to check the validity AV1 - AV2 and AV4. In contrast to the previous examples $|.|_p$ is a non-archimedean absolute value.

4. An example with a field of positive characteristic is $\mathbb{F}_q(T)$, the field of all rational functions with variable t and coefficients in the Galois Field $\mathbb{F}_q$, where $q = p^f$ for some prime number p and $f \in \mathbb{N}$. Now fix an irreducible polynomial $u(T)$ in the euclidean ring $\mathbb{F}_q[T]$. One obvious choice is $u(T) = T$. To define an absolute value on this field we write every $r(T) \in \mathbb{F}_q(T)$ in the form
$$r(T) = u(T)^r \frac{s(T)}{t(T)},$$
where $s(T)$ and $s(T)$ are polynomials having no common divisor. Note here that $\mathbb{F}_q(T)$ is the quotient field of $\mathbb{F}_q[T]$. Now set
$$|r(T)|_{u(T)} = q^{-r}. \tag{1.1.2}$$
Also in this example it is elementary to check, that $|.|_{u(T)}$ is an absolute value.

In a non-archimedean absolute value $|.|$ on a field K the subsets $R_K = R = \{x \in K : |x| \leq 1\}$ and $P = P_K = \{x \in K : |x| < 1\}$ are of particular interest. For the moment we mention that R is a ring and P is an ideal of R. This can be easily derived from AV1-AV2 and AV4. Moreover, P is the unique maximal ideal of R as we will see from

1.1.4 Lemma. *Let $|.|$ be a real valued functions on a ring A satisfying AV1, AV2 and AV4 with A instead of K. Moreover, assume that $|x| \leq 1$ for all $x \in A$, but $|.| \not\equiv 1$. Then $P = \{x \in A : |x| < 1\}$ is a prime ideal of A.*

If A is the ring R from above, then P is the unique maximal ideal of R.

Proof. By AV2 we have $|-x|^2 = |x|^2$ and hence $|x| = |-x|$. From AV4 we see that P is closed under addition. If $x \in A, y \in P$, then $|x| \leq 1,\ |y| < 1$ and therefore $|xy| = |x||y| < 1$ and P is an ideal.

If $x, y \in A$ and $xy \in P$, then $|x||y| = |xy| < 1$, and, hence, one of the factors $|x|$ and $|y|$ must be smaller than one. Thus $x \in P$ or $y \in P$, and P is proved to be a prime ideal.

If $A = R$, then P is just the set of all elements of R which are not invertible within R. With other words $R^\times = R \setminus P$. Since no proper ideal contains any invertible element, every proper ideal of R must be contained in P. □

Wether an absolute value is non-archimedean can be determined with the help of the following assertion.

1.1.5 Proposition. *$|.|$ is bounded on the prime ring of K ($= \mathbb{Z}$ if* char $K = 0$ *and $= \mathbb{Z}/p\mathbb{Z}$ if* char $K = p > 0$*). if and only if $|.|$ is non-archimedean.*

Proof. If $|.|$ is non-archimedean, then by AV4

$$|-n| = |n| = |1 + \cdots + 1| \leq |1|.$$

Conversely, if $|.|$ is bounded by C on the prime ring of K, then by AV3 we have for $x, y \in K$

$$|(x+y)^n| = |\sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}| \leq \sum_{j=0}^{n} C|x^j y^{n-j}| \leq Cn \max(|x|, |y|)^n.$$

Taking n-th roots an letting n tend to ∞ we see that AV4 holds. □

For a non-archimedean absolute value $|.|$ on a field K also the following easy but useful fact holds true.

1.1.6 Proposition. *If $x, y \in K$ such that $|y| < |x|$, then $|x + y| = |x|$.*

Proof. On the one hand side we have

$$|x + y| \leq \max(|x|, |y|) = |x|,$$

and, hence, by our assumption $\max(|x+y|, |y|) \leq |x|$ On the other hand side

$$|x| = |x + y - y| \leq \max(|x + y|, |y|).$$

Thus $|x| = \max(|x + y|, |y|)$. Again using the assumption we see $|x| = |x + y|$. □

1.2 Completions

Let K be a field provided with an absolute value $|.|$. As mentioned above $|.|$ induces a metric on K. It is well known that every metric space admits a completion. Thus there exists a metric space (K_ν, d_ν), which contains K densely such that $d_\nu(x, y) = |x-y|$ whenever $x, y \in K$. We set $|x|_\nu = d_\nu(x, 0)$ and see that this is a continuation of $|.|$ to K_ν. Moreover, $|.|_\nu$ satisfies AV1 and it is a continuous function on K_ν.

Now we can extend the operations $+$ to K_ν. In fact, if $x, y \in K_\nu$ and $(x_n), (y_n)$ are two sequences in K converging to x and y, respectively, then $x_n + y_n$ is a Cauchy sequence in K converging by the completeness of K_ν to some $z \in K_\nu$. We set $x + y = z$ and easily verify that z does not depend on the particularly chosen sequences (x_n) and (y_n). In the same way one defines $-x$ for $x \in K_\nu$, and it is also straight forward to show that K_ν becomes an additive topological group.

With these operation we have $|x - y|_\nu = d_\nu(x, y)$. In fact, take again sequences $(x_n), (y_n)$ as above. Then

$$d_\nu(x_n - y_n, 0) = |x_n - y_n| = d_\nu(x_n, y_n) \to d_\nu(x, y),\ x, y \in K_\nu.$$

On the other hand side we saw above that $x_n - y_n \to x - y$. An approximation argument shows that $|.|_\nu$ satisfies AV3 or even AV4 depending on what $|.|$ is satisfying.

Now we define a multiplication on K_ν: Let $x, y \in K_\nu$ and let $(x_n), (y_n)$ be two sequences in K converging to x and y, respectively. Since these sequences are Cauchy sequences within K, there exists an $C > 0$ such that $|x_n|, |y_n| < C$ for all $n \in \mathbb{N}$. Now we have

$$|x_n y_n - x_m y_m| \leq C|x_n - x_m| + C|y_n - y_m|,$$

and, therefore, $(x_n y_n)$ is a Cauchy sequence in K. We denote its limit by xy. It is again elementary to we see that xy does not depend on the chosen sequences. Moreover, again an approximation argument shows that $|.|_\nu$ satisfies AV2.

Finally, if $x \in K_\nu \setminus \{0\}$ and (x_n) converges to x from within K, then $|x_n| \to d_\nu(0, x)$, and we can therefore assume that $|x_n| > C$ for all $n \in \mathbb{N}$. Then

$$|x_n^{-1} - x_m^{-1}| = |x_m^{-1}(x_m - x_n)x_n^{-1}| \leq \frac{1}{C^2}|x_m - x_n|,$$

shows that x^{-1} can be defined with the already employed approximation procedure. Now we showed the following

1.2.1 Proposition. *Let K be a field and let $|.|$ be an absolute value on K. Then there exists a field extension K_ν of K and an absolute value $|.|_\nu$ on K_ν such that K is dense in K_ν and such that $|.|_\nu$ is an extension of $|.|$. This comlpetion is unique up to isomorphisms.*

Proof. We just have to deal with the uniqueness. So let K_μ and $|.|_\mu$ be another completion of K in the sense of the present proposition. By the well known fact, that the completion of a metric space is unique up to isomorphisms, there exists an isometric mapping ϕ from K_ν onto K_μ such that $\phi_K = \mathrm{id}_K$. By approximation arguments we can show that ϕ is, in fact, a field isomorphism. □

1. If $K = \mathbb{Q}$ and $|.|$ denotes the natural absolute value on $\mathbb{Q}$, then $\mathbb{R}$ provided with the natural absolute value is the completion of $\mathbb{Q}$ with respect to $|.|$.

2. If $K = \mathbb{Q}$ is provided with $|.|_p$, then its completion is the so-called field p-adic numbers $\mathbb{Q}_p$. This field can be realized explicitly as follows: Consider the set $\mathbb{Q}_p$ of all sequences

   $$(a_j)_{j=-\infty}^{\infty},$$

   where $a_j \in \{0, \ldots, p-1\}$ and $a_j = 0$ for all $j \leq n_0$ for some $n_0 \in \mathbb{Z}$. It is often convenient to write these sequences as formal sums

   $$\sum_{j=n_0}^{\infty} a_j p^j.$$

   On $\mathbb{Q}_p$ we define operations $+$ and $\cdot$:

   $$\sum_{j=n_0}^{\infty} a_j p^j + \sum_{j=m_0}^{\infty} b_j p^j = \sum_{j=\min(m_0,n_0)}^{\infty} c_j p^j,$$

where $c_j \equiv a_j + b_j + \epsilon_j \mathrm{mod} p,\ j \in \mathbb{Z}$ and (ϵ_j) is defined inductively as $\epsilon_j = 0,\ j \leq \min(m_0, n_0)$ and $\epsilon_{j+1} = 0$, if $c_j = a_j + b_j + \epsilon_j$ and $\epsilon_{j+1} = 1$, if $c_j = a_j + b_j + \epsilon_j + p$.

Every non-negative integer can uniquely be written as a sum of the form $\sum_{j=0}^{N} a_j p^j$ for some $N \in \mathbb{N}$ and every such sum gives a non-negative integer. We can identify $\mathbb{N} \cup \{0\}$ with a subset of $\mathbb{Q}_p$. Moreover, the natural addition on $\mathbb{N} \cup \{0\}$ corresponds just to the addition defined above.

The operation + is associative and commutative on $\mathbb{Q}_p$, and $(0)_{j=-\infty}^{\infty} =: 0$ is a the neutral element for +. It is straight forward to construct for any $\sum_{j=n_0}^{\infty} a_j p^j$ an element $\sum_{j=n_0}^{\infty} b_j p^j \in \mathbb{Q}_p$ step by step such that

$$\sum_{j=n_0}^{\infty} a_j p^j + \sum_{j=n_0}^{\infty} b_j p^j = 0.$$

Thus we can embed $(\mathbb{Z}, +)$ into $(\mathbb{Q}_p, +)$, more exactly into the subgroup $(\mathbb{Z}_p, +)$, where

$$\mathbb{Z}_p = \{\sum_{j=0}^{\infty} a_j p^j\},$$

the set of all p-adic integers.

The multiplication on $\mathbb{Q}_p$ is defined as follows:

$$(\sum_{j=n_0}^{\infty} a_j p^j) \cdot (\sum_{j=m_0}^{\infty} b_j p^j) = \sum_{j=m_0+n_0}^{\infty} c_j p^j,$$

with $c_j + \delta_{j+1} p = \sum_{k+l=j} a_k b_l + \delta_j$, where $\delta_j \in \mathbb{N} \cup \{0\},\ j \in \mathbb{Z}$ and $\delta_j = 0,\ j \leq m_0 + n_0$.

This operation is associative, commutative, and $1p^0 =: 1$ is a neutral element on $\mathbb{Q}_p^{\times} = \mathbb{Q}_p \setminus \{0\}$. Moreover, the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field yields shows, that for every $\sum_{j=n_0}^{\infty} a_j p^j \neq 0$ one can define inductively an element $\sum_{j=n_0}^{\infty} b_j p^j$ such that

$$(\sum_{j=n_0}^{\infty} a_j p^j)(\sum_{j=n_0}^{\infty} b_j p^j) = 1.$$

Finally, one checks that the distributive law holds on $\mathbb{Q}_p$. Thus we obtain a field containing an isomorphic copy of $\mathbb{Z}$ and therefore also of $\mathbb{Q}$.

Now define a function $|.|_p$ on $\mathbb{Q}_p$ as follows: For $(a_j)_{j=-\infty}^{\infty}$ let n_0 be the smallest integer n such that $a_n \neq 0$ and set $|(a_j)|_p = p^{-n_0}$. One easily checks that $|.|_p$ is an absolute value. For natural numbers this absolute value coincides with the absolute value defined for $\mathbb{Q}$ in (1.1.1). By the axioms of absolute values we obtain, that on all of $\mathbb{Q}$ $|.|_p$ is just the absolute value we dealt with in (1.1.1).

Moreover, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. In fact, if $\sum_{j=n_0}^{\infty} a_j p^j \in \mathbb{Q}_p$, then for all $k \in \mathbb{N},\ k > n_0$: $\sum_{j=n_0}^{k} a_j p^j \in \mathbb{Q}$ and

$$|\sum_{j=n_0}^{\infty} a_j p^j - \sum_{j=n_0}^{k} a_j p^j|_p = |\sum_{j=k+1}^{\infty} a_j p^j|_p \leq p^{-k-1} \to 0$$

as $k \to \infty$. Thus $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. The same kind of argument shows also that $\mathbb{N}$ and therefore also $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Moreover, as we are going to show, $\mathbb{Q}_p$ is a locally compact group (with respect to $+$) and, therefore, complete. Thus $(\mathbb{Q}_p, |.|_p)$ is the completion of $(\mathbb{Q}, |.|_p)$.

Finally it is worth to mention at this place some topological properties of $\mathbb{Q}_p$. First of all the ring $\mathbb{Z}_p$ coincides with $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ and, hence $\mathbb{Z}_p$ is closed in $\mathbb{Q}_p$. Moreover, it is open. In fact, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < p\}$. The most stricing property of $\mathbb{Z}_p$ is its compactness, which can be derived from the fact that $\mathbb{Z}_p$ is homoeomorphic to the compact space (Tychonoff)

$$\Pi_{j=0}^{\infty} \mathbb{Z}/p\mathbb{Z},$$

where each factor is equipped with the discrete topology. Thus $\mathbb{Q}_p$ is locally compact. Moreover, there is a neighbourhood bases of $0 \in \mathbb{Q}_p$ consisting of open and compact ideals, which are topological copies of $\mathbb{Z}_p$. Indeed for any $n \geq 0$ we have

$$p^n \mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq p^{-n}\},$$

and multiplication by p^n is an homoeomorphism on $\mathbb{Q}_p$. Note that $p^n\mathbb{Z}_p$ are ideals of $\mathbb{Z}_p$.

3. In the same manner we can find a realization of the completion of $\mathbb{F}_q(T)$ $(q = p^f)$ with respect to $|.|_{u(T)}$, when $u(T) = T$.

   Consider the set $\mathbb{F}_q((T))$ of all formal Laurent-series with coefficients in $\mathbb{F}_q$ such that the a_j are zero for sufficient small $j \in \mathbb{Z}$:

$$\sum_{j=n_0}^{\infty} a_j T^j.$$

Note that for $q = p$ if we identify $\mathbb{F}_p$ with $\{0, \ldots, p-1\}$, then $\mathbb{F}_q((T))$ and $\mathbb{Q}_p$ coincide as sets.

But in contrast to the p-adic numbers we define the operations $+, -$ and $\cdot, \cdot^{-1}$ just as for conventional Laurent-series. One immediatly checks that $\mathbb{F}_q((T))$ is a field of characteristic p.

To define an absolute value for $\sum_{j=n_0}^{\infty} a_j T^j$ let n_0 be minimal such that $a_{n_0} \neq 0$ and set

$$|\sum_{j=n_0}^{\infty} a_j T^j|_T = q^{-n_0}.$$

Clearly, for polynomials this absolute value coincides with the one defined in (1.1.2). Hence, the same is true for the quotient field $\mathbb{F}_q(T)$ of $\mathbb{F}_q[T]$. Moreover, similarly as in the p-adic case one shows also here that $\mathbb{F}_q(T)$ is densely contained in $\mathbb{F}_q((T))$ and $\mathbb{F}_q[T]$ is densely contained in $\mathbb{F}_q[[T]] = \{x \in \mathbb{F}_q((T)) : |x|_T \leq 1\}$. Thus $\mathbb{F}_q((T))$ is a completion of $\mathbb{F}_q(T)$ with respect to $|.|_T$. Finally, exactly as for the p-adic numbers one shows that $\mathbb{F}_q[[T]]$ is an open and compact subring of $\mathbb{F}_q((T))$, and for n running in $\mathbb{N}$

$$q^n \mathbb{F}_q[[T]] = \{x \in \mathbb{F}_q((T)) : |x|_T \leq q^{-n}\}$$

is a neighbourhood basis of 0, where each set $q^n \mathbb{F}_q[[T]]$ is an open and compact ideal of $\mathbb{F}_q[[T]]$.

For complete absolute values $|.|$ on K there is a unique topological structure on finite dimensional normed vector spaces over K.

1.2.2 Definition. Let V be a vector space over K, then $\|.\| : V \to \mathbb{R}$ is called a norm on V, if the following axioms are satisfied:

NO1 $\|x\| \geq 0,\ \forall x \in V$ and $\|x\| = 0$ if and only if $x = 0$.

NO2 $\|\xi x\| = |\xi| \|x\|,\ \forall x \in V,\ \xi \in K$.

NO3 $\|x + y\| \leq \|x\| + \|y\|,\ \forall x, y \in V$.

$(V, \|\|)$ is called normed space.

Two norms $\|.\|_1, \|, \|_2$ are called equivalent if there exist constants $C_1, C_2 > 0$, such that

$$C_1 \|x\|_1 \leq \|x\|_2 \leq C_2 \|x\|_1,$$

for all $x \in V$.

For a finite dimensional space $V = K^n$ we can for example define:

$$\|x\|_\infty = \sup_{i=1,\dots,n} |x_i|,$$

where x_i denotes the i-th component of x. Then $\|.\|_\infty$ is a norm on V.

