Math 129: Algebraic Number Theory
Lecture 15: Valuations

William Stein

Thursday, March 25, 2004

I don't know about you, but Swinnerton-Dyer's book is getting on my nerves (I will avoid more passionate words), so we're switching to the venerable and famous book by Cassels-Frohlich. In particular, we're going to systematically go through the article *Global Fields* by Cassels, which is chapter 2 of the book. The topics are similar to the ones in chapter 2 of Swinnerton-Dyer, but Cassels's article is amazingly well written. Also, you are well prepared to read and appreciate it given what you've learned so far in this course.

A scan of the article is available on the web page for the course, and you can get a photocopy from me.

The notes for the rest of the course will be a rewrite of *Global Fields* meant to make it more accessible. I will copy Cassels's article closely, except I will fix any typos found, reword things in a way consistent with the rest of these notes, and add exercises and comments you might have. I will also add the details of the implicit exercises and remarks that are left to the reader.

1 Valuations

Definition 1.1 (Valuation). A *valuation* $|\ |$ on a field K is a function defined on K with values in $\mathbf{R}_{\geq 0}$ satisfying the following axioms:

(1) $|a| = 0$ if and only if $a = 0$,

(2) $|ab| = |a|\,|b|$, and

(3) there is a constant $C \geq 1$ such that $|1 + a| \leq C$ whenever $|a| \leq 1$.

The *trivial valuation* is the valuation for which $|a| = 1$ for all $a \neq 0$. We will often tacitly exclude the trivial valuation from consideration.

From (2) we have

$$|1| = |1| \cdot |1|\,,$$

so $|1| = 1$ by (1). If $w \in K$ and $w^n = 1$, then $|w| = 1$ by (2). In particular, the only valuation of a finite field is the trivial one. The same argument shows that $|-1| = |1|$, so

$$|-a| = |a| \qquad \text{all } a \in K.$$

Definition 1.2 (Equivalent). Two valuations $|\ |_1$ and $|\ |_2$ on the same field are equivalent if there exists $c > 0$ such that

$$|a|_2 = |a|_1^c$$

for all $a \in K$.

Note that if $|\ |_1$ is a valuation, then $|\ |_2 = |\ |_1^c$ is also a valuation. Also, equivalence of valuations is an equivalence relation.

If $|\ |$ is a valuation and C is the constant from Axiom (3), then there is a $c > 0$ such that $C^c = 2$ (i.e., $c = \log(C)/\log(2)$). Then we can take 2 as constant for the equivalent valuation $|\ |^c$. Thus every valuation is equivalent to a valuation with $C = 2$. Note that if $C = 1$, e.g., if $|\ |$ is the trivial valuation, then we could simply take $C = 2$ in Axiom (3).

Proposition 1.3. *Suppose $|\ |$ is a valuation with $C = 2$. Then for all $a, b \in K$ we have*

$$|a + b| \leq |a| + |b| \qquad \textit{(triangle inequality).} \tag{1.1}$$

Proof. Suppose $a_1, a_2 \in K$ with $|a_1| \geq |a_2|$. Then $a = a_2/a_1$ satisfies $|a| \leq 1$. By Axiom (3) we have $|1 + a| \leq 2$, so multiplying by a_1 we see that

$$|a_1 + a_2| \leq 2|a_1| = 2 \cdot \max\{|a_1|, |a_2|\}.$$

Also we have

$$|a_1 + a_2 + a_3 + a_4| \leq 2 \cdot \max\{|a_1 + a_2|, |a_3 + a_4|\} \leq 4 \cdot \max\{|a_1|, |a_2|, |a_3|, |a_4|\},$$

and inductively we have for any $r > 0$ that

$$|a_1 + a_2 + \cdots + a_{2^r}| \leq 2^r \cdot \max |a_j|.$$

If n is any positive integer, let r be such that $2^{r-1} \leq n \leq 2^r$. Thenn

