Algebraic number theory **LTCC 2008**

Lecture notes, Part 5

12. Absolute values on fields

We write $\mathbb{R}_{\geq 0}$ for the set of non-negative real numbers.

Definition 12.1. Let K be a field. An *absolute value* on K is a function

$$|\ |: K \to \mathbb{R}_{\geq 0}$$

that satisfies the following conditions.

(1) $|x| = 0$ if and only if $x = 0$.
(2) $|xy| = |x| \cdot |y|$ for all $x, y \in K$.
(3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

We say that an absolute value $|\ |$ on K is *non-archimedean* if it satisfies the following strengthening of (3).

(3') $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.

We say that an absolute value $|\ |$ on K is *archimedean* if it is not non-archimedean.

Some authors use the word *norm* instead of absolute value. If $|\ |$ is an absolute value on K then one easily sees that $|1| = 1$ and $|-x| = |x|$ for all $x \in K$.

For any field K the function $|x| = 0$ if $x = 0$ and $|x| = 1$ if $x \neq 0$ is a non-archimedean absolute value. We call this the *trivial absolute value* and will in general exclude it in the following.

Note that if the field K contains $\mathbb{Z}$ (i.e. K has characteristic 0) and $|\ |$ is a non-archimedean absolute value on K, then for every $n \in \mathbb{N} \subset K$ we have $|n| \leq 1$ (this follows by induction using $|n| = |(n-1) + 1| \leq \max\{|n-1|, |1|\}$).

The usual absolute value $|x + iy| = \sqrt{x^2 + y^2}$ is an example of an absolute value on the field $\mathbb{C}$. This absolute value is archimedean (because $|2| = 2 > 1$ shows that it cannot be non-archimedean).

Lemma 12.2. *Let K be a field and $|\ |$ an absolute value on K. Then the function $d : K \times K \to \mathbb{R}_{\geq 0}$ defined by $d(x, y) = |x - y|$ is a metric on K. We call d the metric induced by the absolute value $|\ |$.*

Proof. Clear. □

If $|\ |$ is a non-archimedean absolute value, then the induced metric satisfies the *ultrametric inequality*

$$d(x, z) \leq \max\{d(x, y), d(y, z)\} \text{ for all } x, y, z \in K.$$

A *Cauchy sequence* in K is a sequence $a_1, a_2, a_3, \cdots \in K$ with the property that for every $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that $d(a_i, a_j) \leq \varepsilon$ for all $i, j \geq N$. A subset $S \subseteq K$ is called *dense* if every non-empty open set in K contains an element from S.

Definition 12.3. Let K be a field with an absolute value $|\ |$. We call K *complete* if every Cauchy sequence in K converges.

Theorem 12.4. *Let K be a field with an absolute value $|\ | : K \to \mathbb{R}_{\geq 0}$. Then there exists a completion $\hat{K}$ of K, i.e. a field extension $\hat{K}/K$ together with an absolute value $|\ | : \hat{K} \to \mathbb{R}_{\geq 0}$ which extends the absolute value on K such that*

(1) *$\hat{K}$ is complete,*
(2) *K is dense in $\hat{K}$.*

This completion $\hat{K}$ is unique up to unique isomorphism.

The idea of the proof is to construct the completion $\hat{K}$ as the quotient of the ring of Cauchy sequences in K modulo the ideal consisting of Cauchy sequences that converge to 0. For details see for example [2, §3.2] and [3, I.4] (in the special case $K = \mathbb{Q}$) and [1, II.3] (in the general case).

Definition 12.5. Two absolute values $|\ |_1$ and $|\ |_2$ on a field K are called *equivalent* if there exists a positive real number α such that $|x|_1 = |x|_2^\alpha$ for all $x \in K$.

We note that two equivalent absolute values on a field K induce equivalent metrics (i.e. a sequence is Cauchy with respect to one metric if and only if it is Cauchy with respect to the other metric). It follows that two equivalent absolute values give rise to the same completion of K.

13. Absolute values on number fields

Now let K be an algebraic number field. In this case it is possible to give a complete classification of all absolute values on K. We begin by constructing certain archimedean and non-archimedean absolute values on K.

