Chapter 6

Valuations

In this chapter, we generalize the notion of absolute value. In particular, we will show how the p-adic absolute value defined in the previous chapter for $\mathbb{Q}$ can be extended to hold for number fields. We introduce the notion of archimedean and non-archimedean places, which we will show yield respectively infinite and finite places. We will characterize infinite and finite places for number fields, and show that they are very well known: infinite places correspond to the embeddings of the number field into $\mathbb{C}$ while finite places are given by prime ideals of the ring of integers.

6.1 Definitions

Let K be a field.

Definition 6.1. An absolute value on K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ which satisfies

- $|\alpha| = 0$ if and only if $\alpha = 0$,
- $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in K$
- there exists $a > 0$ such that $|\alpha + \beta|^a \leq |\alpha|^a + |\beta|^a$.

We suppose that the absolute value $|\cdot|$ is not trivial, that is, there exists $\alpha \in K$ with $|\alpha| \neq 0$ and $|\alpha| \neq 1$.

Note that when $a = 1$ in the last condition, we say that $|\cdot|$ satisfies the triangle inequality.

Example 6.1. The p-adic absolute valuation $|\cdot|_p$ of the previous chapter, defined by $|\alpha|_p = p^{-\mathrm{ord}_p(\alpha)}$ satisfies the triangle inequality.

Definition 6.2. Two absolute values are equivalent if there exists a $c > 0$ such that $|\alpha|_1 = (|\alpha|_2)^c$. An equivalence class of absolute value is called a place of K.

Example 6.2. Ostrowski's theorem, due to the mathematician Alexander Ostrowski, states that any non-trivial absolute value on the rational numbers $\mathbb{Q}$ is equivalent to either the usual real absolute value ($|\cdot|$) or a p-adic absolute value ($|\cdot|_p$). Since $|\cdot| = |\cdot|_\infty$, we have that the places of $\mathbb{Q}$ are $|\cdot|_p$, $p \leq \infty$. By analogy we also call $p \leq \infty$ places of $\mathbb{Q}$.

Note that any valuation makes K into a metric space with metric given by $d(x_1, x_2) = |x_1 - x_2|^a$. This metric does depend on a, however the induced topology only depends on the place. This is what the above definition really means: two absolute values on a field K are equivalent if they define the same topology on K, or again in other words, that every set that is open with respect to one topology is also open with respect to the other (recall that by open set, we just mean that if an element belongs to the set, then it also belongs to an open ball that is contained in the open set).

Lemma 6.1. *Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on a field K. The following statements are equivalent:*

1. *$|\cdot|_1$ and $|\cdot|_2$ define the same topology;*
2. *for any $\alpha \in K$, we have $|\alpha|_1 < 1$ if and only if $|\alpha|_2 < 1$;*
3. *$|\cdot|_1$ and $|\cdot|_2$ are equivalent, that is, there exists a positive real $c > 0$ such that $|\alpha|_1 = (|\alpha|_2)^c$.*

Proof. We prove 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 1.

(1. $\Rightarrow$ 2.) If $|\cdot|_1$ and $|\cdot|_2$ define the same topology, then any sequence that converges with respect to one absolute value must also converge in the other. But given any $\alpha \in K$, we have that

$$\lim_{n\to\infty} \alpha^n = 0 \iff \lim_{n\to\infty} |\alpha^n| = 0$$

with respect to the topology induced by an absolute value $|\cdot|$ (may it be $|\cdot|_1$ or $|\cdot|_2$) if and only if $|\alpha| < 1$. This gives 2.

(2. $\Rightarrow$ 3.) Since $|\cdot|_1$ is not trivial, there exists an element $x_0 \in K$ such that $|x_0|_1 < 1$. Let us set $c > 0$, $c \in \mathbb{R}$, such that

$$|x_0|_1^c = |x_0|_2.$$

We can always do that for a given x_0, the problem is now to see that this holds for any $x \in K$. Let $0 \neq x \in K$. We can assume that $|x|_1 < 1$ (otherwise just replace x by $1/x$). We now set $\lambda \in \mathbb{R}$ such that

$$|x|_1 = |x_0|_1^\lambda.$$

Again this is possible for given x and x_0. We can now combine that

$$|x|_1 = |x_0|_1^\lambda \Rightarrow |x|_1^c = |x_0|_1^{c\lambda}$$

with
$$|x_0|_1^c = |x_0|_2 \Rightarrow |x_0|_1^{c\lambda} = |x_0|_2^\lambda$$
to get that
$$|x|_1^c = |x_0|_1^{c\lambda} = |x_0|_2^\lambda.$$
We are left to connect $|x_0|_2^\lambda$ with $|x|_2$.