Similarly to absolute values also a norm induces a metric on V such that the addition and the scalar multiplication are continuous operations. In particular, V then is a topological vector space over the topological field K. For sake of completeness we bring the exact definition of topological vector space.

1.2.3 Definition. Let K be a topological field and let V be a vector space over K. Then V is called a topological vector space over K, if it carries a topology such that $(V, +)$ is a topological group and such that the scalar multiplication is continuous as a mapping from $K \times V \to V$.

In the following we show that any finite dimensional topological vector space of dimension n over a field K with a complete absolute value is isomorphic (as a topological vector space) to K^n provided with topology induced by the norm $\|.\|_\infty$.

Hereby a commutative topological group G (written additively) is said to be complete if any Cauchy-Moore-Smith sequence $(x_i)_{i\in I}$ is convergent. The property to be a Cauchy-Moore-Smith sequence means that for any 0 neighbourhood U of G there exists an $i_0 \in I$ such that $x_i - x_j \in U$ for all $i, j \geq i_0$. Similar as for metric spaces it can be shown that if H is a complete subgroup of the topological group G, then H is closed in G. Moreover, if G is complete then G^n is complete. In particular, K^n is complete if K has this property.

1.2.4 Lemma. *Let V be a one-dimensional Hausdorff topological vector space over a field K provided with a non-trivial absolute value, and let $x_0 \in V \setminus \{0\}$. Then $\lambda \mapsto \lambda x_0$ is an isomorphism (algebraically and topologically) from K (as a topological vector space) onto V.*

Proof. By definition $\lambda \mapsto \lambda x_0$ is continuous, and by $\dim V = 1$ it is a vector space isomorphism. To finish the proof we are going to show that $\lambda x_0 \mapsto \lambda$ is continuous at 0. Let $0 < \epsilon < 1$. Since $|.|$ is by assumption non-trivial there exists a $\lambda_0 \in K$ such that $0 < |\lambda_0| < \epsilon$, and since V is assumed to be Hausdorff, there exists a neighbourhood U of 0 in V such that $\lambda_0 x_0 \notin U$.

As the scalar multiplication is continuous there exists a neighbourhood W of 0 and a $\delta > 0$ such that $\lambda W \subset U$ for all $\lambda \in K$, $|\lambda| < \delta$. Thus in particular the neighbourhood

$$N = \cup_{|\lambda|<\delta} \lambda W$$

is contained in U. The set N is balanced. This means that with $x \in N$ also $\mu x \in N$ for all $|\mu| \leq 1$.

Now $\lambda x_0 \in N$ implies $|\lambda| < \epsilon$; for $|\lambda| \geq \epsilon$ implies $|\lambda_0 \lambda^{-1}| < 1$ and hence $\lambda_0 x_0 = (\lambda_0 \lambda^{-1})\lambda x_0 \in N \subseteq U$, which is a contradiction. □

Make note of the fact that as a byproduct of the given proof one finds for any 0 neighbourhood U in a topological vector space a balanced 0-neighbourhood $N \subseteq U$.

1.2.5 Proposition. *Let K be a field provided with a complete non-trivial absolute value $|.|$, and let V be a Hausdorff topological vector space of finite dimension over K. Then taking any basis $\{x_1, \ldots, x_n\}$ of V the topological vector space K^n provided with topology induced by the norm $\|.\|_\infty$ is isomorphic to V via the mapping*

$$(\xi_j)_{j=1}^n \mapsto \xi_1 x_1 + \cdots + \xi_n x_n.$$

Hence there exists a unique topology on V such that V becomes a Hausdorff topological vector space. In particular, any two norms on V are equivalent.

Proof. We prove the assertion by induction on the dimension n of V. For $n = 1$ the assertion is the same as the one proved in Lemma 1.2.4.

Assume that the assertion is true for all spaces of dimension less than n, and let V be a Hausdorff topological vector space of dimension n. We take any bases $\{x_1, \ldots, x_n\}$ of V, and consider the isomorphism

$$(\xi_j)_{j=1}^n \mapsto \xi_1 x_1 + \cdots + \xi_n x_n,$$

which maps K^n onto V continuously. This is a consequence of the fact that scalar multiplication is continuous. To show that also the inverse mapping is continuous we are going to show that if $(y_i)_{i \in I}$, where $y_i = \xi_1^i x_1 + \cdots + \xi_n^i x_n$, is a Moore-Smith-sequence converging to 0 in V, then all coefficients converge to zero. If this were false - say for (ξ_1^i) -, then we could find a directed subset $J \subseteq I$ such that $|\xi_1^i| > \delta > 0$ for all $i \in J$. Let $\lambda_0 \in K,\ 0 < |\lambda_0| < \delta$.

If U is any 0-neighbourhood, then by the continuity of the scalar multiplication and by the considerations after the proof of Lemma 1.2.4 there exists a balanced 0-neighbourhood N such that $\lambda_0^{-1} N \subseteq U$. As $(y_i)_{i \in J}$ converges to 0, there exists a $i_0 \in J$ such that $y_i \in N,\ i \geq i_0$. Together with $|\lambda_0 (\xi_1^i)^{-1}| < 1$ we conclude

$$(\xi_1^i)^{-1} y_i = \lambda_0^{-1} \frac{\lambda_0}{\xi_1^i} y_i \in U.$$

Hence we showed that $((\xi_1^i)^{-1} y_i)_{i \in J}$ also converges to 0. Thus

$$(\xi_1^i)^{-1} y_i - x_1 = \frac{\xi_2^i}{\xi_1^i} x_2 + \cdots + \frac{\xi_n^i}{\xi_1^i} x_n \tag{1.2.1}$$

converges to $-x_1$ as i runs in J. The subspace of V spanned by $x_2, \ldots, x_n$ is by the induction hypothesis isomorphic (as a topological vector space) to K^{n-1} and, therefore, complete. This in turn shows that it is closed in V. But this contradicts the fact that the limit of (1.2.1) does not belong to this subspace.

It remains just the possibility that all the coefficient sequences $(\xi_j^i)_{i\in I}$, $j = 1, \ldots, n$ converge to zero and, hence, that

$$\xi_1 x_1 + \cdots + \xi_n x_n \mapsto (\xi_j)_{j=1}^n$$

is continuous at 0. □

1.3 Real Algebras

The main subject of this section will be to prove that there are not many fields extending $\mathbb{R}$ finite-dimensional.

1.3.1 Theorem. *Let A be a commutative algebra with 1 over $\mathbb{R}$, and assume that A contains an element j with $j^2 = -1$. Let $\mathbb{C}$ be identified with a subalgebra of A via $x+iy \mapsto x1+jy$. Assume that A is a normed vector space over $(\mathbb{R}, |.|)$ such that $\|xy\| \leq \|x\|\|y\|$ for all $x, y \in A$. Given $x_0 \in A \setminus \{0\}$, there exists an element $c \in \mathbb{C}$ such that $x_0 - c$ $(= x_0 - c1)$ is not invertible in A.*

Proof. First note that we can view A as a vector space over $\mathbb{C}$ by defining the scalar mulitiplication by

$$(\xi + i\eta)x := \xi x + j\eta x.$$

Moreover, by Proposition 1.2.5 the field $\mathbb{C}$ provided with the ordinary absolute value is isomorphic (algebraically and topologically) to the copy $\mathbb{R}1+\mathbb{R}j$ of $\mathbb{C}$ in A provided with $\|.\|$. Hence, the norms $\|\|$ and $|.|$ are equivalent on $\mathbb{C}$.

Secondly, the mapping $x \mapsto x^{-1}$ is continuous on the set of all invertible elements of A: Assume that $\|x - x_0\| < \frac{1}{2}\|x_0^{-1}\|^{-1}$. Then

$$\|x^{-1} - x_0^{-1}\| \leq \|x_0^{-1}\|\|x^{-1}\|\|x - x_0\|$$

and

$$\|x^{-1}\| - \|x_0^{-1}\| \leq \|x^{-1} - x_0^{-1}\| \leq \|x_0^{-1}\|\|x^{-1}\|\|x - x_0\| \leq \frac{1}{2}\|x^{-1}\|.$$

Thus $\|x^{-1}\| \leq 2\|x_0^{-1}\|$, and the above inequality can be continued:

$$\|x_0^{-1}\|\|x^{-1}\|\|x - x_0\| \leq 2\|x_0^{-1}\|^2\|x - x_0\|.$$

Assume that $x_0 - c$ is invertibel for all $c \in \mathbb{C}$. Consider the mapping $z \mapsto (x_0 - z)^{-1}$ from $\mathbb{C}$ into A. It is continuous, and it tends to 0 as $|z| \to \infty$. In fact, for some fixed $C > 0$ we have

$$\|((x_0 - z)^{-1})\| \leq \|\frac{1}{z}\|\|(\frac{x_0}{z} - 1)^{-1}\| \leq C\frac{1}{|z|}\|(\frac{x_0}{z} - 1)^{-1}\|,$$

and

$$\|(\frac{x_0}{z} - 1)^{-1}\| \to \|1^{-1}\| = 1,$$

as $|z| \to \infty$ because of the above proved continuity of the inversion.

Let φ be a real linear and continuous functional on A, and define $\psi(x) = \varphi(x) - i\varphi(jx)$. Then ψ is a continuous and $\mathbb{R}$-linear mapping from A into $\mathbb{C}$. Moreover, it is easy to check that $\psi((\xi + j\eta)x) = (\xi + i\eta)\psi(x)$, and we see that ψ is a complex linear continuous functional on A seen as a vector space over $\mathbb{C}$.

Now consider the function $f : \mathbb{C} \to \mathbb{C}$ defined by $f(z) = \psi((x_0 - z)^{-1})$. We already know that f is continuous, but it is even analytic at every $\zeta \in \mathbb{C}$:

$$\frac{f(\zeta) - f(z)}{\zeta - z} = \psi((x_0 - \zeta)^{-1}(x_0 - z)^{-1}) \to \psi((x_0 - \zeta)^{-2})$$

as $z \to \zeta$. Moreover, by what we saw above $f(z) \to 0$ as $|z| \to \infty$.

By Liouville's theorem $f(z) = 0$ for all $z \in \mathbb{C}$. Since φ was arbitrarily chosen, the Hahn-Banach Theorem implies $(x_0 - z)^{-1} = 0$, which is clearly a contradiction. □

1.3.2 Corollary. *Let K be a field extending $\mathbb{R}$, and assume that K has an absolute value $|.|$ extending the ordinary absolute value on $\mathbb{R}$. Then $K = \mathbb{R}$ or $K = \mathbb{C}$.*

Proof. If K contains an element j with $j^2 = -1$, then the assumption that K is a field and Theorem 1.3.1 show that $K = \mathbb{C}$.

In the contrary case let $L = K(j)$, where $j^2 = -1$. We define a norm on L (as an $\mathbb{R}$-space) by

$$\|x + jy\| := |x| + |y|.$$

This makes L into a normed $\mathbb{R}$-space. Furthermore, if $x + jy, x' + jy' \in L$, then

$$\|(x + jy)(x' + jy')\| = |xx' - yy'| + |xy' + x'y| \leq$$

$|x||x'| + |y||y'| + |x||y'| + |x'||y| = (|x| + |y|)(|x'| + |y'|) = \|x + jy\|\|x' + jy'\|$, and we can therefore apply Theorem 1.3.1 again to see that $L = \mathbb{C}$ and $K = \mathbb{R}$. □

The above corollary applies to any field extension K of $\mathbb{R}$ as long as there is an absolute value on K. If we assume that K is an algebraic extension of $\mathbb{R}$, then we can drop the existence of an absolute value.

1.3.3 Proposition. *Let K be an algebraic extension of $\mathbb{R}$. Then $K = \mathbb{R}$ or $K = \mathbb{C}$.*

Proof. If K contains an element j with $j^2 = -1$, then we find $\mathbb{C}$ as a subfield of K. As K is algebraic over $\mathbb{R}$ it is also algebraic over $\mathbb{C}$; but $\mathbb{C}$ is algebraically closed, and hence $K = \mathbb{C}$.

If K does not contain such an element j, then consider $K(j)$, which is again algebraic over $\mathbb{R}$. Apply the above argumentation to $K(j)$ we see that $K(j) = \mathbb{C}$, and therefore $K = \mathbb{R}$. □

1.4 The Module of an Automorphism

We are going to consider locally compact fields, and we will see that these fields carry an absolute value, which determines the topology of the field. To find this absolute value we consider the so-called module of Automorphisms.

Let G be a Hausdorff locally compact abelian topological group. Every such group carries a non-trivial translation invariant positive Borel-measure λ:

$$\lambda(x + Y) = \lambda(Y),$$

for all $y \in G$ and Borel-sets $Y \subset G$. Such a measure is determined uniquely up to a positive real factor and is called the Haar measure of G.

1.4.1 Definition. If $\alpha : G \to G$ is a bi-continuous Automorphism, then take any Borel-set $Y \subset G$ with positive and finite measure, and set

$$\mathrm{mod}_G(\alpha) = \frac{\lambda(\alpha(Y))}{\lambda(Y)}.$$

mod_G is called the module of α and neither depends on the particularly chosen Haar measure nor on the Borel-set Y.

The independence of the particularly chosen Haar measure is clear, and the the fact, that it does not depend on Y follows from the observation that with λ also $\lambda \circ \alpha$ is translation invariant and, hence, $\lambda \circ \alpha = c\lambda$ for some $c > 0$. This number is obviously nothing else, but mod_G. We are going to list some of the properties of this function.

1.4.2 Proposition. *1. If α, β are both bi-continuous automorphisms on G, then $\mathrm{mod}_G(\alpha \circ \beta) = \mathrm{mod}_G(\alpha)\mathrm{mod}_G(\beta)$. Trivially, $\mathrm{mod}_G(\mathrm{id}_G) = 1$, and, therefore, mod_G is a homomorphism from $\mathrm{Aut}(G)$ into $\mathbb{R}^+$. Hereby $\mathrm{Aut}(G)$ denotes the group of all bi-continuous automorphisms on G.*

2. If γ denotes the automorphism $x \mapsto -x$, then $\mathrm{mod}_G(\gamma) = 1$. In particular, $\mathrm{mod}_G(\alpha) = \mathrm{mod}_G(-\alpha)$ for any automorphism α on G.

3. Let α be a continuous automorphism. If X is a Borel-subset of G, then $\lambda(\alpha(X)) = \mathrm{mod}_G(\alpha)\lambda(X)$, and if $f \in L_1(G)$, then

$$\int_G f(\alpha^{-1}(x))d\lambda(x) = \mathrm{mod}_G(\alpha)\int_G f(x)d\lambda(x). \tag{1.4.1}$$

4. If G is compact or discrete, then $\mathrm{mod}_G(\alpha) = 1$ for any automorphism α.

5. Let G_1 and G_2 be two locally compact, Hausdorff and abelian topological groups, and $\alpha_1 \in \mathrm{Aut}(G_1), \alpha_2 \in \mathrm{Aut}(G_2)$. Then

$$\mathrm{mod}_{G_1\times G_2}(\alpha_1 \times \alpha_2) = \mathrm{mod}_{G_1}(\alpha_1)\mathrm{mod}_{G_2}(\alpha_2).$$

6. Let H be a closed subgroup of G, and let α be an automorphism on G such that $\alpha(H) = H$. Let α/H be the automorphism on G/H defined by $(\alpha/H)(x + H) = \alpha(x) + H$. Then

$$\mathrm{mod}_G(\alpha) = \mathrm{mod}_H(\alpha|_H)\mathrm{mod}_{G/H}(\alpha/H). \tag{1.4.2}$$

7. Let G_1, G_2 be two locally compact, Hausdorff and abelian topological groups, $\Phi : G_1 \to G_2$ be an isomorphism (topologically and algebraically) and let $\alpha \in \mathrm{Aut}(G_1)$. Then

$$\mathrm{mod}_{G_2}(\Phi \circ \alpha \circ \Phi^{-1}) = \mathrm{mod}_{G_1}(\alpha).$$

Proof. 1. For a Borel-set $Y \subseteq G$ with $0 < \lambda(Y) < \infty$ also $\beta(Y)$ is a Borel-set with non-zero and finite Haar measure. Hence the multiplicativity of mod_G is a consequence of

$$\frac{\lambda((\alpha \circ \beta)(Y))}{\lambda(Y)} = \frac{\lambda((\alpha \circ \beta)(Y))}{\lambda(\beta(Y))}\frac{\lambda(\beta(Y))}{\lambda(Y)}.$$

2. Let U be a compact neighbourhood of 0 in G. Then $U \cap (-U)$ is a compact neighbourhood of 0 such that $-(U \cap (-U)) = U \cap (-U)$. Taking $Y = U \cap (-U)$ in the definition of $\mathrm{mod}_G(\alpha)$ we see $\mathrm{mod}_G(\gamma) = 1$. The second assertion is a consequence of this fact and of the above proved multiplicativity.

3. $\lambda(\alpha(X)) = \mathrm{mod}_G(\alpha)\lambda(X)$ holds by definition for all Borel-sets X with non-zero and finite Haar measure. For the other Borel-sets this equality is easily checked by hand. For characteristic functions f (1.4.1) holds by the just proved equation. Thus it holds for all linear combinations of characteristic functions. An approximation argument shows that (1.4.1) holds for all $f \in L_1(G)$.

4. If G is compact or discrete, then one can assume the set Y in the definition of mod_G to be G or $\{0\}$, respectively, and one sees that $\mathrm{mod}_G(\alpha) = 1$ for any automorphism α.

