Algebraic Number Theory

Harry Armitage

January 23, 2021

Contents

1 Absolute Values and Places

K is a field. An ***absolute value*** (AV) on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that, for all $x, y \in K$:

i) $|x| = 0 \iff x = 0$

ii) $|xy| = |x||y|$

iii) $|x + y| \leq |x| + |y|$

We will also assume that $|\cdot|$ is not trivial, i.e.

iv) $\exists\, x \in K : |x| \neq 0, 1$

An AV is ***non-archimedean*** if it satisfies

iii-NA) $|x + y| \leq \max(|x|, |y|)$

and ***archimedean*** otherwise.

An AV determines a metric $d(x, y) = |x - y|$ which makes K a ***topological field***.

Remark It's convenient to weaken iii):

iii') $\exists\, \alpha > 0$ s.t. $\forall x, y, |x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$

For non-archimedean AVs, this makes no difference. What this does mean is that if $|\cdot|$ is an AV, then so is $|\cdot|^\alpha$ for any $\alpha > 0$. The point of this is that we want $z \mapsto z\bar{z}$ on $\mathbb{C}$ to be an AV - we'll see why later.

Let's suppose $|\cdot|$ is a non-archimedean AV. Then $\{x \in K : |x| \leq 1\} = R$ is a subring of K. It is a local ring with unique maximal ideal $\{|x| < 1\} = \mathfrak{m}_R$.

It is a ***valuation ring*** of K (i.e. $x \in K \setminus R \implies x^{-1} \in R$).

Lemma 1.1. *R is a maximal subring of K.*

Proof. Let $x \in K \setminus R$, so $|x| > 1$. Then if $y \in K$, there is some $n \geq 0$ with $|yx^{-n}| = \frac{|y|}{|x|^n} \leq 1$. So $y \in x^n R$ for $n \gg 0$, and hence $R[x] = K$. Hence R is maximal. □

There is a general notion of valuation (not nec. $\mathbb{R}$-valued). In the more general context, these valuations are called ***rank 1 valuations***, and they have this maximality property.

We say two absolute values $|\cdot|$ and $|\cdot|'$ are ***equivalent*** if there is $\alpha > 0$ with $|\cdot|' = |\cdot|^\alpha$. This is an equivalence relation.

Proposition 1.2. *The following are equivalent:*

i) $|\cdot|, |\cdot|'$ *are equivalent.*

ii) $|x| \leq |y| \iff |x|' \leq |y|'$.

iii) $|x| < |y| \iff |x|' < |y|'$.

Proof. From local fields, or exercise. □

Corollary 1.3. *Let $|\cdot|, |\cdot|'$ be non-archimedean AVs, with valuation rings R, R'. Then $|\cdot|, |\cdot|'$ are equivalent if and only if $R = R'$ if and only if $R \subset R'$.*

Equivalent AVs define equivalent metrics, hence the same topologies, hence the ***completion*** of K with respect to $|\cdot|$ depends only on the equivalence class of $|\cdot|$.

Inequivalent AVs determine "independent" topologies in the following sense:

Proposition 1.4 (Weak Approximation)**.** *Let $|\cdot|_i$ for $1 \leq i \leq n$ be pairwise inequivalent AVs on K, and $a_1, \dots, a_n \in K$, $\delta > 0$.*

Then there is $x \in K$ such that, for all i, $|x - a_i|_i < \delta$.

Proof. Suppose $z_j \in K$ such that $|z_j|_j > 1$, and $|z_j|_i < 1$ for all $i \neq j$. Then $|\frac{z_j^N}{z_j^N+1}|_i \to 0$ as $N \to \infty$ if $i \neq j$, and to 1 if $i = j$.

So then $x = \sum a_j \frac{z_j^N}{z_j^N+1}$ works for N sufficiently large. So it's enough to find z_j, and by symmetry take $j = 1$. We then induct on n. The case $n = 1$ is trivial.