If $m/n > \lambda$, with $m, n \in \mathbb{Z}$, $n > 0$, then
$$\left|\frac{x_0^m}{x^n}\right|_1 = |x_0^{m-\lambda n}|_1 \left|\frac{x_0^{\lambda n}}{x^n}\right|_1 = |x_0|_1^{m-\lambda n} < 1.$$
Thus, by assumption from 2.,
$$\left|\frac{x_0^m}{x^n}\right|_2 < 1$$
that is
$$|x|_2 > |x_0|_2^{m/n} \text{ for all } \frac{m}{n} > \lambda,$$
or in other words,
$$|x|_2 > |x_0|_2^{\lambda+\beta},\ \beta > 0 \Rightarrow |x|_2 \geq |x_0|_2^\lambda.$$
Similarly, if $m/n < \lambda$, we get that $|x|_2 < |x_0|_2^{m/n} \Rightarrow |x|_2 \leq |x_0|_2^\lambda$. Thus
$$|x|_2 = |x_0|_2^\lambda = |x_0|_1^{c\lambda} = |x|_1^c$$
for all $x \in K$.

(3. $\Rightarrow$ 1.) If we assume 3., we get that
$$|\alpha - a|_1 < r \iff |\alpha - a|_2^c < r \iff |\alpha - a|_2 < r^{1/c},$$
so that any open ball with respect to $|\cdot|_1$ is also an open ball (albeit of different radius) with respect to $|\cdot|_2$. This is enough to show that the topologies defined by the two absolute values are identical. Note that having balls of different radius tells us that the metrics are different. □

6.2 Archimedean places

Let K be a number field.

Definition 6.3. An absolute value on a number field K is archimedean if for all $n > 1$, $n \in \mathbb{N}$, we have $|n| > 1$.

The story goes that since for an Archimedean valuation, we have $|m|$ tends to infinity with m, the terminology recalls the book that Archimedes wrote, called "On Large Numbers".

Proposition 6.2. *The only archimedean place of $\mathbb{Q}$ is the place of the real absolute value $|\cdot|_\infty$.*

Proof. Let $|\cdot|$ be an archimedean absolute value on $\mathbb{Q}$. We can assume that the triangle inequality holds (otherwise, we replace $|\cdot|$ by $|\cdot|^a$). We have to prove that there exists a constant $c > 0$ such that $|x| = |x|_\infty^c$ for all $x \in \mathbb{Q}$. Let us first start by proving that this is true for positive integers.

Let $m, n > 1$ be integers. We write m in base n:

$$m = a_0 + a_1 n + a_2 n^2 + \ldots + a_r n^r,\ 0 \le a_i < n.$$

In particular, $m \ge n^r$, and thus

$$r \le \frac{\log m}{\log n}.$$

Thus, we can upper bound $|m|$ as follows:

$$\begin{aligned} |m| &\le |a_0| + |a_1||n| + \ldots + |a_r||n|^r \\ &\le (|a_0| + |a_1| + \ldots + |a_r|)|n|^r \text{ since } |n| > 1 \\ &\le (1+r)|n|^{r+1} \\ &\le \left(1 + \frac{\log m}{\log n}\right)|n|^{\frac{\log m}{\log n}+1}. \end{aligned}$$

Note that the second inequality is not true for example for the p-adic absolute value! We can do similarly for m^k, noticing that the last term is of order at most n^{rk}. Thus

$$|m|^k \le \left(1 + \frac{k\log m}{\log n}\right)|n|^{\frac{k\log m}{\log n}+1},$$

and

$$|m| \le \left(1 + \frac{k\log m}{\log n}\right)^{1/k}|n|^{\frac{\log m}{\log n}+1/k}.$$

If we take the limit when $k \to \infty$ (recall that $\sqrt[n]{n} \to 1$ when $n \to \infty$), we find that

$$|m| \le |n|^{\frac{\log m}{\log n}}.$$

If we exchange the role of m and n, we find that

$$|n| \le |m|^{\frac{\log n}{\log m}}.$$

Thus combining the two above inequalities, we conclude that

$$|n|^{1/\log n} = |m|^{1/\log m}$$

which is a constant, say e^c. We can then write that

$$|m| = e^{c\log m} = m^c = |m|_\infty^c$$

since $m > 1$. We have thus found a suitable constant $c > 0$, which concludes the proof when m is a positive integer.

