Math 129: Algebraic Number Theory
Lecture 16: Examples of Valuations, Topology

William Stein

Tuesday, April 6, 2004

HOMEWORK REMINDER: Because of the senior thesis crunch, several people received extensions on homework. This homework is all due *this Thursday*. I will not accept any of the homework due Thursday later than Thursday.

Projects: Discuss now. The list was as follows, but other projects are possible.

1. How to compute class groups of number fields.
2. How to compute the unit group of a number field (we didn't even prove the unit group is computable in class).
3. How to solve the norm equation $\mathrm{Norm}_{K/\mathbf{Q}}(x) = d$.
4. Explore relations between quadratic reciprocity and class field theory for $\mathbf{Q}$.
5. The Chebotarev Density Theorem: read about it and explain what the point is, and something about why it is true (e.g., for quadratic fields).
6. Give a proof of Dirichlet's theorem on primes in an arithmetic progression (connected to the Chebotarev project above).
7. Connection between ideal class groups of quadratic imaginary fields and classes of positive definite binary quadratic forms. Gauss's class number problem.
8. The conjecture that there are infinitely many number fields of class number 1. What is known? What do the Cohen-Lenstra heuristics predict? Why is this problem so hard?
9. Quadratic imaginary fields and complex multiplication elliptic curves.
10. Elements of Shafarevich-Tate groups: give complete examples with proofs of equations like $3x^3 + 4y^3 + 5z^3 = 0$ that have a solution (with not all x, y, z zero) over every p-adic field $\mathbf{Q}_p$ and over $\mathbf{R}$, but not over $\mathbf{Q}$.

Now the lecture. First, we finish section 2.

2 Types of Valuations (continued)

Let K be a field with a valuation $|\ |$. Suppose the valuation is discrete. Then

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

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

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 2.1. *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 the discrete set S is bounded above. Suppose $a \in \mathfrak{p}$. Then

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

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

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

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

Example 2.2. 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 $\operatorname{ord}(p^n \cdot \frac{a}{b}) = p^n$.

We will need the following lemma later.

Lemma 2.3. *A valuation $|\ |$ is non-archimedean if and only if $|n| \leq 1$ 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. □

3 Examples of Valuations

The archetypal example of an archimedean valuation is the absolute value on the complex numbers. It is essentially the only one:

Theorem 3.1 (Gelfand-Tornheim). *Any field K with an archimedean valuation is isomorphic to a subfield of* $\mathbf{C}$*, the valuation being equivalent to that induced by the usual absolute value on* $\mathbf{C}$*.*

We do not prove this here as we do not need it. For a proof, see [E. Artin, *Theory of Algebraic Numbers*, pages 45 and 67].

There are many non-archimedean valuations. On the rationals $\mathbf{Q}$ there is one for every prime $p > 0$, the p-adic valuation, as in Example 2.2.

Theorem 3.2 (Ostrowski). *The nontrivial valuations on* $\mathbf{Q}$ *are those equivalent to $|\cdot|_p$, for some prime p, and the usual absolute value $|\cdot|_\infty$.*

Remark 3.3. Before giving the proof, we pause with a brief remark about Ostrowski. According to

`http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Ostrowski.html`

Ostrowski was a Ukrainian mathematician who lived 1893–1986. Gautschi writes about Ostrowski as follows: "... you are able, on the one hand, to emphasise the abstract and axiomatic side of mathematics, as for example in your theory of general norms, or, on the other hand, to concentrate on the concrete and constructive aspects of mathematics, as in your study of numerical methods, and to do both with equal ease. *You delight in finding short and succinct proofs, of which you have given many examples* ..." [italics mine]

We will now give an example of one of these short and succinct proofs.

Proof. Suppose $|\cdot|$ is a nontrivial valuation on $\mathbf{Q}$.