5. This is an immediate consequence of the fact that the product measure of the two respective Haar measures of G_1 and G_2 is a Haar measure on $G_1 \times G_2$.

6. It is well known that given a Haar measure λ of G and a Haar measure μ of H one can choose a Haar measure ν on G/H such that

$$\int_G f(x)d\lambda(x) = \int_{G/H} (\int_H f(x+h)d\mu(h))d\nu(x+H).$$

for functions $f \in C_{00}(G)$. Note that the function within the outer integral on the right hand side only depends on $x + H$. Now we apply this equation to $f \circ \alpha^{-1}$:

$$\mathrm{mod}_G(\alpha) \int_G f(x)d\lambda(x) = \int_G f(\alpha^{-1}(x))d\lambda(x) =$$
$$\int_{G/H} (\int_H f(\alpha^{-1}(x) + \alpha^{-1}(h))d\mu(h))d\nu(x+H) =$$
$$\mathrm{mod}_H(\alpha|_H) \int_{G/H} (\int_H f(\alpha^{-1}(x) + h)d\mu(h))d\nu(x+H).$$

The function $x + H \mapsto \int_H f(\alpha^{-1}(x) + h)d\mu(h)$ is nothing else but $g \circ (\alpha/H)^{-1}$ when $g(x+H) = \int_H f(x+h)d\mu(h)$. Thus the above sequence of equalities continues:

$$= \mathrm{mod}_H(\alpha|_H)\mathrm{mod}_{G/H}(\alpha/H) \int_{G/H} (\int_H f(x+h)d\mu(h))d\nu(x+H),$$

and we are done.

7. If λ is a Haar measure on G_1, then $\lambda \circ \Phi^{-1}$. Thus

$$\mathrm{mod}_{G_2}(\Phi \circ \alpha \circ \Phi^{-1}) = \frac{\lambda \circ \Phi^{-1}(\Phi \circ \alpha \circ \Phi^{-1}(Y))}{\lambda \circ \Phi^{-1}(Y)} =$$

$$\frac{\lambda(\alpha(\Phi^{-1}(Y)))}{\lambda(\Phi^{-1}(Y))} = \mathrm{mod}_{G_1}(\alpha).$$

□

1.4.3 Examples. *1. Considering the additive group of a Hausdorff locally compact topological field K for a fixed $a \in K \setminus \{0\}$ one can consider the automophism $(K,+) \to (K,+)$ defined by*

$$x \mapsto ax.$$

We will write $\mathrm{mod}_K(a)$ for the module of this automorphism.

2. For $K = \mathbb{R}$ we have

$$\mathrm{mod}_{\mathbb{R}}(a) = \mathrm{mod}_{\mathbb{R}}(|a|) = \frac{\lambda(0,|a|)}{\lambda(0,1)} = |a|,$$

and for $K = \mathbb{C}$ we have $a\mathbb{D} = |a|\mathbb{D}$ and hence

$$\mathrm{mod}_{\mathbb{C}}(a) = \frac{\lambda(|a|\mathbb{D})}{\lambda(\mathbb{D})} = |a|^2.$$

3. If $K = \mathbb{Q}_p$, then we can write the compact open set $\mathbb{Z}_p$ as the disjoint union

$$\mathbb{Z}_p = \cup_{j=0,\ldots,p-1}\ (j + p\mathbb{Z}_p).$$

The Haar measure of the sets $j + p\mathbb{Z}_p$ is the same for all j. Thus

$$\lambda(\mathbb{Z}_p) = p\lambda(p\mathbb{Z}_p),$$

and hence $\mathrm{mod}_G(p) = \frac{1}{p}$ and further $\mathrm{mod}_{\mathbb{Q}_p}(p^n) = \frac{1}{p^n}$, $n \in \mathbb{Z}$. Moreover, if $a \in \mathbb{Q}_p$, $|a|_p = 1$, then we know that $a, a^{-1} \in \mathbb{Z}_p$ and, therefore, $a\mathbb{Z}_p = \mathbb{Z}_p$. This in turn implies $\mathrm{mod}_{\mathbb{Q}_p}(a) = 1$. Since one can write any $a \in \mathbb{Q}_p$ as $a = p^n b$, where $n \in \mathbb{Z}$ is such that $p^{-n} = |a|_p$ and $|b|_p = 1$. Alltogether we see $\mathrm{mod}_{\mathbb{Q}_p}(a) = |a|_p$.

4. With the same arguments as for $\mathbb{Q}_p$ one shows that for $a \in \mathbb{F}_q((T))$ the relation $\mathrm{mod}_{\mathbb{F}_q((T))}(a) = |a|_T$ holds true.

5. *For a Hausdorff locally compact field K let G be the additive group of the vector space K^n, and let $A \in GL(K,n)$. A represents a continuous automorphism on G, and*

$$\mathrm{mod}_{K^n}(A) = \mathrm{mod}_K(\det(A)). \tag{1.4.3}$$

To see this, note that by the Gaussian algorithm to solve linear equations we can write A as a finite product of matrices of the following three types:

$B = \mathrm{diag}\ (a,\dots,a)$, $a \neq 0$, B is a permutation matrix, or B is of the form

$$B(x_1,x_2,\dots,x_n)^T = (x_1 + \sum_{j=2}^{n} b_j x_j, x_2, \dots, x_n)^T,$$

for some $b_2,\dots,b_n \in K$.

Let U be a compact 0-neighbourhood in K. Then U^n is a compact 0-neighbourhood in K^n.

For diagonal matrices $B = \mathrm{diag}\ (a,\dots,a)$ we have

$$\lambda^n(B(U^n)) = \lambda^n((aU)^n) = \lambda(aU)^n = \mathrm{mod}_K(a)^n\lambda(U)^n = \mathrm{mod}_K(a)^n\lambda(U^n).$$

Hence, $\mathrm{mod}_{K^n}(B) = \mathrm{mod}_K(a)^n = \mathrm{mod}_K(a^n) = \mathrm{mod}_K(\det B)$.

For permutation matrices B we have $B(U^n) = U^n$, and see that $\mathrm{mod}_{K^n}(B) = 1 = \mathrm{mod}_K(\det B)$.

If B is of the third kind, then we calculate using Fubini's theorem and the translation invariance of λ

$$\lambda^n(B(U^n)) = \int_{K^n} \chi_{U^n}(B^{-1}(\xi_j)_j) d\lambda^n((\xi_j)_j) =$$

$$\int_K \chi_U(\xi_n) \int_K \chi_U(\xi_{n-1}) \dots \int_K \chi_U(\xi_1 - \sum_{j=2}^{n} b_j\xi_j) d\lambda(\xi_1)\dots d\lambda(\xi_{n-1}) d\lambda(\xi_n) =$$

$$\int_K \chi_U(\xi_n) \int_K \chi_U(\xi_{n-1}) \dots \int_K \chi_U(\xi_1) d\lambda(\xi_1)\dots d\lambda(\xi_{n-1}) d\lambda(\xi_n) = \lambda^n(U^n).$$

From this we see that $\mathrm{mod}_{K^n}(B) = 1 = \mathrm{mod}_K(\det B)$.

So we see that the assertion holds true for the mentioned three typs of matrices. Since mod *and* det *are multiplicative, the assertion also holds for general matrices.*

Above we defined $\mathrm{mod}_K(a)$ for any $a \in K^\times$. For $a = 0$ we define $\mathrm{mod}_K(0) = 0$. Note that with this definition mod_K satisfies AV1 and AV2.

1.4.4 Proposition. *The function $a \mapsto \mathrm{mod}_K(a)$ is a continuous function from K into $\mathbb{R}_0^+$.*

Proof. Let X be a compact neighbourhood of 0 in K. By the outer regularity of the Haar measure for any $\epsilon > 0$ and any $a \in K$ there exists an open neighbourhood U of aX such that $\lambda(U) \leq \lambda(aX) + \epsilon$; let W be a neighbourhood of a such that $WX \subset U$. Such a W exists by the continuity of the multiplication and by the compactness of X. For all $x \in W$ we have

$$\frac{\lambda(xX)}{\lambda(X)} \leq \frac{\lambda(U)}{\lambda(X)} \leq \frac{\lambda(aX)}{\lambda(X)} + \frac{\epsilon}{\lambda(X)}.$$

Thus $a \mapsto \mathrm{mod}_K(a)$ is upper semicontinuous at every $a \in K$. As $\mathrm{mod}_K(0) = 0$ and $\mathrm{mod}_K(a) > 0,\ a \neq 0$ we see that mod_K is continuous at zero. Moreover, with $a \mapsto \mathrm{mod}_K(a)$ also $a \mapsto \mathrm{mod}_K(a^{-1})$ is upper semicontinuous on $K^\times$ with values in $\mathbb{R}_+^\times$. Thus $a \mapsto \mathrm{mod}_K(a^{-1})^{-1} = \mathrm{mod}_K(a)$ is lower semicontinuous. □

1.4.5 Corollary. *If K is not a discrete field, then for any arbitrarily small $\epsilon > 0$ we can find an $a \in K$ such that $0 < \mathrm{mod}_K(a) \leq \epsilon$. Similarly we can find for any arbitrarily large $M > 0$ a $b \in K$ such that $\mathrm{mod}_K(b) \geq M$*

Moreover, if K is not discrete, K is not compact.

Proof. By the continuity we find a 0-neighbourhood U in K such that $\mathrm{mod}_K(a) = |\mathrm{mod}_K(a) - \mathrm{mod}_K(0)| \leq \epsilon$ for all $a \in U$. By assumption U contains not only the element 0. The second assertion follows if we apply the already shown part to $\epsilon = M^{-1}$ and take $b = a^{-1}$.

If K were compact, then $\mathrm{mod}_K(K)$ would be bounded. But this contradicts the second assertion of the present corollary. □

1.4.6 Proposition. *For every $m > 0$ the set $B_m = \{x \in K : \mathrm{mod}_K(x) \leq m\}$ is compact 0-neighbourhood.*

Proof. By Proposition 1.4.4 B_m is a closed 0-neighbourhood. Let V be any compact 0-neighbourhood in K, and let W be another 0-neighbourhood such that $WV \subseteq V$. It follow from the proof of the previous corollary that we can choose an $r = r^1 \in V \cap W$ such that $0 < \mathrm{mod}_K(r) < 1$. If $r^{n-1} \in V$, then $r^n = rr^{n-1} \in WV \subseteq V$. Hence $r^n \in V,\ n \in \mathbb{N}$, and the sequence (r^n) has an accumulation point r' in V. Since mod_K is continuous and since $\mathrm{mod}_K(r^n) = \mathrm{mod}_K(r)^n \to 0$, we conclude $\mathrm{mod}_K(r') = 0$ or equivalently $r' = 0$. Therefore $(r^n) \to 0$ as $n \to \infty$.

Now let $m > 0$ and let $a \in B_m$. From $r^n a \to 0$ we conclude that there exists a smallest integer $\nu \geq 0$ such that $r^\nu a \in V$; if $a \notin V$ (or equivalently $\nu > 0$), then $r^{\nu-1} a \notin V$, hence $r^\nu a \in V \setminus (rV)$. We also see that $V \setminus (rV) \neq \emptyset$ except $B_m \subseteq V$, in which case we are already done.

The closure X of $V \setminus (rV)$ is a compact set not containing 0. Hence

$$\mu := \inf_{x \in X} \mathrm{mod}_K(x) = \min_{x \in X} \mathrm{mod}_K(x) > 0.$$

Note that μ does not depend on a. Let $N \in \mathbb{N}$ be such that $\mathrm{mod}_K(r)^N \leq \frac{\mu}{m}$. If $a \in B_m \setminus V$ and ν is chosen as above, then we have

$$\mathrm{mod}_K(r)^N m \leq \mu \leq \mathrm{mod}_K(r^\nu a) = \mathrm{mod}_K(r)^\nu \mathrm{mod}_K(a) \leq \mathrm{mod}_K(r)^\nu m,$$

and hence $\nu \leq N$. Thus the number ν defined above is bounded from above by a constant not depending on the particular element $a \in B_m$. This means that any $a \in B_m$ is contained in at least one of the sets

$$V, r^{-1}V, \ldots, r^{-N}V,$$

and, hence, the closed set B_m is contained in the finite union of compact sets. □

1.4.7 Corollary. *The sets B_m, $m > 0$, make up a fundamental system of 0-neighbourhoods in K.*

Proof. Let V be a compact 0-neighbourhood in K and let $m > \sup_{x \in V} \mathrm{mod}_K(x)$ be so large that there exists a $b \in K$ such that $m > \mathrm{mod}_K(b) > \sup_{x \in V} \mathrm{mod}_K(x)$. Then $V \subsetneq B_m$ and the closure X of $B_m \setminus V$ is non-empty, does not contain 0 and is a closed subset of B_m and, therefore, compact. This yields

$$m' := \inf_{x \in X} \mathrm{mod}_K(x) > 0.$$

Clearly, $m' \leq m$. Now take $0 < \mu < m'$. Then $B_\mu \subseteq B_m$ and $B_\mu \cap X = \emptyset$, and, hence, $B_\mu \subseteq V$. □

1.4.8 Corollary. *We have $\mathrm{mod}_K(a) < 1$ if and only if $a^n \to 0$.*

1.4.9 Corollary. *A discrete subfield F of K is always finite.*

Proof. Let $a \in F$. Then $\mathrm{mod}_K(a) \leq 1$, since otherwise (a^{-n}) would converge to 0, which contradicts the fact that F is discrete. We see that the discrete set F is a subset of the compact set B_1. This is only possible if F is finite. □

1.4.10 Proposition. *There exists a constant $A > 0$ such that*

$$\mathrm{mod}_K(x+y) \leq A \max(\mathrm{mod}_K(x), \mathrm{mod}_K(y)) \tag{1.4.4}$$

for all $x, y \in K$. This equation is true for

$$A = \sup_{x \in B_1} \mathrm{mod}_K(1+x) (< \infty), \tag{1.4.5}$$

and this is the smallest value for A such that (1.4.4) holds.

Proof. By symmetry relation (1.4.4) holds for all $x, y \in K$ if and only if it holds for all $x \in K$ and $y \in K \setminus \{0\}$ with $\mathrm{mod}_K(x) \leq \mathrm{mod}_K(y)$. Setting $y = 1$ we see that the constant A from (1.4.4) cannot be smaller than the constant defined in (1.4.5). Conversely, if A is the constant from (1.4.5) and if $y \in K \setminus \{0\}$ with $\mathrm{mod}_K(x) \leq \mathrm{mod}_K(y)$, then because of $\mathrm{mod}_K(xy^{-1}) \leq 1$ we have

$$\mathrm{mod}_K(x+y) = \mathrm{mod}_K(y) \mathrm{mod}_K(1 + \frac{x}{y}) \leq A \mathrm{mod}_K(y).$$

Finally, note that A from (1.4.5) is finite since $1 + B_1$ is compact. □

The following Proposition will imply that some power of mod_K is an absolute value.

1.4.11 Lemma. *Let $|.|$ satisfy AV1 and AV2 on some field F. Then $|.|$ satisfies AV3 (triangle inequality) if and only if*

$$|x+y| \leq c \max(|x|, |y|), \ x, y \in K, \tag{1.4.6}$$

for some constant $c \leq 2$

Proof. Clearly, AV3 implies (1.4.6) with $c = 2$. Now assume that (1.4.6) holds. Let $n = 2^m$ for some $m \in \mathbb{N}$ and let $a_1, \ldots, a_n \in F$. Then by induction on m it is straight forward to prove that

$$|\sum_{j=1}^{2^m} a_j| \leq 2^m \max\{|a_j| : j = 1, \ldots, 2^m\}.$$

If $n > 1$ is arbitrary in $\mathbb{N}$ and $a_1, \ldots, a_n \in F$, then let $m \in \mathbb{N}$ be such that $2^{m-1} < n \leq 2^m$ and let $a_{n+1}, \ldots, a_{2^m}$ be zero. The previous inequality yields

$$|\sum_{j=1}^{n} a_j| \leq c \max(|\sum_{j=1}^{2^{m-1}} a_j|, |\sum_{j=2^{m-1}+1}^{2^m} a_j|) \leq$$

$$2\max(2^{m-1}\max\{|a_j| : j = 1,\dots,2^{m-1}\}, 2^{m-1}\max\{|a_j| : j = 2^{m-1}+1,\dots,2^m\}) =$$
$$22^{m-1}\max\{|a_j| : j = 1,\dots,n\} \le 2n\max\{|a_j| : j1,\dots,n\}.$$

In particular, for $a_j = 1,\ j = 1,\dots,n$ we get $|n| \le 2n$. Moreover, we obtain from the previous inequality trivially

$$|\sum_{j=1}^{n} a_j| \le 2n\sum_{j=1}^{n}|a_j|.$$

We can calculate now

$$|a+b|^n = |(a+b)^n| = |\sum_{j=0}^{n}\frac{n!}{j!(n-j)!}a^j b^{n-j}| \le$$

$$2(n+1)\sum_{j=0}^{n}|\frac{n!}{j!(n-j)!}||a|^j|b|^{n-j} \le$$

$$4(n+1)\sum_{j=0}^{n}\frac{n!}{j!(n-j)!}|a|^j|b|^{n-j} = 4(n+1)(|a|+|b|)^n.$$

Taking n-th roots and letting n tend to ∞ yields AV3. □

1.4.12 Corollary. *Let K be a locally compact Hausdorff topological field. Then there exists a constant $t > 0$ such that $(\mathrm{mod}_K)^t$ is an absolute value inducing the given topology on K.*

Proof. If K is discrete, then $\mathrm{mod}_K(x) = 1$ for all $x \neq 0$ and $\mathrm{mod}_K(0) = 0$. This coincides just with the trivial absolute value on K.