Let $\sigma : K \to \mathbb{C}$ be an embedding of K (i.e. an injective ring homomorphism from K to $\mathbb{C}$). We define an absolute value $|\ |_\sigma$ on K by $|x|_\sigma = |\sigma(x)|$ where $|\sigma(x)|$ is the usual absolute value of the complex number $\sigma(x)$. The absolute value $|\ |_\sigma$ is archimedean. Note that $|\ |_{\overline{\sigma}} = |\ |_\sigma$ where $\overline{\sigma}$ denotes the complex conjugate embedding. Using this construction we obtain $r + s$ archimedean absolute values on K where r is the number of real embeddings and $2s$ is the number of complex embeddings of K.

Now let P be a non-zero prime ideal of the ring of integers R_K. We want to define an absolute value $|\ |_P$ on K. First let $x \in K^\times$. By Theorem 5.2 the principal fractional ideal (x) of R_K can be written as $(x) = P^e Q_1^{e_1} \cdots Q_r^{e_r}$ where $Q_1, \ldots, Q_r$ are non-zero prime ideals different from P and $e, e_1, \ldots, e_r \in \mathbb{Z}$. We define $|x|_P = \mathbf{N}(P)^{-e}$. For $x = 0$ we define $|0|_P = 0$.

Lemma 13.1. *$|\ |_P$ is a non-archimedean absolute value on K.*

Proof. Conditions (1) and (2) of an absolute value are clearly satisfied. It remains to prove condition (3'). We first observe that if $x = 0$ or $y = 0$ or $x + y = 0$ then condition (3') is clearly true, so we can assume that $x, y, x + y \in K^\times$. We write $(x) = P^e Q_1^{e_1} \cdots Q_r^{e_r}$, $(y) = P^f Q_1^{f_1} \cdots Q_r^{f_r}$ and $(x + y) = P^g Q_1^{g_1} \cdots Q_r^{g_r}$. Then

$$x \in (x) \subseteq P^{\min\{e,f\}} Q_1^{\min\{e_1,f_1\}} \cdots Q_r^{\min\{e_r,f_r\}},$$
$$y \in (y) \subseteq P^{\min\{e,f\}} Q_1^{\min\{e_1,f_1\}} \cdots Q_r^{\min\{e_r,f_r\}}.$$

It follows that

$$x + y \in P^{\min\{e,f\}} Q_1^{\min\{e_1,f_1\}} \cdots Q_r^{\min\{e_r,f_r\}},$$

hence $P^g Q_1^{g_1} \cdots Q_r^{g_r} \subseteq P^{\min\{e,f\}} Q_1^{\min\{e_1,f_1\}} \cdots Q_r^{\min\{e_r,f_r\}}$. From this we can deduce that $g \geq \min\{e, f\}, g_1 \geq \min\{e_1, f_1\}, \ldots, g_r \geq \min\{e_r, f_r\}$. It follows that

$$\begin{aligned} |x + y|_P = \mathbf{N}(P)^{-g} &\leq \mathbf{N}(P)^{-\min\{e,f\}} \\ &= \mathbf{N}(P)^{\max\{-e,-f\}} \\ &= \max\{\mathbf{N}(P)^{-e}, \mathbf{N}(P)^{-f}\} = \max\{|x|_P, |y|_P\}. \end{aligned}$$

This completes the proof of condition (3'). □

Hence for each non-zero prime ideal P of R_K we obtain a non-archimedean absolute value $|\ |_P$ on K.

Theorem 13.2. *Let K be an algebraic number field. Then every non-trivial absolute value on K is equivalent to precisely one of either the archimedean absolute values $|\ |_\sigma$ or the non-archimedean absolute values $|\ |_P$.*

Proof. See [1, Theorem 9] for the case $K = \mathbb{Q}$ and [1, p. 112] for the general case. □

It is often useful to consider the archimedean and non-archimedean absolute values of a number field together. We let $S(K)$ denote the set consisting of the non-zero prime ideals of R_K, the real embeddings $\sigma : K \to \mathbb{R}$, and one embedding from each pair of complex conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$. If $v \in S(K)$ we write $|\ |_v$ for the corresponding absolute value of K. By Theorem 13.2 there exists a bijection between $S(K)$ and equivalence classes of non-trivial absolute values on K.

If $v \in S(K)$ then we let K_v denote the completion of K with respect to $|\ |_v$. The extension of $|\ |_v$ to an absolute value on K_v will be denoted by the same symbol $|\ |_v$. One can show that if the absolute value $|\ |_v$ is non-archimedean then the image of the absolute value on K is equal to the image of the absolute value on $\hat{K}$, i.e. $|K|_v = |K_v|_v \subseteq \mathbb{R}_{\geq 0}$.