Nonarchimedean case: Suppose $|c| \leq 1$ for all $c \in \mathbf{Z}$, so by Lemma 2.3, $|\cdot|$ is nonarchimedean. Since $|\cdot|$ is nontrivial, the set

$$\mathfrak{p} = \{a \in \mathbf{Z} : |a| < 1\}$$

is nonzero. Also $\mathfrak{p}$ is an ideal and if $|ab| < 1$, then $|a|\,|b| = |ab| < 1$, so $|a| < 1$ or $|b| < 1$, so $\mathfrak{p}$ is a prime ideal of $\mathbf{Z}$. Thus $\mathfrak{p} = p\mathbf{Z}$, for some prime number p. Since every element of $\mathbf{Z}$ has valuation at most 1, if $u \in \mathbf{Z}$ with $\gcd(u, p) = 1$, then $u \notin \mathfrak{p}$, so $|u| = 1$. Let $\alpha = \log_{|p|} \frac{1}{p}$, so $|p|^\alpha = \frac{1}{p}$. Then for any r and any $u \in \mathbf{Z}$ with $\gcd(u, p) = 1$, we have

$$|up^r|^\alpha = |u|^\alpha\,|p|^{\alpha r} = |p|^{\alpha r} = p^{-r} = |up^r|_p\,.$$

Thus $|\cdot|^\alpha = |\cdot|_p$ on $\mathbf{Z}$, hence on $\mathbf{Q}$ by multiplicativity, so $|\cdot|$ is equivalent to $|\cdot|_p$, as claimed.

Archimedean case: By replacing $|\cdot|$ by a power of $|\cdot|$, we may assume without loss that $|\cdot|$ satisfies the triangle inequality. We first make some general remarks about any valuation that satisfies the triangle inequality. Suppose $a \in \mathbf{Z}$ is greater than 1. Consider, for any $b \in \mathbf{Z}$ the base-a expansion of b:

$$b = b_m a^m + b_{m-1} a^{m-1} + \cdots + b_0,$$

where

$$0 \leq b_j < a \qquad (0 \leq j \leq m),$$

and $b_m \neq 0$. Since $a^m \leq b$, taking logs we see that $m \log(a) \leq \log(b)$, so

$$m \leq \frac{\log(b)}{\log(a)}.$$

Let $M = \max\limits_{1 \leq d < a} |d|$. Then by the triangle inequality for $|\cdot|$, we have

$$\begin{aligned} |b| &\leq |b_m|\,a^m + \cdots + |b_1|\,|a| + |b_0| \\ &\leq M \cdot (|a|^m + \cdots + |a| + 1) \\ &\leq M \cdot (m+1) \cdot \max(1, |a|^m) \\ &\leq M \cdot \left(\frac{\log(b)}{\log(a)} + 1\right) \cdot \max\left(1, |a|^{\log(b)/\log(a)}\right), \end{aligned}$$

where in the last step we use that $m \leq \frac{\log(b)}{\log(a)}$. Setting $b = c^n$, for $c \in \mathbf{Z}$, in the above inequality and taking nth roots, we have

$$\begin{aligned} |c| &\leq \left(M \cdot \left(\frac{\log(c^n)}{\log(a)} + 1\right) \cdot \max(1, |a|^{log(c^n)/\log(a)})\right)^{1/n} \\ &= M^{1/n} \cdot \left(\frac{\log(c^n)}{\log(a)} + 1\right)^{1/n} \cdot \max\left(1, |a|^{\log(c^n)/\log(a)}\right)^{1/n}. \end{aligned}$$

The first factor $M^{1/n}$ converges to 1 as $n \to \infty$, since $M \geq 1$ (because $|1| = 1$). The second factor is

$$\left(\frac{\log(c^n)}{\log(a)} + 1\right)^{1/n} = \left(n \cdot \frac{\log(c)}{\log(a)} + 1\right)^{1/n}$$

which also converges to 1, for the same reason that $n^{1/n} \to 1$ (because $\log(n^{1/n}) = \frac{1}{n}\log(n) \to 0$ as $n \to \infty$). The third factor is

$$\max\left(1, |a|^{\log(c^n)/\log(a)}\right)^{1/n} = \begin{cases} 1 & \text{if } |a| < 1, \\ |a|^{\log(c)/\log(a)} & \text{if } |a| \geq 1. \end{cases}$$