To complete the proof, we notice that the absolute value can be extended to positive rational number, since $|a/b| = |a|/|b|$, which shows that $|x| = |x|_\infty^c$ for $0 < x \in \mathbb{Q}$. Finally, it can be extended to arbitrary elements in $\mathbb{Q}$ by noting that $|-1| = 1$. $\square$

Let K be a number field and $\sigma : K \to \mathbb{C}$ be an embedding of K into $\mathbb{C}$, then $|x|_\sigma = |\sigma(x)|$ is an archimedean absolute value.

Theorem 6.3. *Let K be a number field. Then there is a bijection*

$$\{ \text{ archimedean places } \} \leftrightarrow \{ \text{ embeddings of } K \text{ into } \mathbb{C} \text{ up to conjugation } \}.$$

The archimedean places are also called places at infinity. We say that $|\cdot|$ is a real place if it corresponds to a real embedding. A pair of complex conjugate embeddings is a complex place.

6.3 Non-archimedean places

Let K be a number field. By definition, an absolute value: $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is non-archimedean if there exists $n > 1$, $n \in \mathbb{N}$, such that $|n| < 1$.

Lemma 6.4. *For a non-archimedean absolute value on $\mathbb{Q}$, we have that*

$$|m| \leq 1, \text{ for all } m \in \mathbb{Z}.$$

Proof. We can assume that $|\cdot|$ satisfies the triangle inequality. Let us assume by contradiction that there exists $m \in \mathbb{Z}$ such that $|m| > 1$. There exists $M = m^k$ such that

$$|M| = |m|^k > \frac{n}{1 - |n|},$$

where n is such that $|n| < 1$, which exists by definition. Let us now write M in base n:

$$M = a_0 + a_1 n + \ldots + a_r n^r$$

which is such that

$$\begin{aligned} |M| &\leq |a_0| + |a_1||n| + \ldots + |a_r||n|^r \\ &< n(1 + |n| + \ldots + |n|^r) \end{aligned}$$

since $|a_i| = |1 + \ldots + 1| \leq a_i|1| < n$. Thus

$$|M| < n \sum_{j \geq 0} |n|^j = \frac{n}{1 - |n|}$$

which is a contradiction. □

Lemma 6.5. *Let $|\cdot|$ be a non-archimedean absolute value which satisfies the triangle inequality. Then*

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

for all $\alpha, \beta \in K$. We call $|\cdot|$ ultrametric.

Proof. Let $k > 0$. We have that

$$\begin{aligned} |\alpha+\beta|^k &= |(\alpha+\beta)^k| \\ &= \left|\sum_{j=0}^{k} \binom{k}{j} \alpha^j \beta^{k-j}\right| \\ &\leq \sum_{j=0}^{k} \left|\binom{k}{j}\right| |\alpha|^j |\beta|^{k-j}. \end{aligned}$$

By the previous lemma, we have that $\left|\binom{k}{j}\right| \leq 1$, so that

$$|\alpha+\beta|^k \leq (k+1)\max\{|\alpha|, |\beta|\}^k.$$

Thus

$$|\alpha+\beta| \leq \sqrt[k]{k+1}\max\{|\alpha|, |\beta|\}.$$

We get the result by observing $k \to \infty$. □

Proposition 6.6. *let K be a number field, and $|\cdot|$ be a non-archimedean absolute value. Let $\alpha \neq 0$. Then there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and a constant $C > 1$ such that*

$$|\alpha| = C^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)},$$

where $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ *is the highest power of $\mathfrak{p}$ which divides $\alpha\mathcal{O}_K$.*

Definition 6.4. We call

$$\mathrm{ord}_{\mathfrak{p}} : K^\times \to \mathbb{Z}$$

the $\mathfrak{p}$-adic valuation.

Proof. We can assume that $|\cdot|$ satisfies the triangle inequality. It is enough to show the formula for $\alpha \in \mathcal{O}_K$.

We already know that $|m| \leq 1$ for all $m \in \mathbb{Z}$. We now extend this result for elements of $\mathcal{O}_K$.

($|\alpha| \leq 1$ for $\alpha \in \mathcal{O}_K$). For $\alpha \in \mathcal{O}_K$, we have an equation of the form

$$\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0 = 0,\ a_i \in \mathbb{Z}.$$