For the field $K = \mathbb{Q}$ the non-zero prime ideals of $R_K = \mathbb{Z}$ correspond to the prime numbers and we write $|\ |_p$ instead of $|\ |_{(p)}$. The completion $\mathbb{Q}_p = \mathbb{Q}_{(p)}$ is called the *field of p-adic numbers*. We often use the symbol ∞ to denote the archimedean absolute value on $\mathbb{Q}$, i.e. $|\ |_\infty$ is the usual absolute value on $\mathbb{Q}$. The completion $\mathbb{Q}_\infty$ is the field of real numbers $\mathbb{R}$.

Theorem 13.3 (Product formula)**.** *For all $x \in \mathbb{Q}^\times$ we have*

$$\prod_{v \in S(\mathbb{Q})} |x|_v = 1.$$

Proof. Let $x \in \mathbb{Q}^\times$ and consider the prime factorisation $x = \pm p_1^{e_1} \cdots p_n^{e_n}$ where $p_1, \ldots, p_n$ are distinct prime numbers and $e_1, \ldots, e_n \in \mathbb{Z}$. Then

$$|x|_p = \begin{cases} 1 & \text{if } p \neq p_i \\ p_i^{-e_i} & \text{if } p = p_i \text{ for } i = 1, \ldots, n \\ p_1^{e_1} \cdots p_n^{e_n} & \text{if } p = \infty. \end{cases}$$

Hence

$$\prod_{v \in S(\mathbb{Q})} |x|_v = \left(\prod_{i=1}^{n} p_i^{-e_i} \right) \cdot p_1^{e_1} \cdots p_n^{e_n} = 1. \qquad \square$$

We remark that there exists a similar product formula for any number field K, however one has to use a different normalisation for $|\ |_v$ if v is a complex embedding of K. See [1, III.1].

14. Hensel's lemma

Hensel's lemma allows us to prove the existence of roots of polynomials in fields which are complete with respect to a non-archimedean absolute value. However to simplify the presentation we will only consider the fields $\mathbb{Q}_p$ for some prime number p. We define

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

It is easy to see that $\mathbb{Z}_p$ is a ring. It is called the *ring of p-adic integers*. An element $x \in \mathbb{Z}_p \setminus \{0\}$ is a unit in $\mathbb{Z}_p$ if and only if $x^{-1} \in \mathbb{Z}_p$, i.e. $|x^{-1}|_p \leq 1$. Since $|x|_p \cdot |x^{-1}|_p = 1$ this implies that $x \in \mathbb{Z}_p$ is a unit if and only if $|x|_p = 1$. The set of all non-units in $\mathbb{Z}_p$ is

$$\mathbb{Z}_p \setminus \mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p < 1\}.$$

This set is the unique maximal ideal in the ring $\mathbb{Z}_p$. It is a principal ideal with generator p, because if $x \in \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ then $|x|_p \leq p^{-1}$ which implies $x = (xp^{-1}) \cdot p$ with $xp^{-1} \in \mathbb{Z}_p$. In the following we will write $a \equiv b \pmod{p^i}$ for $a, b \in \mathbb{Z}_p$ if $a - b \in (p^i)$. So in particular $a \not\equiv 0 \pmod{p}$ means $a \notin (p) = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$, i.e. a is a unit in $\mathbb{Z}_p$.

Theorem 14.1 (Hensel's lemma)**.** *Let $f(X) = c_n X^n + \cdots + c_1 X + c_0$ be a polynomial with coefficients in $\mathbb{Z}_p$, and let $f'(X) = nc_n X^{n-1} + \cdots + c_1$ be the derivative of $f(X)$. Let $a_1 \in \mathbb{Z}_p$ be such that $f(a_1) \equiv 0 \pmod{p}$ and $f'(a_1) \not\equiv 0 \pmod{p}$. Then there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_1 \pmod{p}$.*

Proof. We will construct a sequence $a_1, a_2, a_3, \ldots$ in $\mathbb{Z}_p$ such that for all $i \in \mathbb{N}$ we have

(i) $f(a_i) \equiv 0 \pmod{p^i}$,
(ii) $a_i \equiv a_{i-1} \pmod{p^{i-1}}$ if $i \geq 2$.