$$|a_1 + a_2 + \cdots + a_n| \leq 2^r \cdot \max\{|a_j|\} \leq 2n \cdot \max\{|a_j|\},$$

since $2^r \leq 2n$. In particular,

$$|n| \leq 2n \cdot |1| = 2n \qquad \text{(for } n > 0\text{).} \tag{1.2}$$

Applying (1.2) to $\left|\binom{n}{j}\right|$ and using the binomial expansion, we have for any $a, b \in K$

that

$$
\begin{aligned}
|a+b|^n &= \left|\sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}\right| \\
&\leq 2(n+1)\max_j \left\{\left|\binom{n}{j}\right| |a|^j\, |b|^{n-j}\right\} \\
&\leq 2(n+1)\max_j \left\{2\binom{n}{j} |a|^j\, |b|^{n-j}\right\} \\
&\leq 4(n+1)\max_j \left\{\binom{n}{j} |a|^j\, |b|^{n-j}\right\} \\
&\leq 4(n+1)(|a|+|b|)^n.
\end{aligned}
$$

Now take nth roots of both sides to obtain

$$|a+b| \leq \sqrt[n]{4(n+1)} \cdot (|a|+|b|).$$

We have by elementary calculus that

$$\lim_{n\to\infty} \sqrt[n]{4(n+1)} = 1,$$

so $|a+b| \leq |a|+|b|$. (The "elementary calculus": We instead prove that $\sqrt[n]{n} \to 1$, since the argument is the same and the notation is simpler. First, for any $n \geq 1$ we have $\sqrt[n]{n} \geq 1$, since upon taking nth powers this is equivalent to $n \geq 1^n$, which is true by hypothesis. Second, suppose there is an $\varepsilon > 0$ such that $\sqrt[n]{n} \geq 1+\varepsilon$ for all $n \geq 1$. Then taking logs of boths sides we see that $\frac{1}{n}\log(n) \geq \log(1+\varepsilon) > 0$. But $\log(n)/n \to 0$, so there is no such ε. Thus $\sqrt[n]{n} \to 1$ as $n \to \infty$.) $\square$

Note that Axioms (1), (2) and Equation (1.1) imply Axiom (3) with $C = 2$. We take Axiom (3) instead of Equation (1.1) for the technical reason that we will want to call the square of the absolute value of the complex numbers a valuation.

Lemma 1.4. *Suppose $a, b \in K$, and $|\ |$ is a valuation on K with $C \leq 2$. Then*

$$\Big||a|-|b|\Big| \leq |a-b|\,.$$

(Here the big absolute value on the outside of the left-hand side of the inequality is the usual absolute value on real numbers, but the other absolute values are a valuation on an arbitrary field K.)

Proof. We have

$$|a| = |b+(a-b)| \leq |b|+|a-b|,$$

so $|a|-|b| \leq |a-b|$. The same argument with a and b swapped implies that $|b|-|a| \leq |a-b|$, which proves the lemma. $\square$

2 Types of Valuations

We define two important properties of valuations, both of which apply to equivalence classes of valuations (i.e., the property holds for $|\ |$ if and only if it holds for a valuation equivalent to $|\ |$).

Definition 2.1 (Discrete). A valuation $|\ |$ is *discrete* if there is a $\delta > 0$ such that for any $a \in K$

$$1 - \delta < |a| < 1 + \delta \implies |a| = 1.$$

Thus the absolute values are bounded away from 1.

To say that $|\ |$ is discrete is the same as saying that the set

$$G = \bigl\{\log |a| : a \in K, a \neq 0\bigr\} \subset \mathbf{R}$$

forms a discrete subgroup of the reals under addition (because the elements of the group G are bounded away from 0).