Suppose we have y with $|y|_1 > 1$, and $|y|_2, \dots, |y|_{n-1} < 1$. If $|y|_n < 1$, we're finished, otherwise pick $w \in K$ with $|w|_1 > 1 > |w|_n$, by **1.2**. If $|y|_n = 1$, then $z = y^N w$ works, and if $|y|_n > 1$, then $z = \frac{y^N w}{y^N+1}$ works. □

Remark. If $K = \mathbb{Q}$, $|\cdot|_1, \dots, |\cdot|_n$ are the p_i-adic AVs for distinct primes p_i and $a_i \in \mathbb{Z}$, then weak approximation says that, for all $n_i \geq 1$, there is $x \in \mathbb{Q}$ which is a p_i-adic integer for all i, and $x \equiv a_i \mod p_i^{n_i}$ for all i. This is weaker than CRT, which guarantees $x \in \mathbb{Z}$.

Definition. A ***place*** of K is an equivalence class of AVs on K.

Example $K = \mathbb{Q}$. ***Ostrowski's Theorem*** implies every AV on $\mathbb{Q}$ is equivalent to one of $|\cdot|_p, |\cdot|_\infty$. So places of $\mathbb{Q}$ are the primes, and ∞. We write V_K for the set of places of K.

We write $V_{K,\infty}$ for the places given by archimedean AVs (the infinite places).

We write $V_{K,f}$ for the places given by non-archimedean AVs (the finite places).

We often use letters v, w denote places. Given $v \in V_K$, K_v will denote the completion of K at v. If $v : K^\times \to \mathbb{R}$ is a ***valuation***, we will also use v to denote the corresponding place, i.e. the equivalence class of AVs $x \mapsto \gamma^{-v(x)}$.

We can restate the weak approximation in terms of places:

Proposition 1.4. *Let $v_1, \dots, v_n$ be distinct places of K. Then the image of the diagonal inclusion*

$$K \hookrightarrow \prod_{1 \leq i \leq n} K_{v_i}$$

is dense.

1.1 Extensions and Places

Let L/K be finite and separable, and let v, w be places of K, L respectively. Say w ***lies over*** or ***divides*** v (notation $w|v$) if v is the restriction of w to K.

Then there is a unique continuous $K_v \hookrightarrow L_w$ extending $K \hookrightarrow L$.

Proposition 1.5. *There is a unique isomorphism of topological rings*

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$$

mapping $x \otimes y$ to $(xy)_w$.

Corollary 1.6.

1. *$\{w|v\}$ is finite, nonempty, and $[L : K] = \sum_{w|v}[L_w : K_v]$*
2. *$\forall x \in K$,*
   $N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x)$
   $\mathrm{Tr}_{L/K}(x) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x)$.

If L/K is Galois with Galois group G, then G acts on the places w of L lying over a given v. We define the ***decomposition group*** D_w or G_w to be the stabiliser of w. This action is transitive. If $g \in D_w$, then it is continuous for the topology induced by w on L, so it extends to an automorphism of L_w, the completion of L at w.

$$G \supset D_w \cong \mathrm{Gal}(L_w/K_v)$$

Suppose v is a ***discrete valuation*** of L, i.e. it is a finite place, and the valuation ring is a DVR. Then so is any $w|v$, and we define:

- $f(w|v)$, the degree of residue class extension, $= e_{L_w/K_v}$
- $e(w|v)$, the ramification degree

and $[L_w : K_v] = e(w|v)f(w|v)$.

2 Number Fields

A lot of this theory applies to other global fields, e.g. function fields. K will here be a number field (i.e. finite extension of the rationals) with ring of integers O_K. We have some basic properties:

- O_K is a ***Dedekind domain***, i.e.
  1. Noetherian (in fact, O_K is a f.g. $\mathbb{Z}$-module).
  2. Integrally closed in K (by definition).
  3. Every non-zero prime ideal is maximal, so has Krull dimension ≤ 1.

We have some basic results about Dedekind domains:

Theorem 2.1.

1. *A local domain is Dedekind if and only if it is a DVR.*
2. *For a domain R, TFAE:*
   (a) *R is Dedekind.*
   (b) *R is Noetherian and for every non-zero prime $\mathfrak{p}$, $R_\mathfrak{p}$ is a DVR.*
   (c) *Every fractional ideal of R is invertible.*

3. *A Dedekind domain with only finitely many prime ideals (i.e.* **semi-local***) is a PID.*

Proof.