Let A be defined by (1.4.5) and in case $A > 2$ choose $t > 0$ such that $A^t \le 2$. By Proposition 1.4.10 $|.| = (\mathrm{mod}_K)^t$ satisfies (1.4.6) for $c = A^t \le 2$. By Lemma 1.4.11 $(\mathrm{mod}_K)^t$ is an absolute value, and Corollary 1.4.7 shows that the topology on K is the same as the one induced by $(\mathrm{mod}_K)^t$. □

We note once again, that for a K as above the topology is locally compact and hence K is complete. This is the same as saying that $|.| = (\mathrm{mod}_K)^t$ is complete.

1.4.13 Corollary. *Let K be as above. Then the following assertions are equivalent*

- *The constant A in (1.4.5) is one.*
- $\mathrm{mod}_K(m1_K) \le 1$ *for all* $m \in \mathbb{N}$.

- $\mathrm{mod}_K(m1_K) \leq C$ *for all* $m \in \mathbb{N}$ *and some fixed* $C > 0$.
- $(\mathrm{mod}_K)^t$ *is a non-archimedian absolute value for all* $t > 0$.
- $(\mathrm{mod}_K)^t$ *is a non-archimedian absolute value for some* $t > 0$.

Proof. If $A = 1$, then by (1.4.4) mod_K is a non-archimedian absolute value. The latter fact immediatley yields $\mathrm{mod}_K(m1_K) \leq \mathrm{mod}_K(1_K) = 1$.

If $\mathrm{mod}_K(m1_K) \leq C$ for all $m \in \mathbb{N}$, then the absolute value $|.| = (\mathrm{mod}_K)^t$ satisfies the assumptions in Proposition 1.1.5. Hereby $t > 0$ is chosen according to Corollary 1.4.12. Hence, $|.|$ satisfies AV4 and is therefore non-archimedian. But this yields that $(\mathrm{mod}_K)^t$ satisfies AV4 for all $t > 0$.

Finally, the fact that $(\mathrm{mod}_K)^t$ is non-archimedian for some $t > 0$ implies that mod_K satisfies AV4. By Proposition 1.4.10 we get $A = 1$. □

We are going to show that in the non-archimedian situation the absolute value mod_K is discrete.

1.4.14 Lemma. *Let* K *be a locally compact Hausdorff topological field. Then* mod_K *is a continuous and open homomorphism from* $K^\times$ *onto a closed subgroup of* Γ *of* $\mathbb{R}_+^\times$.

Proof. We already saw that mod_K satisfies AV2 and that it is continuous. Thus $\Gamma = \mathrm{mod}_K(K^\times)$ is a subgroup of $\mathbb{R}_+^\times$. This subgroup is closed. In fact, $(\Gamma \cup \{0\}) \cap [0, m]$ coincides with $\mathrm{mod}_K(B_m)$, and this set is compact (see Proposition 1.4.6) and hence closed.

It remains to prove that $\mathrm{mod}_K : K^\times \to \Gamma$ is open, which is done, if we have shown that $\mathrm{mod}_K(U)$ is a neighbourhood of $1 \in \mathbb{R}_+^\times$ for any neighbourhood U of 1. Assume the contrary, then there exists a sequence (γ_n) in $\Gamma \setminus \mathrm{mod}_K(U)$ which converges to 1. Let $a_n \in K^\times$ with $\mathrm{mod}_K(a_n) = \gamma_n$. Then $a_n \notin U$, but $\mathrm{mod}_K(a_n) \to 1$, and hence $a_n \in B_m$ for sufficiently large $m > 0$. By Proposition 1.4.6 $a_n \to a$ with $\mathrm{mod}_K(a) = 1$.

Therefore, we find an $n \in \mathbb{N}$ such that a_n lies in the neighbourhood aU of a. This implies $\gamma_n = \mathrm{mod}_K(a_n) \in \mathrm{mod}_K(U)$, which contradicts the choice of the sequence (γ_n). □

1.4.15 Corollary. *If the constant* A *in (1.4.5) is one (non-archimedian case), then* mod_K *is a discrete absolute value.*

Proof. By Proposition 1.1.6 applied to the non-archimedian value mod_K we have $\mathrm{mod}_K(1 + B_{\frac{1}{2}}) = \{1\}$. On the other hand Lemma 1.4.14 yields that $\mathrm{mod}_K(1 + B_{\frac{1}{2}})$ is open in Γ. □

We already know that the module induces an absolute value. We are going to examine all possibilities for this absolute value.

1.4.16 Lemma. *Let $F : \mathbb{N}_0 \to \mathbb{R}_+$ be a function satisfying*

$$F(mn) = F(n)F(m) \tag{1.4.7}$$

for all $m, n \in \mathbb{N}_0$. Moreover, assume that there exists a constant $c > 0$ such that

$$F(m+n) \leq c \max(F(m), F(n)), \tag{1.4.8}$$

for all $m, n \in \mathbb{N}_0$. Then either $F(m) \leq 1,\ m \in \mathbb{N}_0$, or there exists a real number $\delta > 0$ such that $F(m) = m^\delta,\ m \in \mathbb{N}_0$.

Proof. By (1.4.7) we have $F(0) = 0$ unless F is identically equal to one and $F(1) = 1$ unless F is identically equal to zero. Assuming $F \not\equiv 0$ and $F \not\equiv 1$ we define

$$f(m) = \max(0, \log F(m)).$$

In particular, we have $f(m) = 0$ if $F(m) = 0$. Our lemma will be proved as soon as we have shown that $f(m) = d \log(m)$ for some fixed constant $d \geq 0$. By (1.4.7) and (1.4.8) f satisfies ($m, n, k \in \mathbb{N}_0$)

$$f(m^k) = kf(m),\ f(mn) \leq f(m) + f(n),\ f(m+n) \leq a + \max(f(m), f(n)), \tag{1.4.9}$$

where $a = \max(0, \log c)$. By induction on r we find:

$$f(\sum_{j=0}^{r} m_j) \leq ra + \max(f(m_1), \ldots, f(m_r)).$$

For integers $m, n \geq 2$ we can express m in the form

$$m = \sum_{j=0}^{r} e_j n^j,$$

where $n^r \leq m < n^{r+1}$ and $0 \leq e_j < n,\ j = 0, \ldots, r$. By (1.4.9)

$$f(e_i n^i) \leq \max(f(0), \ldots, f(n-1)) + if(n),$$

and hence

$$f(m) \leq ra + \max(f(0), \ldots, f(n-1)) + rf(n).$$

As $n^r \leq m$ we have

$$\frac{f(m)}{\log(m)} \leq \frac{a + f(n)}{\log(n)} + \frac{\max(f(0), \ldots, f(n-1))}{\log(m)}.$$

Since m was arbitrarily chosen, we can replace m by m^k, and let k tend to ∞ in order to obtain

$$\frac{f(m)}{\log(m)} \leq \frac{a + f(n)}{\log(n)}.$$

Replacing n by n^k and letting k tend to ∞ yields

$$\frac{f(m)}{\log(m)} \leq \frac{f(n)}{\log(n)}.$$

Finally, if we interchange the roles of m and n, we see that $f(m)(\log m)^{-1}$ is constant for $m \geq 2$. □

Now we consider a non-discrete locally compact Hausdorff field K. From this Lemma and Corollary 1.4.13 we find two possibilities for $F(m) = \mathrm{mod}_K(m1_K)$. Either mod_K is a non-archimedian absolute value or $\mathrm{mod}_K(m1_K) = m^\delta$ for some $\delta > 0$. The archimedian case can be refined so that we have

1.4.17 Proposition. *Let K be a non-discrete locally compact Hausdorff topological field. Then exactly one of the following possibilities occurs.*

1. *The field K is of characteristic zero,* $\mathrm{mod}_K(m1_K) = |m|^c,\ m \in \mathbb{Z}$ *for some $c > 0$, and* mod_K *is not a non-archimedian absolute value.*

2. $\mathrm{char}\ K = 0$ *and* mod_K *is a non-archimedian absolute value. Moreover, there exists a prime number p and a constant $c > 0$ such that* $\mathrm{mod}_K(m1_K) = |m|_p^c,\ m \in \mathbb{Z}$.

3. $\mathrm{char}\ K = p$ *and* mod_K *is a non-archimedian absolute value. Moreover,* $\mathrm{mod}_K(m1_K) = 0$ *for $m \in p\mathbb{Z}$ and* $\mathrm{mod}_K(m1_K) = 1$ *if $p \not| m$.*

Proof. If $\mathrm{char}\ K = p > 0$, then we know from Corollary 1.4.13 that mod_K is a non-archimedian absolute value. Clearly, $\mathrm{mod}_K(np1_K) = \mathrm{mod}_K(0) = 0$. If m is not a multiple of p, then the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field shows that there is an integer l, such that $lm \equiv_p 1$. Thus

$$\mathrm{mod}(l1_K)\mathrm{mod}_K(m1_K) = \mathrm{mod}_K(ml1_K) = \mathrm{mod}_K(1_K) = 1.$$

Since both factors on the left hand side of this relation are at most one, they must be one.

If $\mathrm{char}\ K = 0$ and if $\mathrm{mod}_K(m1_K)$ is not bounded on $\mathbb{N}$, then Corollary 1.4.13 shows that mod_K is not a non-archimedian absolute value, and by Lemma 1.4.16

$$\mathrm{mod}_K(m1_K) = \mathrm{mod}_K(|m|1_K) = |m|^c,\ m \in \mathbb{Z}$$

for some $c > 0$.

Finally, if char $K = 0$ and $\mathrm{mod}_K(m1_K)$ is bounded on $\mathbb{N}$, then mod_K is a non-archimedian absolute value, and $\mathrm{mod}_K(m1_K),\ m \in \mathbb{Z}$ is, in fact, bounded by one (see Corollary 1.4.13). By Corollary 1.4.12 the absolute value mod_K induces the topology of K.

Consider $\mathbb{N}1_K \subseteq K$. This set is contained in the compact set B_1. Hence it has an accumulation point $a \in B_1$, and we find for any $\epsilon > 0$ infinitly many $m \in \mathbb{N}$ such that $\mathrm{mod}_K(a - m1_K) < \epsilon$. For two such numbers $m < m'$ AV4 yields

$$\mathrm{mod}_K(m'1_K - m1_K) \leq \max(\mathrm{mod}_K(a - m1_K), \mathrm{mod}_K(a - m'1_K)) < \epsilon.$$

Thus $m' - m$ is a natural number k such that $\mathrm{mod}_K(k1_K) < \epsilon$. Chosing $\epsilon \leq 1$ we see that $\{k \in \mathbb{Z} : \mathrm{mod}_K(k1_K) < 1\} \neq \emptyset$. By Lemma 1.1.4 this set is a prime ideal of $\mathbb{Z}$, and hence of the form $p\mathbb{Z}$ for some prime number p.

Let $c > 0$ be such that $\mathrm{mod}_K(p1_K) = p^{-c}$. If $n \in \mathbb{Z}$, then we can write $n = p^r m$ for some $r \geq 0$ and $m \in \mathbb{Z},\ m \notin p\mathbb{Z}$.

$$\mathrm{mod}_K(n1_K) = \mathrm{mod}_K(m1_K)\mathrm{mod}_K(p1_K)^r = p^{-rc} = |n|_p^c.$$

□

1.4.18 Definition. A non-discrete locally compact T2 field K will be called an $\mathbb{R}$-field if for K the first possibility of Proposition 1.4.17 occurs. Otherwise K is called a p-field when p is the smallest natural number such that $\mathrm{mod}_K(p1_K) < 1$.

To give a more detailed picture of how locally compact fields look like we bring

1.4.19 Proposition. *Let V be a locally compact topological vector space over a non-discrete locally compact Hausdorff topological field. Then V has finite dimension d over K, and $\mathrm{mod}_V(a) = \mathrm{mod}_K(a)^d$ for $a \in K^\times$.*

Proof. Once we have proved that V is finite dimensional the latter assertion is an immediate consequence of the fact that V is isomorphic to K^d (see Corollary 1.4.12 and Proposition 1.2.5) and of (1.4.3).

Let $a \in K$ such that $\mathrm{mod}_K(a) \in (0, 1)$. By Corollary 1.4.8 $a^n \to 0$ for $n \to \infty$. This implies $\mathrm{mod}_V(a) \in (0, 1)$. In fact, choose a compact neighbourhood U of 0. Thus $\mu(U) \in (0, \infty)$, when μ denotes the Haar measure of V.

As K is non-discrete the same is true for V, and therefore U contains infinitly many points and we see that $\mu(\{0\}) = 0$. By the outer regularity we

can find a 0-neighbourhood W contained in U such that $\mu(W) \in (0, \frac{\mu(U)}{2})$. By the continuity of the scalar multiplication we find a 0-neighbourhood Y such that $YU \subseteq W$. For sufficiently large n we have $a^n \in Y$, and hence for these n

$$\mu(a^n U) \leq \mu(W) \leq \frac{\mu(U)}{2}.$$

We see that $\mathrm{mod}_V(a^n) \leq \frac{1}{2}$. Thus $\mathrm{mod}_V(a) < 1$.

Let V' be a subspace of V of finite dimension δ. By Proposition 1.2.5 V' is isomorphic to K^δ. In particular, it is a complete and, hence, closed subgroup of V. Consider the locally compact topological vector space $V'' = V/V'$. By (1.4.2) we have

$$\mathrm{mod}_V(a) = \mathrm{mod}_{V'}(a)\mathrm{mod}_{V''}(a) = \mathrm{mod}_K(a)^\delta \mathrm{mod}_{V''}(a).$$

As for V'' the fact $\mathrm{mod}_K(a) \in (0,1)$ implies $\mathrm{mod}_{V''}(a) \in (0,1)$. This shows that there must be an upper bound for δ since otherwise $\mathrm{mod}_V(a)$ would be zero. In other words, V must be finite dimensional. □

1.4.20 Lemma. *Let K be a p-field. Then $k = R/P$ is a finite field of characteristic p. Hereby $R = \{x \in K : \mathrm{mod}_K(x) \leq 1\} = B_1$ and $P = \{x \in K : \mathrm{mod}_K(x) < 1\}$.*

Proof. By Lemma 1.1.4 P is a maximal ideal of R. Hence $k := R/P$ is a field. Since p is the smallest natural number with $\mathrm{mod}_K(p1_K) < 1$, we see $\mathrm{char}\ k = p$. Moreover, the cosets of P in R make up an open covering of the compact set $R = B_1$. Thus there are only finitely many cosets, and therefore $k \cong \mathbb{F}_q$ for some $q = p^f$. □

1.4.21 Theorem. *Let K be a non-discrete locally compact Hausdorff topological field. Then exactly one of the follwing possibilities occurs.*

1. *K is an $\mathbb{R}$-field, then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.*
2. *$\mathrm{char}\ K = 0$ and K is a p-field. In this case there exists a subfield L of K, which is an isomorphic copy of $\mathbb{Q}_p$ in the algebraic and in the topologic sense. If $d = \dim_L(K)$, then $\mathrm{mod}_K(x) = |x|_p^d$ for all $x \in L$.*
3. *$\mathrm{char}\ K = p$ and mod_K is an non-archimedian absolute value. There exists a maximal number $f \in \mathbb{N}$ such that K contains a finite subfield, which is isomorphic to $\mathbb{F}_q$, $q = p^f$.*

Proof. If $\mathrm{char}\ = p$, then we know from Proposition 1.4.17 that K is a p-field. By Lemma 1.4.20 we know that $k := R/P$ is a finite field of characteristic p with $q = p^f$ elements. If F is a finite subfield of K, then F is of characteristic

p and it contains at most q elements. In fact, $F \subseteq R$ since any $x \in F^\times$ has finite order, and the difference of two distinct elements of F is invertible in $F \subseteq R$. Thus different elements are contained in different cosets, and the canonical mapping from R onto R/P restricted to F is injective.

Now assume that char $K = 0$. By Proposition 1.4.17 we have $\mathrm{mod}_K(m1_K) = |m|_p^c$, where p is a prime number if mod_K is a non-archimedian absolute value, and $p = \infty$ and $|.|_\infty = |.|$ is the ordinary absolute value if mod_K is not a non-archimedian absolute value. By AV2 we can lift this relation to $\mathbb{Q} \subseteq K$. Since $|.|_p$ is an absolute value equivalent to $(\mathrm{mod}_K)^t$ (see Corollary 1.4.12) on $\mathbb{Q}$, we see from Proposition 1.2.1 that the closure L of $\mathbb{Q}$ in K is a completion of $\mathbb{Q}$ with respect to $|.|_p$. By the examples following Proposition 1.2.1 we see that $L \cong \mathbb{Q}_p$ if $p < \infty$ and $L \cong \mathbb{R}$ if $p = \infty$. Moreover, K is a locally compact vector space over the locally compact field L. By Proposition 1.4.19 $d = \dim_L(K) < \infty$, and $\mathrm{mod}_K(a) = \mathrm{mod}_L(a)^d$, $a \in L$. In particular, with the notation of Proposition 1.4.17 we obtain $d = c$.