Let us assume by contradiction that $|\alpha| > 1$. By Lemma 6.4, we have that $|a_i| \leq 1$ for all i. In the above equation, the term α^m is thus the one with maximal absolute value. By Lemma 6.5, we get

$$\begin{aligned} |\alpha|^m &= |a_{m-1}\alpha^{m-1} + \ldots + a_0| \\ &\leq \max\{|a_{m-1}||\alpha|^{m-1}, \ldots, |a_1||\alpha|, |a_0|\} \\ &\leq \max\{|\alpha|^{m-1}, \ldots, 1\} \end{aligned}$$

thus a contradiction. We have thus shown that $|\alpha| \leq 1$ for all $\alpha \in \mathcal{O}_K$. We now set

$$\mathfrak{p} = \{\alpha \in \mathcal{O}_K \mid |\alpha| < 1\}.$$

($\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.) Let us first show that $\mathfrak{p}$ is an ideal of $\mathcal{O}_K$. Let $\alpha \in \mathfrak{p}$ and $\beta \in \mathcal{O}_K$. We have that

$$|\alpha\beta| = |\alpha||\beta| \leq |\alpha| < 1$$

showing that $\alpha\beta \in \mathfrak{p}$ and $\alpha + \beta \in \mathfrak{p}$ since

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} < 1$$

where the first inequality follows from Lemma 6.5. Let us now show that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. If $\alpha, \beta \in \mathcal{O}_K$ are such that $\alpha\beta \in \mathfrak{p}$, then $|\alpha||\beta| < 1$, which means that at least one of the two terms has to be < 1, and thus either α or β are in $\mathfrak{p}$.

(There exists a suitable $C > 1$.) We now choose π in $\mathfrak{p}$ but not in $\mathfrak{p}^2$ and let α be an element of $\mathcal{O}_K$. We set $m = \mathrm{ord}_{\mathfrak{p}}(\alpha)$. We consider α/π^m, which is of valuation 0 (by choice of π and m). We can write

$$\frac{\alpha}{\pi^m}\mathcal{O}_K = IJ^{-1}$$

with I and J are integral ideals, both prime to $\mathfrak{p}$. By the Chinese Remainder Theorem, there exists $\beta \in \mathcal{O}_K$, $\beta \in J$ and β prime to $\mathfrak{p}$. We furthermore set

$$\gamma = \beta\frac{\alpha}{\pi^m} \in I \subset \mathcal{O}_K.$$

Since both γ and β are elements of $\mathcal{O}_K$ not in $\mathfrak{p}$, we have that $|\gamma| = 1$ and $|\beta| = 1$ (if this is not clear, recall the definition of $\mathfrak{p}$ above). Thus

$$\left|\frac{\alpha}{\pi^m}\right| = \left|\frac{\gamma}{\beta}\right| = 1.$$

We have finally obtained that

$$|\alpha| = |\pi|^m$$

for all $\alpha \in \mathcal{O}_K$, so that we conclude by setting

$$C = \frac{1}{|\pi|}.$$

□

Corollary 6.7. *For a number field K, we have the following bijection*

$$\{\textit{places of } K\} \leftrightarrow \{\textit{real embeddings}\} \cup \{\textit{pairs of complex embeddings}\} \cup \{\textit{prime ideals}\}.$$

For each place of a number field, there exists a canonical choice of absolute values (called normalized absolute values).

- real places:
$$|\alpha| = |\sigma(\alpha)|_{\mathbb{R}},$$
where σ is the associated embedding.

- complex places:
$$|\alpha| = |\sigma(\alpha)|_{\mathbb{C}}^2 = |\sigma(\alpha)\bar{\sigma}(\alpha)|_{\mathbb{R}},$$
where $(\sigma, \bar{\sigma})$ is the pair of associated complex embeddings.

- finite places (or non-archimedean places):
$$|\alpha| = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)}$$
where $\mathfrak{p}$ is the prime ideal associated to $|\cdot|$.

Proposition 6.8. (Product Formula). *For all $0 \neq \alpha \in K$, we have*
$$\prod_{\nu} |\alpha|_\nu = 1$$
where the product is over all places ν, and all the absolute values are normalized.

Proof. Let us rewrite the product as
$$\prod_{\nu} |\alpha|_\nu = \prod_{\nu \text{ finite}} |\alpha|_\nu \prod_{\nu \text{ infinite}} |\alpha|_\nu$$
We now compute $\mathrm{N}(\alpha\mathcal{O}_K)$ in two ways, one which will make appear the finite places, and the other the infinite places. First,
$$\mathrm{N}(\alpha\mathcal{O}_K) = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(\alpha)} = \prod_{\nu \text{ finite}} |\alpha|_\nu^{-1}$$
which can be alternatively computed by
$$\mathrm{N}(\alpha\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|_{\mathbb{R}} = \prod_{\sigma} |\sigma(\alpha)|_{\mathbb{C}} = \prod_{\nu \text{ infinite}} |\alpha|_\nu.$$
□

6.4 Weak approximation

We conclude this chapter by proving the weak approximation theorem. The term "weak" can be thought by opposition to the "strong approximation theorem", where in the latter, we will state the existence of an element in $\mathcal{O}_K$, while we are only able to guarantee this element to exist in K for the former. Those approximation theorems (especially the strong one) restate the Chinese Remainder Theorem in the language of valuations.