Proposition 2.2. *A nonzero discrete subgroup G of $\mathbf{R}$ is free on one generator.*

Proof. Since G is discrete there is a positive $m \in G$ such that for any positive $x \in G$ we have $m \leq x$. Suppose $x \in G$ is an arbitrary positive element. By subtracting off integer multiples of m, we find that there is a unique n such that

$$0 \leq x - nm < m.$$

Since $x - nm \in G$ and $0 < x - nm < m$, it follows that $x - nm = 0$, so x is a multiple of m. $\square$

By Proposition 2.2, the set of $\log |a|$ for nonzero $a \in K$ is free on one generator, so there is a $c < 1$ such that $|a|$, for $a \neq 0$, runs precisely through the set

$$c^{\mathbf{Z}} = \{c^m : m \in \mathbf{Z}\}$$

(Note: we can replace c by c^{-1} to see that we can assume that $c < 1$).

Definition 2.3 (Order). If $|a| = c^m$, we call $m = \operatorname{ord}(a)$ the *order* of a.

Axiom (2) of valuations translates into

$$\operatorname{ord}(ab) = \operatorname{ord}(a) + \operatorname{ord}(b).$$

Definition 2.4 (Non-archimedean). A valuation $|\ |$ is *non-archimedean* if we can take $C = 1$ in Axiom (3), i.e., if

$$|a + b| \leq \max\bigl\{|a|, |b|\bigr\}. \tag{2.1}$$

If $|\ |$ is not non-archimedean then it is *archimedean*.

Note that if we can take $C = 1$ for $|\ |$ then we can take $C = 1$ for any valuation equivalent to $|\ |$. To see that (2.1) is equivalent to Axiom (3) with $C = 1$, suppose $|b| \leq |a|$. Then $|b/a| \leq 1$, so Axiom (3) asserts that $|1 + b/a| \leq 1$, which implies that $|a + b| \leq |a| = \max\{|a|, |b|\}$, and conversely.

We note at once the following consequence:

Lemma 2.5. *Suppose $|\ |$ is a non-archimedean valuation. If $a, b \in K$ with $|b| < |a|$, then $|a + b| = |a|$.*

Proof. Note that $|a + b| \leq \max\{|a|, |b|\} = |a|$, which is true even if $|b| = |a|$. Also,

$$|a| = |(a + b) - b| \leq \max\{|a + b|, |b|\} = |a + b|,$$

where for the last equality we have used that $|b| < |a|$ (if $\max\{|a + b|, |b|\} = |b|$, then $|a| \leq |b|$, a contradiction).

□

Definition 2.6 (Ring of Integers). Suppose $|\ |$ is a non-archimedean absolute value on a field K. Then

$$\mathcal{O} = \{a \in K : |a| \leq 1\}$$

is a ring called the *ring of integers* of K with respect to $|\ |$.

Lemma 2.7. *Two non-archimedean valuations $|\ |_1$ and $|\ |_2$ are equivalent if and only if they give the same $\mathcal{O}$.*

We will prove this modulo the claim (to be proved next time) that valuations are equivalent if (and only if) they induce the same topology.

Proof. Suppose suppose $|\ |_1$ is equivalent to $|\ |_2$, so $|\ |_1 = |\ |_2^c$, for some $c > 0$. Then $|c|_1 \leq 1$ if and only if $|c|_2^c \leq 1$, i.e., if $|c|_2 \leq 1^{1/c} = 1$. Thus $\mathcal{O}_1 = \mathcal{O}_2$.

Conversely, suppose $\mathcal{O}_1 = \mathcal{O}_2$. Then $|a|_1 < |b|_1$ if and only if $a/b \in \mathcal{O}_1$ and $b/a \notin \mathcal{O}_1$, so

$$|a|_1 < |b|_1 \iff |a|_2 < |b|_2. \tag{2.2}$$

The topology induced by $|\ |_1$ has as basis of open neighborhoods the set of open balls

$$B_1(z, r) = \{x \in K : |x - z|_1 < r\},$$

for $r > 0$, and likewise for $|\ |_2$. Since the absolute values $|b|_1$ get arbitrarily close to 0, the set $\mathcal{U}$ of open balls $B_1(z, |b|_1)$ also forms a basis of the topology induced by $|\ |_1$ (and similarly for $|\ |_2$). By (2.2) we have

$$B_1(z, |b|_1) = B_2(z, |b|_2),$$

so the two topologies both have $\mathcal{U}$ as a basis, hence are equal. That equal topologies implies equivalence of the corresponding valuations will be proved later. □