If $p < \infty$, then we are done. Otherwise, Proposition 1.3.3 yields $K = L \cong \mathbb{R}$ or $K \cong \mathbb{C}$. □

We will see that in the case char $(K) > 0$ the space K is isomorphic to $\mathbb{F}_q((T))$.

1.5 The structure of p-fields

In this section we are going to examine the structure of non-archimedian absolute values in detail.

1.5.1 Proposition. *Let K be a p-field and let*

$$R = \{x \in K : \mathrm{mod}_K(x) \leq 1\}, \quad P = \{x \in K : \mathrm{mod}_K(x) < 1\}.$$

Then R is a commutative ring with 1 and P is its unique maximal ideal of R. $R \setminus P$ coincide with the units of R. Both sets R and P are open and compact in K. $k = R/P$ is a finite field with char $(k) = p$. *Moreover, R is the unique maximal compact subring of K.*

Let $f \in \mathbb{N}$ such that k has $q = p^f$ elements, and let $\Gamma = \mathrm{mod}_K(K^\times)$ as in Lemma 1.4.14 and Corollary 1.4.15. Then this subgroup of $\mathbb{R}_+^\times$, is generated by q, i.e. $\Gamma = \{q^n : n \in \mathbb{Z}\}$.

If $\pi \in K$ such that $\mathrm{mod}_K(\pi) = q^{-1}$, then $P = \pi R$. In fact, we have

$$P^n = \pi^n R = \{x \in K : \mathrm{mod}_K(x) \leq \frac{1}{q^n}\}. \tag{1.5.1}$$

for all $n \in \mathbb{N}$. These sets are ideals of R. We set $P^n = \pi^n R$ for $n \in \{0, -1, -2, \dots\}$. Then for all $n \in \mathbb{Z}$ (1.5.1) holds, and P^n is open and compact in K.

For integers $m \leq n$ multiplication with π^m sets up an isomorphism from R/P^{n-m} onto P^m/P^n, and these rings have q^{n-m} elements.

Proof. By Lemma 1.1.4 we already know that R is a commutative ring and P is its unique maximal ideal. As the units of a ring are just the elements, which are not contained in the maximal ideal of R we see that $R \setminus P = R^\times$. By Lemma 1.4.20 k is a finite field of characteristic p, i.e. contains $q = p^f$ elements for some $f \in \mathbb{N}$.

By Corollary 1.4.15 the subgroup $\Gamma = \mathrm{mod}_K(K^\times)$ is discrete in $\mathbb{R}_+^\times$, i.e. $\Gamma = \{\gamma^n : n \in \mathbb{Z}\}$ for some $\gamma > 1$. Thus we can rewrite R and P as

$$R = \{x \in K : \mathrm{mod}_K(x) \leq 1\} = \{x \in K : \mathrm{mod}_K(x) < \gamma\},$$

$$P = \{x \in K : \mathrm{mod}_K(x) < 1\} = \{x \in K : \mathrm{mod}_K(x) \leq \frac{1}{\gamma}\},$$

and see that R and P are both closed and open in K. As $R = B_1$ and $P = B_{\gamma^{-1}}$ both sets are compact (see Proposition 1.4.6). Now let $\pi \in K$ such that $\mathrm{mod}_K(\pi) = \gamma^{-1}$. Then we obtain

$$\pi R = \{x \in K : \mathrm{mod}_K(x) \leq \frac{1}{\gamma}\} = P,$$

and further from this $P^n = \pi^n R = \{x \in K : \mathrm{mod}_K(x) \leq \gamma^{-n}\}$.

If R' is a subring of K and if $x \in R' \setminus R$, then $\mathrm{mod}_K(x) > 1$, and, hence, (x^n) has no converging subsequence. Thus R' cannot be compact, and R is the unique maximal compact subring of K.

Now we have

$$\gamma = \frac{1}{\mathrm{mod}_K(\pi)} = \frac{\lambda(R)}{\lambda(\pi R)} = \frac{\lambda(R)}{\lambda(P)} = q,$$

because R is the disjoint union of $\#(R/P)$ many cosets $x + P$, which all have the same Haar measure as P has.

Finally, for integers $m \leq n$ the multiplication with π^m is an isomorphism from R onto $\pi^m R = P^m$ such that it maps the ideal $\pi^{n-m} R = P^{n-m}$ of R onto the subgroup with respect to $+$ (ideal in the case $0 \leq m \leq n$) $\pi^{n-m} P^m = \pi^{n-m} \pi^m R = P^n$ of P^m. In particular, R/P^{n-m} has the same number of elements as P^m/P^n, which we denote for the moment by l. Thus

we can write P^m as the disjoint union of l many cosets $x + P^n$; these cosets are open and compact. This yields

$$\frac{1}{\mathrm{mod}_K(\pi^{n-m})}\lambda(\pi^{n-m}P^m) = \lambda(P^m) = l\lambda(P^n),$$

and hence $l = \mathrm{mod}_K(\pi^{n-m})^{-1} = q^{n-m}$. □

1.5.2 Corollary. *If ϕ is a bi-continuous automorphism on K, then $\phi(R) = R$, $\phi(P) = P$ and $\mathrm{mod}_{(K,+)}(\phi) = 1$.*

Proof. With R also $\phi(R)$ is a maximal compact subring of K. This yields $R = \phi(R)$. Moreover, the unique maximal ideal P is mapped onto a maximal ideal, and hence $\phi(P) = P$. Finally,

$$\mathrm{mod}_{(K,+)}(\phi) = \frac{\lambda(\phi(R))}{\lambda(R)} = 1.$$

□

1.5.3 Definition. With the notation from Proposition 1.5.1 the number q will be called the module of K. Any element $\pi \in K^\times$ with $\mathrm{mod}_K(\pi) = q^{-1}$ or equivalently with $\pi R = P$ will be called a prime element of K. For any $x \in K^\times$ let $\mathrm{ord}_K(x)$ the integer n such that $\mathrm{mod}_K(x) = q^{-n}$. We set $\mathrm{ord}_K(0) = +\infty$.

1.5.4 Corollary. *R is an euclidean ring, and if I is an ideal of R, then $I = P^n$ for some integer $n \geq 0$.*

Proof. Let $a, b \in R$, $b \neq 0$ and set $m = \mathrm{ord}_K(a)$, $n = \mathrm{ord}_K(b)$. If $m \geq n$, we have $a = bs + 0$ with some $s \in K$ such that $\mathrm{ord}_K(s) \geq 0$, i.e. $s \in R$. Otherwise, we have $a = b0 + a$ with $\mathrm{ord}_K(a) < ord_K(b)$. Thus R is an euclidean ring.

If $\{0\} \subsetneq I \subsetneq R$ is an ideal of R, then I is contained in the unique maximal ideal P. Let n be the minimal order of elements in P. Then $n \in \mathbb{N}$, and choose $x \in I$ such that $\mathrm{ord}_K(x) = n$. Moreover, $xR \subseteq I$. On the other hand if $y \in I$, then $\mathrm{ord}_K(y) \geq n$, and further $\mathrm{ord}(x^{-1}y) \geq 0$. This yields $y = x(x^{-1}y)$ with $x^{-1}y \in R$, and hence $y \in xR$. Finally, it is elementary to see that

$$I = xR = \{y \in K : \mathrm{mod}_K(y) \leq \mathrm{mod}_K(x)\} = P^{\mathrm{ord}_K(x)}.$$

□

With the help of the notation introduced above we will obtain a series representation of each element in K. In order to show this we need the following lemma.

1.5.5 Lemma. *Let K be a field and let $|.|$ be a complete non-archimedian absolute value. If $(a_j)_{j\in\mathbb{N}_0}$ is a sequence in K, then*

$$\sum_{j=0}^{\infty} a_j$$

converges if and only if the sequence $(a_j)_{j\in\mathbb{N}_0}$ converges to zero.

Proof. The convergence of the serie means the convergence of the sequence of the partial sums

$$(s_n)_{n\in\mathbb{N}_0} = (\sum_{j=0}^{n} a_j)_{n\in\mathbb{N}_0}.$$

Thus $a_n = s_n - s_{n-1} \to 0$ as $n \to \infty$.

Conversely, assume that the sequence $(a_j)_{j\in\mathbb{N}_0}$ converges to zero. For $m, n \in \mathbb{N}_0,\ m < n$ we have

$$|s_n - s_m| = |\sum_{j=m+1}^{n} a_j| \leq \max\{|a_j| : j = m+1, \ldots, n\},$$

and see that $(s_n)_{n\in\mathbb{N}_0}$ is a Cauchy sequence. By the completeness assumption it converges. □

1.5.6 Corollary. *With the notation from Proposition 1.5.1 let $\xi \in P \setminus \{0\}$ and set $n = \mathrm{ord}_K(\xi)$. Let A be a full set of representatives of the the classes modulo P^n in R.*

Then any $x \in P^{nm},\ m \in \mathbb{Z}$ can be expressed in one and only one way as the limit of a series of the form

$$\sum_{j=m}^{\infty} a_j \xi^j, \tag{1.5.2}$$

where all the coefficients a_j belong to A. Conversely, any such series determines a unique element of $x \in P^{nm}$.

Proof. By Lemma 1.5.5 applied to $|.| = \mathrm{mod}_K(.)$ shows that any series of the form (1.5.2) converges, and since all the partial sums of this series belong to the closed set P^{nm}, also its limit lies in P^{nm}.

If the limits a and b of two such series with coefficients (a_j) and (b_j) coincide, and if these coefficient sequences would not be the same, then we could find a smallest index $l \geq m$ with $a_l \neq b_l$.

As

$$\sum_{j>l}^{\infty} a_j \xi^j, \quad \sum_{j>l}^{\infty} b_j \xi^j \in P^{(l+1)n}$$

we get $0 = a - b \in a_l \xi^l - b_l \xi^l + P^{(l+1)n}$ and from this $\mathrm{ord}_K(a_l - b_l) \geq n$, or $a_l - b_l \in P^n$. But this contradicts the fact, that by the choice of A the different elements a_l and b_l must belong to different cosets modulo P^n.

Finally if $x \in P^{nm}$, then $\xi^{-m} x \in R$ and we choose $a_m \in A$ such that $\xi^{-m} x - a_m \in P^n$, or $x - \xi^m a_m \in P^{n(m+1)}$. Continuing inductively in that manner we find a sequence $(a_m, a_{m+1}, \dots)$ such that

$$x - \sum_{j=m}^{N} a_j \xi^j \in P^{n(N+1)}.$$

But this means that the series (1.5.2) converges to x. □

In the following theorem we will meet a very particular full set of representatives of the the classes modulo P in R. Before this we are going to bring a lemma.

1.5.7 Lemma. *For all $n \in \mathbb{N}_0$ we have $(1+P)^{p^n} \subseteq 1 + P^{n+1}$.*

Proof. For $n = 0$ we trivially have equality. Assume that is true for n. Then we have

$$(1+P)^{p^{n+1}} = ((1+P)^{p^n})^p \subseteq (1 + P^{n+1})^p.$$

If $1 + x \in 1 + P^{n+1}$, then

$$(1+x)^p = 1 + px + \sum_{j=2}^{p} \frac{p!}{(p-j)!j!} x^j.$$

The addends in the sum all belong to $Rx^2 \subseteq RP^{2n+2} \subseteq P^{n+2}$. Moreover, $\mathrm{ord}_K(px) = \mathrm{ord}_K(p1_K) + \mathrm{ord}_K(x) > \mathrm{ord}_K(x) \geq n+1$, and hence $px \in P^{n+2}$. We obtain $(1+x)^p \in 1 + P^{n+2}$ and see that $(1 + P^{n+1})^p \subseteq 1 + P^{n+2}$. □

1.5.8 Theorem. *With the notation from Proposition 1.5.1 there exists a unique subgroup $M^\times$ of $K^\times$ with $q-1$ elements.*

This subgroup is cyclic and $M = M^\times \cup \{0\}$ is contained in R and is a full set of representatives of the the classes modulo P in R.

If $N^\times$ is a subgroup of $K^\times$ with the property that all $x \in N^\times$ are of finite order $\mathrm{ord}_{N^\times}(x)$ *such that p does not divide* $\mathrm{ord}_{N^\times}(x)$*, then $N^\times \subseteq M^\times$. In particular,*

$$M^\times = \{x \in K : x^{q-1} = 1_K\} = \{x \in K : \exists n \in \mathbb{N} : p \not| n \text{ and } x^n = 1_K\}.$$

Proof. Let ρ be the canonical mapping from R onto $k = R/P$. It is well known that $k^\times$ is cyclic of order $q-1$. Hence $\rho(x)^{q-1} = 1_k$ for $x \in R^\times = R\backslash P$.

This means that $x^{q-1} \in 1 + P$. Lemma 1.5.7 and the fact that $q = p^f$ we get $x^{(q-1)q^n} \in 1 + P^{fn+1}$ and further

$$x^{q^{n+1}} - x^{q^n} = -x^{q^n}(1 - x^{(q-1)q^n}) \in RP^{fn+1} = P^{fn+1},\ n \in \mathbb{N}_0.$$

We conclude from this that for $x \in R^\times$ the limit

$$\omega(x) = \lim_{n\to\infty} x^{q^n}$$

exists. In fact,

$$\lim_{n\to\infty} x^{q^n} = x + \sum_{n=0}^{\infty}(x^{q^{n+1}} - x^{q^n}), \tag{1.5.3}$$

and the addends of the series belong to P^{fn+1} and, therefore, converge to zero. By Lemma 1.5.5 the series converges.

Clearly, $\omega(xy) = \omega(x)\omega(y)$ and $\omega(1_K) = 1_K$. Thus ω is a homomorphism from $R^\times$ into $R^\times$. As

$$\omega(x)^{q^k} = \lim_{n\to\infty} x^{q^{n+k}} = \omega(x),$$

we have $\omega \circ \omega = \omega$. From (1.5.3) we see that

$$\omega(x) - x = \sum_{n=0}^{\infty}(x^{q^{n+1}} - x^{q^n}) \in P. \tag{1.5.4}$$

If $x \in 1_K + P$, then by Lemma 1.5.7 we have $x^{q^n} \in 1 + P^{fn}$, and $x^{q^n} \to 1_K$, i.e. $\omega(x) = 1_K$. Conversely, if $x \notin 1_K + P$, then by (1.5.4) $\omega(x) \in x + P$, $(x + P) \cap (1_k + P) = \emptyset$, and hence $\omega(x) \neq 1_K$. We showed that $\ker(\omega) = 1_K + P$.

An equivalent formulation of (1.5.4) is to say that $\rho \circ \omega = \rho|_{R^\times}$. From this we see that ρ restricted to the $M^\times = \omega(R^\times)$ is surjective as a mapping into $k^\times$. As $\ker(\rho|_{R^\times}) = 1_K + P = \ker(\omega)$ we also obtain the injectivity of $\rho|_{M^\times}$.

Thus $\rho|_{M^\times}$ is an isomorphism from $M^\times$ onto $k^\times$. Hence $M^\times$ is a cyclic subgroup of $K^\times$ with $q - 1$ elements, and $M = M^\times \cup \{0\}$ is a full set of representatives of the the classes modulo P in R.

Let $N^\times$ be a finite subgroup of $K^\times$ and $n \in \mathbb{N}$, $\gcd(q,n) = 1$ with the property that $\mathrm{ord}_{N^\times}(x) | n$ for all $x \in N^\times$. As $1 = \mathrm{mod}_K(1_K) = \mathrm{mod}_K(x^n) = \mathrm{mod}_K(x)^n$, $x \in N$ we have $N^\times \subseteq R^\times$. Moreover, $\gcd(q,n) = 1$ is equivalent to the fact that $[q]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus there exists an $m \in \mathbb{N}$ such that $[q^m]_n = [q]_n^m = [1]_n$ or $q^m = 1 + nl$. For $x \in N^\times$ we have

$$x^{q^m} = x^{1+nl} = x^{1+\mathrm{ord}_{N^\times}(x)l'} = x,$$

and therefore

$$\omega(x) = \lim_{j\to\infty} x^{q^{jm}} = x \in M^\times.$$

In particular, we just proved that $M^\times$ is the maximal subgroup of $K^\times$ whose order is relatively prime to q.

As $M^\times$ has $q-1$ elements we have $M^\times \subseteq \{x \in K : x^{q-1} = 1_K\}$, and since $p \not| (q-1)$,

$$\{x \in K : x^{q-1} = 1_K\} \subseteq \{x \in K : \exists n \in \mathbb{N} : p \not| n \text{ and } x^n = 1_K\}.$$

Finally, if $x^n = 1$ with $p \not| n$, then all roots of the polynomial $X^n - 1$ in K form a subgroup $N^\times$ of order at most n in $K^\times$. As the order of every element of $N^\times$ must divide n the considerations from above show $x \in N^\times \subseteq M^\times$.