1. Proved in local fields, $\implies$ is the hardest part.
2. Let $K = \text{Frac}(R)$. A fractional ideal of R is a non-zero R-submodule $I \subset K$ for some $0 \neq x \in R$ where $xI \subset R$ is an ideal. For $(a) \implies (b)$ it is enough to check (exercise) that the basic properties are preserved under localisation.

   For $(b) \implies (c)$, I is invertible if there is a fractional ideal I^{-1} such that $II^{-1} = R$. To prove (c), we may assume $I \subset R$ is an ideal. Then let $I^{-1} = \{x \in K : xI \subset R\}$. If $0 \neq y \in I$, then $R \subset I^{-1} \subset y^{-1}R$, and so I^{-1} is a fractional ideal. Clearly $I^{-1}I \subset R$. Now let $P \subset R$ be prime - it is sufficient to show $I^{-1}I \not\subset P$. Let $I = (a_1, \ldots, a_n)$. WLOG take $v_P(a_1) \leq v_P(a_i)$ for all $i > 1$. Then $IR_P = a_1R_P$, as R_P is a DVR.

   Hence $a_i/a_1 = x_i/y_i \in R_P$ where $x_i \in R, y_i \in R \setminus P$. Then $y = \prod y_i \notin P$ as P is prime, and $ya_i/a_1 \in R$ for all i, and so $y/a_i \in I^{-1}$, so $y \in II^{-1} \setminus P$.

   For $(c) \implies (a)$, we check the properties. R is Noetherian - let $I \subset R$ be an ideal. Then $II^{-1} = R \implies 1 = \sum_{i=1}^{n} a_i b_i, a_i \in I, b_i \in I^{-1}$. Let $I' = (a_1, , a_r) \subset I$. Then $I'I^{-1} = R = II^{-1}$, and so $I' = I$, and I is finitely generated.

   R is integrally closed. Let $x \in K$, integral over R. Then $I := R[x] = \sum_{0 \leq i < d} Rx^i \subset K$ is a fractional ideal. Obviously $I^2 = I$, so $I = I^2I^{-1} = II^{-1} = R$, i.e. $x \in R$.

   Every non-zero prime is maximal. Take $\{0\} \neq Q \subset P \subsetneq R$ where P, Q are prime. Then $R \subsetneq P^{-1} \subset Q^{-}1$, and $Q \subsetneq P^{-1}Q \subset R$, and $P(P^{-1}Q) = Q$, so as Q is prime and $P^{-1}Q \not\subset R$, we must have $P \subset Q$, and so $P = Q$.
3. Let R be a semi-local Dedekind domain with non-zero primes $P_1, \ldots, P_n$. Choose $x \in R$ with $x \in P_1 \setminus P_1^2, x \in P_2, \ldots, P_n$. Then $P_1 = (x)$ and every ideal is a product of powers of $\{P_i\}$ (see below), hence R is a PID.

□

Theorem 2.2. *Let R be Dedekind. Then:*

1. *The group of fractional ideals is freely generated by the non-zero prime ideals, and*

$$I = \prod_P P^{v_P(I)}$$

   with $v_P(I) = \inf_{x \in I}(v_P(x))$.

2. *If $(R : I) < \infty$ for all $I \neq (0)$, then for all I, J, $(R : IJ) = (R : I)(R : J)$.*

Proof.

1. If $I \neq R$, then $I \subset P$ for some prime ideal P. Then $I = PI', I' = IP^{-1} \supsetneq I$. Then by Noetherian induction, I is a product of powers of prime ideals, say $I = \prod P^{a_P}$.

   We get the same for fractional ideals $J = x^{-1}I$.

   Consider the homomorphisms $\{\text{fractional ideals of } R\} \to \{\text{fractional ideals of } R_P\} \to \mathbb{Z}$ given by $I \mapsto IR_P$, $(\pi^n) \mapsto n$.

The composition is $I \mapsto v_P(I)$, and if $Q \neq P$ then $v_P(Q) = 0$.

So {fractional ideals of R} $\longrightarrow \bigoplus_P \mathbb{Z}$ maps $\prod P^{a_P}$ to $(a_P)_P$. Hence the a_P are unique and this is an isomorphism.

$\square$