The set of $a \in \mathcal{O}$ with $|a| < 1$ forms an ideal $\mathfrak{p}$ in $\mathcal{O}$. The ideal $\mathfrak{p}$ is maximal, since if $a \in \mathcal{O}$ and $a \notin \mathfrak{p}$ then $|a| = 1$, so $|1/a| = 1/|a| = 1$, hence $1/a \in \mathcal{O}$, so a is a unit.

Lemma 2.8. *A non-archimedean valuation $|\ |$ is discrete if and only if $\mathfrak{p}$ is a principal ideal.*

Proof. First suppose that $|\ |$ is discrete. Choose $\pi \in \mathfrak{p}$ with $|\pi|$ maximal, which we can do since

$$S = \{\log|a| : a \in \mathfrak{p}\} \subset (-\infty, 1],$$

so S is discrete and bounded above. Suppose $a \in \mathfrak{p}$. Then

$$\left|\frac{a}{\pi}\right| = \frac{|a|}{|\pi|} \le 1,$$

so $a/\pi \in \mathcal{O}$. Thus

$$a = \pi \cdot \frac{a}{\pi} \in \pi\mathcal{O}.$$

Conversely, suppose $\mathfrak{p} = (\pi)$ is principal. For any $a \in \mathfrak{p}$ we have $a = \pi b$ with $b \in \mathcal{O}$. Thus

$$|a| = |\pi| \cdot |b| \le |\pi| < 1.$$

Thus $\{|a| : |a| < 1\}$ is bounded away from 1, which is exactly the definition of discrete. $\square$

Example 2.9. For any prime p, define the p-adic valuation $|\ |_p : \mathbf{Q} \to \mathbf{R}$ as follows. Write a nonzero $\alpha \in K$ as $p^n \cdot \frac{a}{b}$, where $\gcd(a, p) = \gcd(b, p) = 1$. Then

$$\left|p^n \cdot \frac{a}{b}\right|_p := p^{-n} = \left(\frac{1}{p}\right)^n.$$

This valuation is both discrete and non-archimedean. The ring $\mathcal{O}$ is the local ring

$$\mathbf{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbf{Q} : p \nmid b\right\},$$

which has maximal ideal generated by p. Note that $\mathrm{ord}(p^n \cdot \frac{a}{b}) = p^n$.

We will need the following lemma later.

Lemma 2.10. *A valuation $|\ |$ is non-archimedean if and only if $|n| \le 1$ for all n in the ring generated by 1 in K.*

Note that we cannot identify the ring generated by 1 with $\mathbf{Z}$ in general, because K might have characteristic $p > 0$.

Proof. If $| \ |$ is non-archimedean, then $|1| \leq 1$, so by Axiom (3) with $a = 1$, we have $|1 + 1| \leq 1$. By induction it follows that $|n| \leq 1$.

Conversely, suppose $|n| \leq 1$ for all integer multiples n of 1. This condition is also true if we replace $| \ |$ by any equivalent valuation, so replace $| \ |$ by one with $C \leq 2$, so that the triangle inequality holds. Suppose $a \in K$ with $|a| \leq 1$. Then by the triangle inequality,

$$\begin{aligned} |1+a|^n &= |(1+a)^n| \\ &\leq \sum_{j=0}^{n} \left| \binom{n}{j} \right| |a| \\ &\leq 1 + 1 + \cdots + 1 = n. \end{aligned}$$

Now take nth roots of both sides to get

$$|1 + a| \leq \sqrt[n]{n},$$

and take the limit as $n \to \infty$ to see that $|1 + a| \leq 1$. This proves that one can take $C = 1$ in Axiom (3), hence that $| \ |$ is non-archimedean. □