For the sake of completeness we mention that if $x \in P$, then one has $x^{q^n} \in P^{q^n}$, and therefore $\omega(x) = \lim_{n\to\infty} x^{q^n} = 0$. Now we have $M = \omega(R)$ and $x - \omega(x) \in P$ holds for all $x \in R$. The latter assertion can also be expressed as $\rho \circ \omega = \rho$. Moreover, $\omega^{-1}(\{0\}) = P$ and, hence, $\rho|_M$ is a bijection from M onto k. □

1.5.9 Corollary. *With the notation from Theorem 1.5.8 assume* $\mathrm{char}\,(K) = p$. *Then M is a subfield of K.*

Proof. With the notation of the proof of Theorem 1.5.8 let $x, y \in R$ and calculate

$$(x-y)^{q^n} = x^{q^n} - y^{q^n} + q^n \sum_{j=1}^{q^n-1} \frac{(q^n-1)!}{(q^n-j)!j!} x^{q^n-j} y^j = x^{q^n} - y^{q^n},$$

because $q1_K = 0$ and $(-1_K)^{q^n} = -1_K$. Thus by the last paragraph in the proof of Theorem 1.5.8 $\omega(x) = \lim_{n\to\infty} x^{q^n}$ is a ring homomorphism with kernel P. As $\rho = \rho\circ\omega$ also has kernel P we see that $\rho|_M$ is a ring isomorphism from M onto k. Thus M is a field isomorphic to k. □

1.5.10 Corollary. *Let K be a p-field of characteristic p, and let $q = p^f = \#k$. Then $K \cong \mathbb{F}_q((T))$.*

Proof. By Corollary 1.5.9 and Theorem 1.5.8 M is a subfield of K and a full set of representatives of the the classes modulo P in R. By Corollary 1.5.6 every element of $K^\times$ can be written uniquely as

$$\sum_{l=m}^{\infty} a_l \xi^l,$$

where $\mathrm{ord}_K(\xi) = 1$ and $a_j \in M$. m is chosen such that $a_m \neq 0$, i.e. m is just the order of this series. Moreover, every such series converges to a unique element in $K^\times$.

Using the continuity of the multiplication and the fact that M is a field we obtain

$$(\sum_{l=m}^{\infty} a_l \xi^l)(\sum_{l=n}^{\infty} b_l \xi^l) = \sum_{l=m+n}^{\infty} (\sum_{i=m}^{l-n} a_i b_{l-i})\xi^l.$$

Now let $\phi : K \to \mathbb{F}_q((T))$ by defined by $\phi(0) = 0$ and

$$\phi(\sum_{l=m}^{\infty} a_l \xi^l) = \sum_{l=m}^{\infty} a_l T^l,$$

and see that ϕ is an isomorphism. Moreover, if $x = \sum_{l=m}^{\infty} a_l \xi^l$, $a_m \neq 0$, then $m = \mathrm{ord}_K(m)$, and hence $\mathrm{mod}_K(x) = q^{-m} = |\phi(x)|_T$. Thus ϕ is a bi-continuous isomorphism. □

1.6 Extensions of locally compact fields

An algebra L over a field K is a vector space over K, which is provided with a multiplication (in general not commutative):

$$(x; y) \mapsto xy,$$

from $L \times L \to L$ such that the distributive and associative law holds true, and $\alpha(xy) = ()y = x(\alpha y)$, $x, y \in L$, $\alpha \in K$. An algebra is called division algebra, if $(L^\times, \cdot)$ is a group. Hereby $L^\times = L \setminus \{0\}$. In this case we always think of K to be contained in L by the embedding $\xi \mapsto \xi 1_L$. In particular, $1_K = 1_L$.

If K is a topological field and L a topological vector space over K, then L is called a topological algebra, if it is a an algebra over K such that the multiplication is continuous.

1.6.1 Proposition. *Let K be a locally compact Hausdorff topologocal field, and let L be a finite dimensional vector space over K.*

If L is a division algebra and if $L(\cong K^n)$ is provided with the product topology, then L is a locally compact Hausdorff topological in general non-commutative field. This topology is in fact the unique topology such that L becomes a Hausdorff topological vector space.

Proof. We can provide $L \cong K^n$ with the product topology, which is the unique topology, such that L becomes a topological vector space (see Proposition 1.2.5). This topology is clearly locally compact.

If L is an algebra over K, then for a fixed $a \in L$ the multiplication with a is a linear mapping $x \mapsto ax$ on L. Thus it can be realized as a matrix $M(a) \in K^{n\times n}$. Clearly, $M(ab) = M(a)M(b),\ M(\xi a) = \xi M(a)$ and $M(a+b) = M(a) + M(b)$ for $a, b \in L,\ \xi \in K$.

The mapping $M : a \mapsto M(a)$ is therefore a linear mapping from $L \cong K^n$ into $K^{n\times n}$. Its kernel is the zero space because for $a \neq 0$ we have $M(a)M(a^{-1}) = I$. The inverse mapping $M^{-1} : \text{ran } (M) \to L$ is also linear.

As every linear mapping within finite dimensional vector spaces and as the matrix multiplication $(A; B) \mapsto AB$ is continuous as a mapping $K^{n\times n} \times K^{n\times n} \to K^{n\times n}$ we see that

$$(a; b) \mapsto (M(a); M(b)) \mapsto M(a)M(b) \mapsto M^{-1}(M(a)M(b)) = ab$$

is continuous. By Cramer's rule the mapping $A \mapsto A^{-1}$ is continuous an $GL(K, n) \subseteq K^{n\times n}$. Thus

$$a \mapsto M(a) \mapsto M(a)^{-1} \mapsto M^{-1}(M(a)^{-1}) = a^{-1}$$

is a continuous mapping from $L^\times$ onto itself. □

1.6.2 Proposition. *Let K be a p-field and let K' be a commutative division algebra over K of finite dimension n. Then K' is also a p-field.*

Moreover, if R and R' denote the maximal compact subring of K and K', respectively, and P and P' their respective maximal ideals, then $R' \cap K = R$ and $P' \cap K = P$.

Finally, if $k' = R'/P',\ k = R/P, q' = \#k',\ q = \#k$ and if π is a prime element of K and we set $e = \text{ord}_{K'}(\pi)$, then $q' = q^f$ for some $f \in \mathbb{N}$ and $\dim_K(K') = n = ef$.

Proof. By Proposition 1.6.1 K' can be provided with a unique topology such that it becomes a locally compact Hausdorff topological vector space.

By Proposition 1.4.19 we have $\mathrm{mod}_K(x)^n = \mathrm{mod}_{K'}(x)$ for $x \in K$. Thus p is also the smallest natural number such that $\mathrm{mod}_{K'}(p1_{K'}) < 1$, i.e. K' is a p-field. Finally because of $\mathrm{mod}_K(x)^n = \mathrm{mod}_{K'}(x)$ we have

$$R' \cap K = \{x \in K : \mathrm{mod}_{K'}(x) \leq 1\} = \{x \in K : \mathrm{mod}_K(x) \leq 1\} = R,$$

$$P' \cap K = \{x \in K : \mathrm{mod}_{K'}(x) < 1\} = \{x \in K : \mathrm{mod}_K(x) < 1\} = P.$$

Let ρ be the canonical mapping from R' onto R'/P', and consider the restriction $\rho|_R$. The kernel of this mapping is $R \cap P' = P$. Factoring out the kernel we obtain an isomorphism from k into k', and hence $q' = q^f$. For a prime element π of K we have

$$\frac{1}{q^{ef}} = \frac{1}{(q')^e} = \mathrm{mod}_{K'}(\pi) = \mathrm{mod}_K(\pi)^n = \frac{1}{q^n},$$

and therefore $n = ef$. □

1.6.3 Definition. With the notation of the previous Proposition the number e is called the order of ramification of K' over K, and f is called the modular degree of K' over K. If $e = 1$, then K' is said to be unramified, and if $f = 1$, then K' is said to be fully ramified.

1.6.4 Proposition. *Let K, K' be two p-fields such that K' is a fully ramified extension of K. If π' is a prime element in K', then $K' = K(\pi')$ and $R' = R[\pi']$.*

Proof. Let A be a full set of representatives of the the classes modulo P in R. By assumption we have

$$R'/P' \cong R/P = (R' \cap K)/(P \cap K),$$

and see that A is also a full set of representatives of the the classes modulo P' in R'. The subset

$$A' = \{\sum_{i=0}^{e-1} a_i(\pi')^i : a_0, \ldots, a_{e-1} \in A\}. \tag{1.6.1}$$

of R' makes up a full set of representatives of the the classes modulo $(P')^e$ in R'. This is an immediate consequence of Corollary 1.5.6.

If π is any prime element of K, then we have $e = \mathrm{ord}_{K'}(\pi)$ and by Corollary 1.5.6 every element of $(P')^{em}$ can be written in one and only one way in the form

$$\sum_{j=m}^{\infty} a'_j \pi^j,$$

with coefficients $a'_j \in A'$. In view of (1.6.1) every element of $(P')^{em}$ can be written in one and only one way in the form

$$\sum_{j=m}^{\infty}(\sum_{i=0}^{e-1} a_{ij}(\pi')^i)\pi^j = \sum_{i=0}^{e-1}(\sum_{j=m}^{\infty} a_{ij}\pi^j)(\pi')^i \tag{1.6.2}$$

with coefficients $a_{ij} \in A$. The inner sum represent elements in K. Thus any element from K' can be written as a linear combination of $1, \pi', \ldots, (\pi')^{e-1}$ with coefficients in K, which implies $K' = K(\pi')$. Applying (1.6.2) in the case $m = 0$ shows that any element from R' can be written as a linear combination of $1, \pi', \ldots, (\pi')^{e-1}$ with coefficients in R, i.e. $R' = R[\pi']$. □

1.6.5 Corollary. *Let K be a p-field of characteristic p. Call K^p the image of K under the mapping $x \mapsto x^p$. Then K is a fully ramified extension of K^p of degree p. If π is a prime element of K, then we have $K^p(\pi) = K$.*

Proof. As char $(K) = p$ the mapping $x \mapsto x^p$ is an algebraic isomorphism from K onto $K^p \subseteq K$. Since $\mathrm{mod}_K(x^p) = \mathrm{mod}_K(x)^p$, the mapping is bi-continuous, and, hence, K^p provided with the subspace topology is a locally compact Hausdorff topological field. By Proposition 1.4.19 the field K has finite dimension over K^p.

As K and K^p are isomorphic the corresponding fields $k(K)$ and $k(K^p)$ are isomorphic, too, and hence $f = 1$. The order e of ramification of K over K^p coincides therefore with the dimension of K over K^p. Moreover, for any prime element π of K its image π^p under the isomorphism $x \mapsto x^p$ is a prime element of K^p.

By Proposition 1.6.4 we have $K = K^p(\pi)$, and by the definition of e

$$\frac{1}{q^e} = \mathrm{mod}_K(\pi^p) = \mathrm{mod}_K(\pi)^p = \frac{1}{q^p}.$$

Thus $e = p = \dim_{K^p}(K)$. □

In the following we are going to deal with unramified extensions K' of a p-field K.

1.6.6 Proposition. *Let K be a p-field and let $K' = K(\epsilon_1, \ldots, \epsilon_n)$, where $\epsilon_1, \ldots, \epsilon_n$ are roots of 1 of order prime to p. Then K' is an unramified extensions of K. Moreover, with the notation of Proposition 1.6.2 restricting an automorphism α of K' over K to R' and factoring out P' induces an isomorphism*

$$\psi : G(K', K) \to G(k', k),$$

which satisfies $\rho' \circ \alpha = \psi(\alpha) \circ \rho',\ \alpha \in G(K', K)$. *In particular,* $G(K', K)$ *is a cyclic group* $\langle \alpha_0 \rangle$ *of order* f, *where* $\psi(\alpha_0)$ *is the automorphism* $x \mapsto x^q$ *and* f *is the modular degree of* K' *over* K. α_0 *is called the Frobenius automorphism of* K' *over* K.

Proof. As K' is a finite extension of K it can be provided with a uniquely determined topology such that it becomes a p-field (see Propositions 1.6.1 and 1.6.2). Because $\{\epsilon_1, \ldots, \epsilon_n\}$ is a subset of

$$(M')^\times = \{x \in K' : x^{q'-1} = 1\} = \{x \in K' : \exists n \in \mathbb{N} : p \not| n \text{ and } x^n = 1\},$$

(Theorem 1.5.8 applied to K') we have $K' = K((M')^\times)$. By Proposition 1.6.2 we have $R = K \cap R',\ P = K \cap P'$ and hence, we can think of k as a subfield of k' and have $\rho'|_R = \rho$, when ρ (ρ') denotes the canonical mapping from R (R') onto $k = R/P$ ($k' = R'/P'$).

If $\alpha \in G(K', K)$, then we know from Corollary 1.5.2 that $\alpha(R') = R'$ and $\alpha(P') = P'$. Thus

$$\psi(\alpha)(x + P') := \alpha(x) + P',\ x \in R',$$

is a well defined automorphism on k' such that $\rho' \circ \alpha = \psi(\alpha) \circ \rho'$. Moreover, as $\alpha(y) = y,\ y \in K$, we have $\psi(\alpha)|_k = \mathrm{id}_k$, i.e. $\psi(\alpha) \in G(k', k)$. It is elementary to check that ψ is a homomorphism.

If A' is a full set of representatives of cosets modulo P' in R', then $\alpha \in \ker(\psi)$ is the same as saying that $\alpha(a)$ and a belong to the same coset for all $a \in A'$. We apply this fact to $A' = M'$ and see in particular that for any $\mu \in M'$ the image $\alpha(\mu)$ does not coincide with any other element from M'.

But M' is just the set of all roots of the polynomial $X^{q'} - X$ in K' and therefore with $\mu \in M'$ we also have $\alpha(\mu) \in M'$. Together with the considerations in the previous paragraph we obtain $\alpha(\mu) = \mu$. As K' is generated by M' over K we have $\alpha = \mathrm{id}_{K'}$, and see that ψ is injective. In particular, $\#G(K', K) \leq \#G(k', k)$.

The field K' is the splitting field of the polynomial $X^{q'-1} - 1$ over K, and k' is the splitting field of the same polynomial over k. As $X^{q'-1} - 1$ is a separable polynomial we have $n = \dim_K(K') = \#G(K', K)$ and $f = \dim_k(k') = \#G(k', k)$. If e is the order of ramification of K' over K, then $n = ef$. On the other hand $n \leq f$. We conclude $e = 1,\ f = n$, and see that ψ is bijective.

Finally, it is well known that $G(k', k)$ is generated by $x \mapsto x^q$. Applying ψ^{-1} we are finished. □

1.6.7 Corollary. *If* K *is a* p *field, then a finite extension* K' *of* K *is an unramified extension if and only if* $K' = K(\epsilon_1, \ldots, \epsilon_n)$, *where* $\epsilon_1, \ldots, \epsilon_n$ *are roots of* 1 *of order prime to* p.

For any $f \in \mathbb{N}$ there exists one and only one (up to isomorphic copies) unramified extension of K of dimension f. This extension is generated by a primitive $(q^f - 1)$-th root of 1.

Proof. One direction of the 'if and only if' statement follows immediately from Proposition 1.6.6. So assume that K' is an unramified extension of K. Let μ be a generator of the multiplicative group $(M')^\times$. Then $\mathrm{ord}_{(M')^\times}(\mu) = q' - 1 = q^f - 1$ (see Theorem 1.5.8) and $K \subseteq K(\mu) \subseteq K'$. By assumption we have $f = \dim_K(K')$. On the other hand we have $M' \subseteq K(\mu)$. By Theorem 1.5.8 the modular degree of $K(\mu)$ over K is at least f. Thus $K(\mu) = K'$.

Now take any $f \in \mathbb{N}$, and let K' be the splitting field of $X^{q'-1} - 1$ where $q' = q^f$. Thus

$$K' = K(\{x \in K' : x^{q'-1} = 1\}).$$

Clearly, also $K' = K(\mu)$, if μ is a primitive $(q^f - 1)$-th root of 1. By Theorem 1.5.8 we have $\{x \in K' : x^{q'-1} = 1\} \subseteq (M')^\times$ and the modular degree $\tilde{f}$ of K' over K is at least f.

On the other hand by Proposition 1.6.6 K' is unramified and $G(K', K)$ is a cyclic group $\langle \alpha_0 \rangle$ of order $\tilde{f}$. But for our primitive $(q^f - 1)$-th root of 1, μ we have

$$\rho'(\alpha_0^f(\mu)) = \psi(\alpha_0)^f \rho'(\mu) = \rho'(\mu)^{q^f} = \rho'(\mu^{q^f}) = \rho'(\mu).$$

Since with μ also $y = \alpha_0^f(\mu)$ satisfies $y^{q'-1} = 1$ we have $\mu, \alpha_0^f(\mu) \in (M')^\times$. But on $(M')^\times$ ρ' is injective (see Theorem 1.5.8). Thus $\alpha_0^f(\mu) = \mu$. As $K' = K(\mu)$ we have $\alpha_0^f = \mathrm{id}_{K'}$, and hence $\tilde{f} = f$. □

1.6.8 Corollary. *If K is a p-field and K' a finite extension of modular degree f and order of ramification e over K, then there exists a unique maximal unramified extension L of K contained in K', such that* $\dim_K(L) = f$ *and* $\dim_L(K') = e$.

Proof. Take $L = K((M')^\times)$ and let $\mu \in (M')^\times$ be a primitive root of 1 of order $q' - 1 = q^f - 1$. Then $L = K(\mu)$. We just saw that $\dim_K(L) = f$, and as $ef = \dim_K(K') = \dim_K(L) \dim_L(K')$ we have $\dim_L(K') = e$.