Clearly a_1 satisfies (i) and (ii).

Now assume that we have constructed $a_1, a_2, \ldots, a_i$ satisfying (i) and (ii). We want to find a_{i+1} in the form $a_{i+1} = a_i + \lambda p^i$ for some $\lambda \in \mathbb{Z}_p$. Note that

$$\begin{aligned} f(a_i + \lambda p^i) &= \sum_{k=0}^{n} c_k (a_i + \lambda p^i)^k \\ &= \sum_{k=0}^{n} c_k (a_i^k + k a_i^{k-1} \lambda p^i + \text{ terms divisible by } p^{i+1}) \\ &\equiv \sum_{k=0}^{n} c_k a_i^k + \left(\sum_{k=0}^{n} k c_k a_i^{k-1} \right) \lambda p^i \pmod{p^{i+1}} \\ &= f(a_i) + f'(a_i) \lambda p^i. \end{aligned}$$

Hence we will have $f(a_i + \lambda p^i) \equiv 0 \pmod{p^{i+1}}$ if and only if

$$f(a_i) + f'(a_i) \lambda p^i \equiv 0 \pmod{p^{i+1}}. \tag{1}$$

By assumption $f(a_i) \equiv 0 \pmod{p^i}$, hence (1) is equivalent to

$$\frac{f(a_i)}{p^i} + f'(a_i) \lambda \equiv 0 \pmod{p}. \tag{2}$$

Now $a_i \equiv a_1 \pmod{p}$ implies that $f'(a_i) \equiv f'(a_1) \pmod{p}$ and hence $f'(a_i) \not\equiv 0 \pmod{p}$. Therefore $f'(a_i)$ is a unit in $\mathbb{Z}_p$, so if we set

$$\lambda = -\frac{f(a_i)}{p^i} \cdot f'(a_i)^{-1}$$

then $\lambda \in \mathbb{Z}_p$ satisfies (2). Therefore $a_{i+1} = a_i + \lambda p^i$ satisfies (i) and (ii).

Now by (ii) the sequence $a_1, a_2, a_3, \ldots$ is a Cauchy sequence in $\mathbb{Z}_p$. Hence we can define $a = \lim_{i \to \infty} a_i \in \mathbb{Z}_p$. Then (again by (ii)) we have $a \equiv a_1 \pmod{p}$. Furthermore $f(a) = f(\lim_{i \to \infty} a_i) = \lim_{i \to \infty} f(a_i) = 0$ where the last equality comes from (i).

The uniqueness of a follows by observing that if $a' \in \mathbb{Z}_p$ satisfies $f(a') = 0$ and $a' \equiv a_1 \pmod{p}$ then a' must satisfy $a' \equiv a_i \pmod{p^i}$ for all $i \in \mathbb{N}$, and hence $a' = \lim_{i \to \infty} a_i = a$. The details are left to the reader. □

15. Local-global principles

Let K be an algebraic number field. It is often easier to solve problems in the completions K_v of K. So if we are given a question about K then we can first try to answer the question in K_v for all $v \in S(K)$ and then try to deduce the answer for the original question in K. In this context we call a problem for K a *global*

problem and the corresponding problems in K_v *local* problems. We first consider an easy example.

Lemma 15.1. *A number $x \in \mathbb{Q}$ is a square if and only if it is a square in all completions $\mathbb{Q}_v$ with $v \in S(\mathbb{Q})$.*

Proof. It is clear that if x is a square in $\mathbb{Q}$ then x is also a square in all $\mathbb{Q}_v$.

Conversely assume that x is a square in all $\mathbb{Q}_v$. We consider the prime factorisation

$$x = \pm \prod_p p^{e_p}$$

where $e_p \in \mathbb{Z}$ and all but finitely many e_p are zero. Now if x is a square in $\mathbb{Q}_\infty = \mathbb{R}$ then x is positive. If p is a prime number and x is a square in $\mathbb{Q}_p$ then $x = y^2$ with $y \in \mathbb{Q}_p$. Let $|y|_p = p^{-f}$ with $f \in \mathbb{Z}$. Then $p^{-e_p} = |x|_p = |y|_p^2 = p^{-2f}$ which shows that e_p is even. It follows that

$$x = \left(\prod_p p^{e_p/2} \right)^2 . \qquad \square$$

Let $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ be a polynomial with coefficients in K. If the equation $f(X_1, \ldots, X_n) = 0$ has a solution in K then clearly it also has a solution in every completion K_v. The converse is in general not true as the following example shows.