Let K be a number field.

Lemma 6.9. *Let ω be a place of K and $\{\nu_1, \ldots, \nu_N\}$ be places different from ω. Then there exists $\beta \in K$ such that $|\beta|_\omega > 1$ and $|\beta|_{\nu_i} < 1$ for all $i = 1, \ldots, N$.*

Proof. We do a proof by induction on N.

(N=1). Since $|\cdot|_{\nu_1}$ is different from $|\cdot|_\omega$, they induce different topologies, and thus there exists $\delta \in K$ with

$$|\delta|_{\nu_1} < 1 \text{ and } |\delta|_\omega \geq 1$$

(recall that we proved above that if the two induced topologies are the same, then $|\delta|_{\nu_1}| < 1$ implies $|\delta|_\omega| < 1$). Similarly, there exists $\gamma \in K$ with

$$|\gamma|_\omega < 1 \text{ and } |\gamma|_{\nu_1} \geq 1.$$

We thus take $\beta = \delta\gamma^{-1}$.

(Assume true for $N-1$). We assume $N \geq 2$. By induction hypothesis, there exists $\gamma \in K$ with

$$|\gamma|_\omega > 1 \text{ and } |\gamma|_{\nu_i} < 1,\ i = 1, \ldots, N-1.$$

Again, as we proved in the case $N = 1$, we can find δ with

$$|\delta|_\omega > 1 \text{ and } |\delta|_{\nu_N} < 1.$$

We have now 3 cases:

- if $|\gamma|_{\nu_N} < 1$: then take $\beta = \gamma$. We have that $|\beta|_\omega > 1$, $|\beta|_{\nu_i} < 1$, $i = 1, \ldots, N-1$ and $|\beta|_{\nu_N} < 1$.
- if $|\gamma|_{\nu_N} = 1$: we have that $\gamma^r \to 0$ in the ν_i-adic topology, for all $i < N$. There exists thus $r >> 0$ such that

  $$\beta = \gamma^r \delta$$

  which satisfies the required inequalities. Note that $|\beta|_\omega > 1$ and $|\beta|_{\nu_N} > 1$ are immediately satisfied, the problem is for ν_i, $i = 1, \ldots, N-1$ where we have no control on $|\delta|_{\nu_i}$ and need to pick $r >> 0$ to satisfy the inequality.
- if $|\gamma|_{\nu_N} > 1$: we then have that

  $$\frac{\gamma^r}{1+\gamma^r} = \frac{1}{1+\frac{1}{\gamma^r}} \to_{r\to\infty} \begin{cases} 1 & \text{for } |\cdot|_{\nu_N} \\ 0 & \text{for } |\cdot|_{\nu_i},\ i < N \end{cases}$$

  Take

  $$\beta = \frac{\gamma^r}{1+\gamma^r}\delta,\ r >> 0.$$

□

Theorem 6.10. *Let K be a number field, $\epsilon > 0$, $\{\nu_1, \ldots, \nu_m\}$ be distinct places of K, and $\alpha_1, \ldots, \alpha_m \in K$. Then there exist $\beta \in K$ such that*

$$|\beta - \alpha_i|_{\nu_i} < \epsilon.$$

Proof. By the above lemma, there exist $\beta_j \in K$ with $|\beta_j|_{\nu_j} > 1$ and $|\beta_j|_{\nu_i} < 1$ for $i \neq j$. Set

$$\gamma_r = \sum_{j=1}^{m} \frac{\beta_j^r}{1+\beta_j^r}\alpha_j.$$

When $r \to \infty$, we have $\gamma_r \to \alpha_j$ for the ν_j-adic topology, since as in the above proof

$$\frac{\beta^r}{1+\beta^r} = \frac{1}{1+\frac{1}{\beta^r}} \to_{r\to\infty} \begin{cases} 1 & \text{for } |\beta_j|_{\nu_j} > 1 \\ 0 & \text{for } |\beta_j|_{\nu_i} < 1,\ i \neq j. \end{cases}$$

Thus take $\beta = \gamma_r$, $r >> 0$. □

Let K_{ν_i} be the completion of K with respect to the ν_i-adic topology. We can restate the theorem by saying that the image of

$$K \to \prod_{i=1}^{m} K_{\nu_i},\ x \mapsto (x, x, \dots, x)$$

is dense.

The main definitions and results of this chapter are

- Definition of absolute value, of place, of archimedean and non-archimedean places
- What are the finite/infinite places for number fields
- The product formula