Moreover, any unramified extension L' of K is generated by its roots $N^\times$ of 1 of order prime to p. These roots are clearly also roots of 1 of order prime to p in K', i.e. $N^\times \subseteq (M')^\times$ and $L' \subseteq L$. □

1.6.9 Proposition. *Let K be a p-field and K' a finite extension of K. Denoting by R and R' the maximal compact subrings of K and K', respectively, the ring R' is the set of all integral elements of K' over R.*

Proof. If $x \in K'$ is integral over R, then

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

with $a_1, \ldots, a_n \in R$. Then

$$1 = -a_1 x^{-1} - \cdots - a_n x^{-n}.$$

If we had $\mathrm{mod}_{K'}(x) > 1$, then this would imply the false statement $\mathrm{mod}_{K'}(1) < 1$.

Conversely, for $x \in R'$ denote by $f(X)$ the monic irreducible polynomial of x over K. Let L be the splitting field of $f(X)$ over K and L' be the splitting field of $f(X)$ over K'. Then all the fields are p-fields and

$$K \subseteq K' \subseteq L', \quad K \subseteq L \subseteq L',$$

where x is contained in K', L, L'. As $R' = R(L') \cap K'$ (Proposition 1.6.2) we have $x \in R(L')$, and as $R(L) = R(L') \cap L$ we obtain $x \in R(L)$. In L we have

$$f(X) = \prod_{i=1}^{m} (X - x_i),$$

where $x = x_1, x_2 \ldots x_m \in L$. Any root x_i of $f(X)$ in L can be obtained by applying an appropriate automorphism α_i from $G(L, K)$ to x. By Corollary 1.5.2 $\psi_i(x) \in R(L)$ and, hence, all the coefficients of $f(X)$ are contained in $R(L) \cap K = R$, i.e. x is integral over R. □

1.7 Global fields and their places

1.7.1 Definition. A field k is called a global field either if it is isomorphic to a finite extension of $\mathbb{Q}$ or if it is isomorphic to a finite extension of $\mathbb{F}_q(T)$, where $q = p^f$, $f \in \mathbb{N}$ for some prime p.

Global fields are interesting objects to study because of the fact that for any absolute value $|.|$ on them the completion with respect to $|.|$ is a locally compact field.

1.7.2 Definition. Given a global field k and considering all absolute values on k we call an equivalence class of non-trivial absolute values a place of k. Hereby two absolute values are called equivalent if they induce the same topology.

Recall from Proposition 1.1.3 that two absolute $|.|$ and $|.|'$ values are equivalent if and only if $|.|' = |.|^c$ for some $c > 0$ such that with $|.|$ also $|.|^c$ is an absolute value.

1.7.3 Proposition. *Let ν be a place of $\mathbb{Q}$. Then either ν is the place spanned by the classical absolute value $|.|_\infty$, or there exists exactly one prime number p such that ν is spanned by $|.|_p$. All the mentioned absolute values are not equivalent.*

Proof. The proof runs along the lines of Proposition 1.4.17. Let $|.| \in \nu$. According to Lemma 1.4.16 either $|n| \leq 1,\ n \in \mathbb{N}$ or $|n| = n^\delta,\ n \in \mathbb{N}$ and some $\delta > 0$.

In the second case it follows from the axioms AV1-AV3 that $|q| = |q|_\infty^\delta$. In particular, $\nu = [|.|_\infty]_\sim$.

In the first case we see from Proposition 1.1.5 that $|.|$ is non-archimedian. Let p be the smallest number in $\mathbb{N}$ such that $|p| < 1$. Let $c > 0$ be such that $|p| = p^{-c}$. By Lemma 1.1.4 p is a prime number and

$$p\mathbb{Z} = \{m \in \mathbb{Z} : |m| < 1\}.$$

We write any $q \in \mathbb{Q}^\times$ in the form

$$q = p^n \frac{s}{t},$$

where $n \in \mathbb{Z},\ s, t \in \mathbb{Z}, t > 0$ such that p, s, t are pairwise relatively prime. Then

$$|q| = |p|^n \frac{|s|}{|t|} = |p|^n = p^{-nc} = |q|_p^c,$$

and we see that $\nu = [|.|_p]_\sim$.

Finally we see from Proposition 1.1.3, the fact that $|.|_\infty$ is archimedian and $|.|_p$ not, and the fact that p is the smallest positive integer such that $|p|_p < 1$, that the absolute values $|.|_p,\ p \in \mathbb{P} \cup \{\infty\}$ are pairwise not equivalent. □

A similar result holds true for $\mathbb{F}_q(T)$.

1.7.4 Theorem. *Let ν be a place of $\mathbb{F}_q(T)$. Then either ν is the place spanned by the absolute value $|.|_\infty$ defined by*

$$\left|\frac{F(T)}{G(T)}\right|_\infty = q^{\deg(F)-\deg(G)},\ F, G \in \mathbb{F}_q[T],$$

or there exists a monic irreducible polynomial $P(T) \in \mathbb{F}_q[T]$ such that ν is spanned by $|.|_P$ (= $|.|_{P(T)}$ defined in (1.1.2)). All the mentioned absolute values are not equivalent.

Proof. Let $|.| \in \nu$. By Proposition 1.1.5 $|.|$ is non-archimedian. Moreover, $|n| = 1,\ n \in \mathbb{F}_q^\times$

Suppose first that $|T| \leq 1$. By AV2,AV4 we see that $|Q| \leq 1$ for all $Q \in \mathbb{F}_q[T]$. Moreover, there exists a polynomial $P \in \mathbb{F}_q[T]$ such that $|P| < 1$. For otherwise, we would have $|.| \equiv 1$.

By Lemma 1.1.4 we find a monic irreducible $P \in \mathbb{F}_q[T]$ such that

$$P(T)\mathbb{F}_q[T] = \{R(T) \in \mathbb{F}_q[T] : |R(T)| < 1\}.$$

Let $c > 0$ be such that $|P(T)| = q^{-c}$. If $f \in \mathbb{F}_q[T]^\times$, then write f uniquely in the form

$$f(T) = P(T)^n \frac{F(T)}{G(T)},$$

where $n \in \mathbb{Z}, F(T), G(T) \in \mathbb{F}_q[T]$ such that $P(T), F(T), G(T)$ are pairwise relatively prime. It follows

$$|f(T)| = |P(T)|^n = q^{-nc} = |f(T)|_P^c,$$

and hence $\nu = [|.|_P]_\sim$.

Now we come to the case that $|T| > 1$. Then

$$\left|\frac{1}{T}\right| < 1,$$

and by Proposition 1.1.6 we have for $a_0, \ldots, a_n \in \mathbb{F}_q$

$$|a_0 + a_1\frac{1}{T} + \cdots + a_n\frac{1}{T^n}| = 1,$$

whenever $a_0 \neq 0$. Thus for a polynomial $F(T) = b_nT^n + \cdots + b_0 \in \mathbb{F}_q[T]$, where $b_n \neq 0$

$$|F| = |T|^n|b_n + b_{n-1}\frac{1}{T} + \cdots + b_0\frac{1}{T^n}| = |T|^{\deg(F)}.$$

Letting $c > 0$ be such that $|T| = q^c$ it follows that for $f \in \mathbb{F}_q[T]$

$$|f| = |f|_\infty^c,$$

and hence $\nu = [|.|_\infty]_\sim$.

Finally by Proposition 1.1.3 $|.|_\infty$ is not equivalent to any of the absolute values $|.|_P$ because $|T|_\infty > 1$ and $|T|_P \leq 1$. Moreover, if $P(T) \neq Q(T)$ are irreducible and monic polynomials then $|P|_P < 1$ but $|P|_Q = 1$ which by Proposition 1.1.3 implies that $|.|_P \not\sim |.|_Q$. □

If k is a global field, ν is a place of k and $|.|, |.|' \in \nu$, then the completion of k with respect to $|.|$ is the same as that with respect to $|.|'$ because they induce the same metric on k.

1.7.5 Theorem. *Let k be $\mathbb{Q}$ or $\mathbb{F}_q(T)$. If ν is a place of k and $|.| \in \nu$, then the completion K of k with respect to $|.|$ is a locally compact field. If $k = \mathbb{Q}$, then $K \cong \mathbb{R}$ or $K \cong \mathbb{Q}_p$ for some prime $p \in \mathbb{P}$.*

In the case $k = \mathbb{F}_q(T)$ the completion K is isomorphic to some $\mathbb{F}_{q^f}((X))$. More detailed, if $|.|_P \in \nu$ then $f = \deg(P(T))$ and $\mathbb{F}_{q^f}((X)) \cong K$ via the mapping

$$\sum_{j=N}^{\infty} a_j X^j \mapsto \sum_{j=N}^{\infty} a_j P(T)^j, \quad a_j \in \mathbb{F}_{q^f},$$

where we identify $\mathbb{F}_{q^f}$ with $M(K)$ (see Corollary 1.5.9). If $|.|_\infty \in \nu$ then $\mathbb{F}_q((X)) \cong K$ via the mapping

$$\sum_{j=N}^{\infty} a_j X^j \mapsto \sum_{j=N}^{\infty} a_j T^{-j}, \quad a_j \in \mathbb{F}_{q^f}.$$

Proof. If $k = \mathbb{Q}$, then by Proposition 1.7.3 $|.| \sim |.|_p$ for some $p \in \mathbb{P} \cup \{\infty\}$, and hence $K \cong \mathbb{Q}_p$ (in the case $p \in \mathbb{P}$) or $K \cong \mathbb{R}$.

If $k = \mathbb{F}_q(T)$, then by Theorem 1.7.4 $|.| \sim |.|_P$ for some irreducible $P(T) \in \mathbb{F}_q[T]$ or $|.| \sim |.|_\infty$. In the first case assume that $P(T) = T$. Then we already saw in Section 1.2 that K is isomorphic to $\mathbb{F}_q((T))$.

If $P(T)$ is not T, then consider $\mathbb{F}_q(X)$ and the embedding

$$\iota : \mathbb{F}_q(X) \to \mathbb{F}_q(T), \quad Q(X) \mapsto Q(P(T)).$$

Clearly, $\mathbb{F}_q(T)$ is a field extension of $\iota(\mathbb{F}_q(X))$ of finite degree $d \leq \deg P = f$. In fact, T is a zero of the polynomial $P(Y) - P(T) \in \iota(\mathbb{F}_q(X))[Y]$. Thus $1, T, \ldots, T^{f-1}$ is a generating system of $\mathbb{F}_q(T)$ over $\iota(\mathbb{F}_q(X))$.

Moreover, $|.|_P$ restricted to $\iota(\mathbb{F}_q(X))$ coincides with $|\iota^{-1}(.)|_X$. Thus we can extend ι to an embedding of the the completion $\mathbb{F}_q((X))$ of $\mathbb{F}_q(X)$ into the completion K of $\mathbb{F}_q(T)$ with respect to $|.|_P$. Clearly, this extension is also a field embedding, i.e. it respects the field operations. Note also that K is a topological vector space over $\iota(\mathbb{F}_q((X)))$.

We claim that K is the span of $1, T, \ldots, T^{f-1}$ over $\iota(\mathbb{F}_q((X)))$. In fact, this span is a finite dimensional vector space V over $\iota(\mathbb{F}_q((X)))$ contained in K. The topology from K induces on V a topological vector space topology. By Proposition 1.2.5 this topology is uniquely determined and coincides with the product topology induced by $\iota(\mathbb{F}_q((X)))$ on V. Moreover, V is complete with respect to this topology. On the other hand V contains $\mathbb{F}_q(T)$, and

hence $K = V$ and the dimension of K over $\iota(\mathbb{F}_q((X)))$ is at most f. Since $\mathbb{F}_q((X))$ is locally compact, we proved now that K is a p-field extension of the p-field $\iota(\mathbb{F}_q((X)))$.

Since mod_K is a continuous mapping from $K^\times$ onto $\Gamma = \mathrm{mod}_K(K^\times)$ and since $\mathbb{F}_q(T)$ is dense in K, we obtain $\Gamma = \mathrm{mod}_K(\mathbb{F}_q(T)^\times)$. In particular, we find prime elements of K in $\mathbb{F}_q(T)^\times$, and all these elements are the x in $\mathbb{F}_q(T)^\times$ such that $\mathrm{mod}_K(x) < 1$ and $\mathrm{mod}_K(x)$ is maximal with respect to the property $\mathrm{mod}_K(x) < 1$. As $|.|_P$ and mod_K induce the same topology on K we can replace mod_K by $|.|_P$ in the previous sentence. By the definition of $|.|_P$ we see that $P(T)$ is a prime element of K.

We calculate the modular degree of K over $\iota(\mathbb{F}_q((X)))$. All polynomials $Q(T) \in \mathbb{F}_q[T],\ \deg(Q(T)) < f$ are contained in different cosets module $P(T)$. In fact, $|Q(T)|_P = 1$ and $|Q(T) - R(T)|_P = 1$ for $Q(T) \neq R(T) \in \mathbb{F}_q[T],\ \deg(Q(T)), \deg(R(T)) < f$. Thus $k(K)$ has at least q^f elements, and hence the modular degree of K over $\iota(\mathbb{F}_q((X)))$ is at least f. But as the dimension of K over $\iota(\mathbb{F}_q((X)))$ is at most f Proposition 1.6.2 yields

$$\dim_{\iota(\mathbb{F}_q((X)))}(K) = f,$$

the modular degree is f and the ramification index is one, i.e. K is an unramified extension. By Corollary 1.5.10 $K \cong \mathbb{F}_{q^f}((X))$ by representing each $x \in K$ as a series

$$\sum_{j=N}^{\infty} a_j P(T)^j, \quad a_j \in M(K) \cong \mathbb{F}_{q^f}.$$

Note that by the form of ι an $x \in K$ lies in $\iota(\mathbb{F}_q((X)))$ if and only if $a_j \in \mathbb{F}_q$ for all $j \in \mathbb{Z}$.

Finally we come to the case that $|.| \sim |.|_\infty$ on k. By setting $X = \frac{1}{T}$ and by writing every $f(T) \in \mathbb{F}_q(T)$ as

$$f(T) = \frac{a_0 + \cdots + a_n T^n}{b_0 + \cdots + b_m T^m} = \frac{a_0 T^{-l} + \cdots + a_n T^{n-l}}{b_0 T^{-l} + \cdots + b_m T^{m-l}}, \quad l = \max(m, n)$$

we get an isomorphism from $\mathbb{F}_q(T)$ onto $\mathbb{F}_q(X)$. Hereby $|.|_\infty$ corresponds $|.|_X$. So we see that by mapping T^{-1} to X the completion of $\mathbb{F}_q(T)$ with respect to $|.|_\infty$ is isomorphic to $\mathbb{F}_q((X))$. □

1.7.6 Remark. Let k, k' be global fields such that $k \subseteq k'$, and let ν' be a place of k' with $|.| \in \nu'$. Then $|.||_k$ is a non-trivial absolute value.

In fact, if $|.|$ is archimedian on k', then k and k' are both extensions of $\mathbb{Q}$ (see Proposition 1.1.5). If $|.|$ were trivial on k, it would be so on $\mathbb{Q}$. By Proposition 1.1.5 $|.|$ would be non-archimedian on k'.

If $|.|$ is non-archimedian on k', take $x \in k' \setminus k$ with $|x| > 1$. As k' is an algebraic extension of k

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

for some $a_0, \ldots, a_{n-1} \in k$. If we had $|a_j| = 1$ for all j with $a_j \neq 0$, then by Proposition 1.1.6 we would get the contradiction $|0| = |x|^n \neq 0$.

We are now sure to be able to restrict a place ν' on a global field k' to a smaller global field k. In fact, take $|.| \in \nu'$. By what we just saw $|.||_k$ is non-trivial on k. It therefore spans a place ν on k. Clearly, ν does not depend on the chosen $|.|$ on ν'. It is determined only by ν'.

1.7.7 Definition. Let k, k' be two global fields such that k is a subfield of k'. If ν is a place on k and ν' is a place on k', then we say that ν' lies over ν ($\nu'|\nu$) if $|.| \in \nu'$ implies $|.||_k \in \nu$.

1.7.8 Definition. Let k be a global field. A place ν on k is called infinite, if ν lies over $[|.|_\infty]_\sim$. In all other cases ν is called finite on k.

1.7.9 Remark. From Proposition 1.1.5 we see in the case $\mathbb{Q} \subseteq k$ that ν is finite on k if and only if one and hence all $|.| \in \nu$ are non-archimedian.

1.7.10 Corollary. *Let k be a global field and let ν be a place of k. Take any $|.| \in \nu$. Then the completion K of k with respect to $|.|$ is a locally compact topological field.*

Proof. By definition k is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_q(T)$. Let $x_1, \ldots, x_n$ be a basis. $|.|$ restricted to $\mathbb{Q}$ or $\mathbb{F}_q(T)$, respectively, is an absolute value. The completion L of the smaller field can therefore be seen as a closed subfield of K. As in the previous proof we show that K coincides with the span V of $x_1, \ldots, x_n$ over L. In fact, with the topology induced on V by $|.|$ the vector space V is a topological vector space of finite dimension over L. By Proposition 1.2.5 V is complete and, clearly, contains k. Thus it is already the whole space K.

From Theorem 1.7.5 we know that L is locally compact. By Proposition 1.6.1 we then also obtain that K is locally compact. □

1.7.11 Remark. If k is a global field and K is its completion with respect to some finite place ν or infinite in the case of non-zero characteristic, then by Lemma 1.4.14 $\mathrm{mod}_K(K^\times)$ is a discrete subgroup of $(\mathbb{R}_+^\times, \cdot)$. Therefore the range of $|.| \in \nu$ is also discrete.