Example 15.2. Let $f(X) = (X^2-2)(X^2-17)(X^2-34) \in \mathbb{Q}[X]$. Then the equation $f(X) = 0$ has no solutions in $\mathbb{Q}$ (because $\sqrt{2}$, $\sqrt{17}$ and $\sqrt{34}$ are irrational). But one can show that the equation $f(X) = 0$ has solutions in $\mathbb{Q}_\infty = \mathbb{R}$ (this is clear) and in $\mathbb{Q}_p$ for all prime numbers p (this follows from Hensel's lemma, the details are left as an exercise).

A *quadratic form* $f(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ is a homogeneous polynomial of degree 2 with coefficients in $\mathbb{Q}$, i.e. a polynomial of the form

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{n} c_i X_i^2 + \sum_{1 \le i < j \le n} c_{ij} X_i X_j$$

with $c_i, c_{ij} \in \mathbb{Q}$.

Theorem 15.3 (Hasse-Minkowski)**.** *Let $f(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ be a quadratic form. The equation*

$$f(X_1, \ldots, X_n) = 0$$

has a non-trivial solution in $\mathbb{Q}$ if and only if it has a non-trivial solution in $\mathbb{Q}_v$ for every $v \in S(\mathbb{Q})$.

A proof of Theorem 15.3 can be found in [5, Chapter IV, Theorem 8]. The Hasse-Minkowski theorem holds not only for $\mathbb{Q}$ but for arbitrary number fields (see [4, Chapter VI] for a proof).

As a final example of a local-global principle we consider the Dedekind zeta function. Let K be an algebraic number field. Recall the Euler product for the Dedekind zeta function

$$\zeta_K(z) = \prod_{\substack{P \subseteq R_K \\ P \neq \{0\}}} \frac{1}{1 - \mathbf{N}(P)^{-z}}$$

where the product runs over all non-zero prime ideals P of R_K (see Theorem 9.2). Now each Euler factor $\frac{1}{1-\mathbf{N}(P)^{-z}}$ depends only on the completion K_P and not on K itself. Indeed, if $R_P = \{x \in K_P : |x|_P \le 1\}$ and $M_P = \{x \in K_P : |x|_P < 1\}$ then one has an isomorphism $R_K/P \cong R_P/M_P$ and hence $\mathbf{N}(P) = |R_K/P| = |R_P/M_P|$.

Therefore the Dedekind zeta function can be considered as an object which encodes local information from all completions K_P. But the analytic class number formula

$$\lim_{z\to 1}(z-1)\zeta_K(z) = \frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{|\mu_K|\sqrt{|d_K|}}$$

shows that from $\zeta_K(z)$ one can then obtain some interesting global information about the number field K.

The function

$$\begin{aligned} Z_K(z) &= \left(\pi^{-z/2}\Gamma(z/2)\right)^r \cdot \left(2(2\pi)^{-z}\Gamma(z)\right)^s \cdot \zeta_K(z) \\ &= \left(\pi^{-z/2}\Gamma(z/2)\right)^r \cdot \left(2(2\pi)^{-z}\Gamma(z)\right)^s \cdot \prod_{\substack{P\subseteq R_K \\ P\neq\{0\}}} \frac{1}{1-\mathbf{N}(P)^{-z}} \end{aligned}$$

which we used to formulate the functional equation (see Theorem 9.4.(2)) can also be interpreted in terms of completions: for every non-archimedean completion K_P of K we have the Euler factor $\frac{1}{1-\mathbf{N}(P)^{-z}}$, and for every archimedean completion K_v of K we have the Euler factor $\pi^{-z/2}\Gamma(z/2)$ or $2(2\pi)^{-z}\Gamma(z)$ depending on whether K_v is real or complex.

References

[1] A. Fröhlich, M.J. Taylor, *Algebraic number theory*, CUP, 1991.
[2] F.Q. Gouvêa, *p-adic numbers*, 2nd edition, Springer, 1997.
[3] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd edition, Springer, 1984.
[4] T.Y. Lam, *Introduction to quadratic forms over fields*, American Mathematical Society, 2005.
[5] J.-P. Serre, *A course in arithmetic*, Springer, 1973.