Note that we did not yet treat the existence of of absolute values on an arbitrary global field.

1.7.12 Proposition. *Let k, k' be two global fields with $k \subseteq k'$, and let ν be a place of k. Then there exist a place ν' of k' with $\nu'|\nu$. There are only finitely many places ν' of k' lying above k.*

If K' is the completion of k' with respect to some $\nu'|\nu$, then K' is a finite extension of K.

Proof. By assumption $k' = k(x_1, \ldots, x_n)$ where the x_j's are algebraic over k. Let F be an algebraic closure of K. Clearly, F is also algebraicly closed and therefore contains the algebraic closure f of k. Thus there exists at least one isomorphism α from k' onto $\alpha(k') \subseteq F$ with $\alpha|_k = \mathrm{id}_k$.

Set $K_\alpha = K(\alpha(x_1), \ldots, \alpha(x_n))$ and note that this is then a finite extension of K. By Corollary 1.7.10 K is locally compact and, hence, we see from Proposition 1.6.1 that K_α carries a unique topology such that it becomes a topological field over the topological field K. This topology is locally compact and, therefore, complete. By Corollary 1.4.12 a proper power of the modular function is an absolue value $|.|$ inducing this locally compact topology. We conclude that $|.||_k \in \nu$ and, therefore, $|\alpha(.)|$ induces a place ν' on k' with $\nu'|\nu$. The completion of k' with respect to $|\alpha(.)|$ is a locally compact field K', which is isomorphic (algebraically and topologically) to K_α via an isomorphism which continues α. We denote this continuation also by α. As α is continuous and as $\alpha|_k = \mathrm{id}_k$ we have $\alpha_K = \mathrm{id}_K$.

Conversely, let $\nu'|\nu$ be a place on k'. The argumentation in the proof of Corollary 1.7.10 shows that the completion K' of k' with respect to ν' satisfies $K' = K(x_1, \ldots, x_n)$, and is therefore a finite algebraic extension of K. It follows that there exists an isomorphism α from K' onto $\alpha(K') \subseteq F$ with $\alpha|_K = \mathrm{id}_K$ and $\alpha(K') = K(\alpha(x_1), \ldots, \alpha(x_n))$. $\alpha|_{k'}$ is an isomorphism from k' onto $\alpha(k') \subseteq f$ whose restriction to k is the identity. Thus $\alpha(K')$ coincides with K_α constructed in the previous paragraph, and $\alpha : K' \to K_\alpha$ is an isomorphism also in the topological sense because it is linear over the field K.

If two places ν', ν'' over ν induce the isomorphisms $\alpha' : K' \to \alpha'(K')$ and $\alpha'' : K'' \to \alpha''(K'')$, and if $\alpha'|_{k'} = \alpha''|_{k'}$, then the fact that $\alpha'|_K = id_K = \alpha''|_K$ yields that

$$K_{\alpha'} = K(\alpha'(x_1), \ldots, \alpha'(x_n)) = K(\alpha''(x_1), \ldots, \alpha''(x_n)) = K_{\alpha''}.$$

Let $|.|' \in \nu'$, $|.|'' \in \nu''$, and denote the continuation of these absolute values to K' and K'' also by $|.|'$ and $|.|''$, respectively.

We conclude that $(\alpha'')^{-1} \circ \alpha'$ is a K-linear field isomorphism from K' onto K''. It is therefore bi-continuous with respect to $|.|'$ and $|.|''$. Since the restriction of this isomorphism to k' is the identity, we obtain $|.|' \sim |.|''$, i.e. $\nu' = \nu''$.

Thus we showed that there are as many places ν' over ν as there are isomorphism α from k' into F such that $\alpha|_k = \mathrm{id}_k$. This number is bounded by the dimension of k' over k. □

1.7.13 Corollary. *Let k be a global field and let $x \in k$ be a fixed element. Then for all but finitely many (almost all) places ν of k, $|.| \in \nu$ implies $|x| = 1$.*

Proof. If $k = \mathbb{Q}$, the assertion is clear since we can write $x \in \mathbb{Q}$ as $\frac{a}{b}$, $a \in \mathbb{Z}, b \in \mathbb{N}$ where a and b are relatively prime. Thus $|x|_p = 1$ for all prime numbers p except those which divide a or b. These are only finitely many. By Proposition 1.7.3 this implies the assertion for $k = \mathbb{Q}$.

Almost the same kind of argumentation applies to $k = \mathbb{F}_q(T)$. We just cite Theorem 1.7.4 instead of Proposition 1.7.3.

For a finite extension k of $\mathbb{Q}$ or $\mathbb{F}_q(T)$, respectively, the element x satisfies the equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

with coefficients $a_0, \ldots, a_{n-1} \in \mathbb{Q}$, $a_0 \neq 0$ ($\mathbb{F}_q(T)$). For j with $a_j \neq 0$ let $\mathcal{P}_j$ be the (finite) set of all finite places of $\mathbb{Q}$ ($\mathbb{F}_q(T)$) such that $|a_j| \neq 1$ for $|.| \in \nu \in \mathcal{P}_j$. Let $\mathcal{Q}$ be the set of all places of k such that for $|.| \in \nu$ we have $|.||_{\mathbb{Q}} \in \mathcal{P}_j$ for some j with $a_j \neq 0$. By Proposition 1.7.12 $\mathcal{Q}$ is finite.

If for $\nu \notin \mathcal{Q}$ and $|.| \in \nu$ we had $|x| > 1$, then by Proposition 1.1.6 we get the contradiction

$$|0| = |x^n + a_{n-1}x^{n-1} + \cdots + a_0| = |x^n| > 1,$$

In the case $|x| < 1$ we would get

$$|0| = |1 + a_{n-1}x^{-1} + \cdots + a_0x^{-n}| = |x^{-n}| > 1.$$

□

1.8 Valuations

First we are going to define a generalisation of the concept of non-archimedian absolute value.

1.8.1 Definition. Let Γ be an abelian group (written multiplicatively). Γ is called an ordering if there exists $S \subseteq \Gamma$, which is closed under multiplication, such that

$$\Gamma = S \dot\cup \{1\} \dot\cup S^{-1}.$$

For $\alpha, \beta \in \Gamma$ we write $\alpha < \beta$ if $\alpha\beta^{-1} \in S$. We shall write $\alpha \leq \beta$ if $\alpha < \beta$ or $\alpha = \beta$.

1.8.2 Remark. It is elementary to verify the following properties.

1. For $\alpha, \beta \in \Gamma$ we have $\alpha < \beta$, $a = b$, or $\alpha > \beta$, and these possibilities are mutually exclusive.
2. $\alpha < \beta$ implies $\alpha\gamma < \beta\gamma$ for any $\gamma \in \Gamma$.
3. $\alpha < \beta$ and $\beta < \gamma$ implies $\alpha < \gamma$.

We already saw that the range Γ of an absolute value is an ordered group. In fact, these ranges are subgroups of the ordered group $(\mathbb{R}_+^\times, \cdot)$

1.8.3 Definition. Let K be a field, Γ be an ordered group, $(0 \notin \Gamma)$. A mapping

$$v : \begin{cases} K & \to & \Gamma \cup \{0\} \\ x & \mapsto & v(x) \end{cases}$$

is called valuation on K (with range $v(K \setminus \{0\}) \subseteq \Gamma$) if

1. $v(x) = 0 \iff x = 0$
2. $v(xy) = v(x) \cdot v(y)$
3. $v(x + y) \leq \max\{v(x), v(y)\}$.

The valuation is called discrete, if $v(K^\times) = \{1\}$.

Clearly, non-archimedian absolute values $|.|$ are valuations with range contained in $(\mathbb{R}_+^\times, \cdot)$.

1.8.4 Definition. Let K be a field, R be a subring of K. Then R is called a valuation ring if

$$\forall x \in K : (x \in R \vee x^{-1} \in R).$$

1.8.5 Remark. It is straight forward to verify that for a valuations $v : K \to \Gamma \cup \{0\}$ the subset

$$R_v := v^{-1}(S \cup \{1\}) = \{x \in K : v(x) \leq 1\}$$

is a valuation ring.

We are going to show that, conversely, every valuation ring gives rise to a valuation.

1.8.6 Proposition. *Let K be a field, and let $R \subseteq K$ be a valuation ring. Then there exists a valuation v on K with $R = R_v$. The ring R_v has a unique maximal ideal $\mathfrak{m} = \{x \in K : v(x) < 1\}$ und $R_v^\times = \{x \in K : v(x) = 1\}$.*

v is non-trivial if and only if $R_v \neq K$.

Proof. Let R be a valuation ring. We are going to show that R has a unique maximal ideal (see Lemma 1.1.4). Let $U = R^\times$ be the group of units in R. It is sufficient to show that $R \setminus U$ is an ideal of R, because any non-trivial ideal I of R is contained in $R \setminus U$.

So let $x, y \in R \setminus U$ and assume for example that $\frac{x}{y} \in R$. Then

$$1 + \frac{x}{y} = (x + y)\frac{1}{y} \in R.$$

If we had $x + y \in U$, then in contradiction to the assumption $y \in R \setminus U$ also y would be contained in U. If with the assumption $x \in R \setminus U, z \in R$ we had $zx \in U$, then $(zx)b = 1$ for some $b \in R$, and hence the contradiction $x \in U$.

Let $\mathfrak{m}$ be the maximal ideal of R, then $R = U \dot\cup \mathfrak{m}$ and hence ($\mathfrak{m}^\times = \mathfrak{m} \setminus \{0\}$)

$$K^\times = \mathfrak{m}^\times \dot\cup U \dot\cup (\mathfrak{m}^\times)^{-1},$$

As $\mathfrak{m}^\times$ is closed under multiplication

$$\Gamma = K^\times / U$$

is an ordered group ($xU < U \iff x \in \mathfrak{m}^\times$). For $x \in K^\times$ set $v(x) := xU \in \Gamma$, and for $x = 0$ set $v(x) = 0$.

v clearly satisfies the first two axioms for valuations. Let $x, y \in K^\times$ with e.g. $\frac{x}{y} \in R = \mathfrak{m}^\times \dot\cup U$. Then $v(x)v(y)^{-1} \leq U$.

From $1 + \frac{x}{y} \in R$ we conclude $v(1 + \frac{x}{y}) \leq U$. Because of $1 + \frac{x}{y} = (x + y)\frac{1}{y}$ it follows that $v(x + y)v(y)^{-1} \leq U$, and therefore $v(x + y) \leq v(y)$.

Clearly, if v is a valuation the maximal ideal of R_v is $R_v \setminus R_v^\times$, i.e. it is given by $\{x \in K : v(x) < 1\}$.

The final statement is obvious. □

1.8.7 Proposition. *With the above notation let v map $K^\times$ surjectively onto Γ. Then Γ is cyclic ($\Gamma = \langle\gamma\rangle$) if and only if the unique maximal ideal $\mathfrak{m}$ of R_v is of the form yR_v for some $y \in R_v$ and*

$$\cap_{n\in\mathbb{N}} \mathfrak{m}^n = \{0\}. \tag{1.8.1}$$

In this case $v(x) = v(y)^n$, where $n \in \mathbb{Z}$ such that $x \in y^n R_v$, but $x \notin y^{n+1} R_v$.

Proof. If $\Gamma = \langle\gamma\rangle$ with $\gamma < 1$ and $y \in R_v$ with $v(y) = \gamma$, then $v(x) < 1$ if and only if $v(x) = \gamma^n$ for some $n \in \mathbb{N}$. This in turn is the case if and only if $x = uy$ for some $u \in K$ with $u \in R$. Hence

$$\{x \in K : v(x) < 1\} = yR. \tag{1.8.2}$$

We conclude

$$\mathfrak{m}^n = y^n R = \{x \in K : v(x) \leq \gamma^n\}, \tag{1.8.3}$$

and see that (1.8.1) must hold true.

Conversely, if we assume (1.8.2), then

$$\{x \in K : v(x) < 1\} = \{x \in K : v(x) \leq v(y)\}.$$

We set $\gamma = v(y)$. It is straight forward to see that the relation (1.8.3) holds true. By (1.8.1) we find for an arbitrary $x \in R$ an $n \in \mathbb{N}$ such that $x \in y^{n-1}R_v$ but $x \notin y^n R_v$. Thus $v(x) \leq \gamma^{n-1}$ and $v(x) > \gamma^n$. If we had $v(x) < \gamma^{n-1}$, then it would follow that $xy^{-n+1} \in \mathfrak{m}$ and by (1.8.3) $v(xy^{-n+1}) \leq \gamma$. This contradicts $v(x) > \gamma^n$, and we proved the final assertion of the present proposition for $x \in R_v$. As for $x \in K^\times$ we have $x \in R_v$ or $x^{-1} \in R_v$ we conclude that $\Gamma = v(K^\times) = \langle\gamma\rangle$ is cyclic.

Finally, it is elementary to see that the second equality in (1.8.3) holds true for all $n \in \mathbb{Z}$. This immediately yields the final assertion of the current Proposition. □

1.8.8 Lemma. *Let K be a field, and let $|.|$ and $|.|'$ be two non-archimedian absolute values on K. Then $|.| \sim |.|'$ if and only if $R_{|.|} = R_{|.|'}$.*

In particular, for a global field the ring $R_{|.|}$ just depends on the place such that $|.| \in \nu$ ($R_\nu := R_{|.|}$), and different places ν induce different rings R_ν.

Proof. If $|.| \sim |.|'$, then $|x| \leq 1$ if and only if $|x|' \leq 1$.

Conversely, if $R_{|.|} = R_{|.|'}$, then the unique maximal ideal is given by $\{x \in K : |x| < 1\} = \{x \in K : |x|' < 1\}$ (see Lemma 1.1.4). From Proposition 1.1.3 we obtain $|.| \sim |.|'$. □

1.8.9 Proposition. *Let L be a finite extension of the field K of degree n. Let w be a valuation of L with range $\Gamma' \cup \{0\} = w(L)$. Setting $\Gamma = w(K^\times)$ we have*

$$(\Gamma' : \Gamma) \leq n.$$

Proof. Let $y_1, \ldots, y_r \in L^\times$ such that

$$w(y_i)\Gamma \neq w(y_j)\Gamma, \quad i \neq j.$$

We shall prove that $y_1, \ldots, y_r \in L$ are linearly independent over K, and hence $n \geq r$.

If we had $a_1y_1 + \cdots + a_ry_r = 0$ for some $a_1, \ldots, a_r \in K$ and $a_j \neq 0$ for some j. If the elements $w(a_jy_j) \neq 0$ in Γ were pairwise different, then the same argumentation which proves Proposition 1.1.6 would yield

$$w(0) = w(a_1y_1 + \cdots + a_ry_r) = \max\{w(a_jy_j) : j = 1, \ldots, n\} \neq 0.$$

Thus there exist $i \neq j$ such that $w(a_i y_i) = w(a_j y_j)$, and hence

$$w(y_i) = w(a_i^{-1} a_j) w(y_j).$$

But this contradicts $w(y_i)\Gamma \neq w(y_j)\Gamma$. □

1.8.10 Lemma. *Let Γ be a subgroup of the ordered group Γ'. If Γ is cyclic and if $(\Gamma' : \Gamma) = n$ is finite, then Γ' is cyclic, too. If $\Gamma' = \langle\gamma\rangle$ then $\langle\gamma^n\rangle$.*

Proof. As Γ' is ordered the homomorphism $\alpha \mapsto \alpha^n$ is injective. By assumption $(\Gamma')^n \subseteq \Gamma$. With Γ also its subgroup $(\Gamma')^n$ is cyclic. As $(\Gamma')^n$ is isomorphic to Γ' the same is true for Γ'. If γ is a generator of Γ', then clearly γ^n is a generator of Γ. □

1.8.11 Corollary. *Let ν be a finite place on a global field k. Let k' be a finite field extension of k. Then the places ν' of k' lying over ν correspond bijectively via the relation*

$$R' = R_{\nu'}$$

to the set of all valuation rings R' of k' such that $R_\nu = R' \cap k$.

Proof. If $\nu' | \nu$, then, clearly, $R_\nu = R_{\nu'} \cap k$. By Lemma 1.8.8 two different places induce two different valuation rings.

If R' be a valuation ring such that $R_\nu = R' \cap k$, then $R' = R_w$ for some valuation $w : k' \to \Gamma' \cup \{0\}$ (see Proposition 1.8.6). By Proposition 1.8.9 $(\Gamma' : w(k^\times)) < \infty$.

On the other hand by Remark 1.7.11 $|k^\times|$ is a discrete subgroup of $(\mathbb{R}_+^\times, \cdot)$. Hence it is cyclic, i.e. it is generated by some $c \in (0,1)$. By Proposition 1.8.7 also $w(k^\times) = \langle\delta\rangle,\ \delta < 1$ is cyclic, and $w(x) = \delta^n$ if and only if $|x| = c^n$.

We learn from Lemma 1.8.10 that then Γ' is cyclic, too. If $\Gamma' = \langle\gamma\rangle$, $\gamma < 1$, then $\gamma^{(\Gamma' : w(k^\times))} = \delta$. Let $d \in (0,1)$ be such that $d^{(\Gamma' : w(k^\times))} = c$. It is now clear that $\gamma \mapsto d$ induces an isomorphism ϕ from Γ' onto $\langle d\rangle$ such that $\phi \circ w$ is a non-archimedian absolute value on k' which continues $|.|$. It spans a place ν' such that $R_{\nu'} = R'$. □