Putting this all together, we see that

$$|c| \leq \max\left(1, |a|^{\frac{\log(c)}{\log(a)}}\right).$$

Our assumption that $|\cdot|$ is nonarchimedean implies that there is $c \in \mathbf{Z}$ with $c > 1$ and $|c| > 1$. Then for all $a \in \mathbf{Z}$ with $a > 1$ we have

$$1 < |c| \leq \max\left(1, |a|^{\frac{\log(c)}{\log(a)}}\right), \tag{3.1}$$

so $1 < |a|^{\log(c)/\log(a)}$, so $1 < |a|$ as well (i.e., any $a \in \mathbf{Z}$ with $a > 1$ automatically satisfies $|a| > 1$). Also, taking the $1/\log(c)$ power on both sides of (3.1) we see that

$$|c|^{\frac{1}{\log(c)}} \leq |a|^{\frac{1}{\log(a)}}. \tag{3.2}$$

Because, as mentioned above, $|a| > 1$, we can interchange the roll of a and c to obtain the reverse inequality of (3.2). We thus have

$$|c| = |a|^{\frac{\log(c)}{\log(a)}}.$$

Letting $\alpha = \log(2) \cdot \log_{|2|}(e)$ and setting $a = 2$, we have

$$|c|^{\alpha} = |2|^{\frac{\alpha}{\log(2)} \cdot \log(c)} = \left(|2|^{\log_{|2|}(e)}\right)^{\log(c)} = e^{\log(c)} = c = |c|_{\infty}.$$

Thus for all integers $c \in \mathbf{Z}$ with $c > 1$ we have $|c|^{\alpha} = |c|_{\infty}$, which implies that $|\cdot|$ is equivalent to $|\cdot|_{\infty}$. □

Let k be any field and let $K = k(t)$, where t is transcendental. Fix a real number $c > 1$. If $p = p(t)$ is an irreducible polynomial in the ring $k[t]$, we define a valuation by

$$\left|p^a \cdot \frac{u}{v}\right|_p = c^{-\deg(p) \cdot a}, \tag{3.3}$$

where $a \in \mathbf{Z}$ and $u, v \in k[t]$ with $p \nmid u$ and $p \nmid v$.

Remark 3.4. This definition differs from the one page 46 of [Cassels-Frohlich, Ch. 2] in two ways. First, we assume that $c > 1$ instead of $c < 1$, since otherwise $|\cdot|_p$ does not satisfy Axiom 3 of a valuation. Also, we write $c^{-\deg(p)\cdot a}$ instead of c^{-a}, so that the product formula will hold.

In addition there is a a non-archimedean valuation $|\cdot|_\infty$ defined by

$$\left|\frac{u}{v}\right|_\infty = c^{\deg(u)-\deg(v)}. \tag{3.4}$$

Remark 3.5. In [Cassels-Frohlich, Ch. 2] page 46 Cassels writes $c^{\deg(v)-\deg(u)}$, which is not correct, because the product formula would not hold.

Note the (albeit imperfect) analogy between $K = k(t)$ and $\mathbf{Q}$. If $s = t^{-1}$, so $k(t) = k(s)$, the valuation $|\cdot|_\infty$ is of the type (3.3) belonging to the irreducible polynomial $p(s) = s$.

The reader is urged to prove the following lemma as a homework problem.

Lemma 3.6. *The only nontrivial valuations on $k(t)$ which are trivial on k are equivalent to the valuation (3.3) or (3.4).*

For example, if k is a finite field, there are no nontrivial valuations on k, so the only nontrivial valuations on $k(t)$ are equivalent to (3.3) or (3.4).

4 Topology

A valuation $|\cdot|$ on a field K induces a topology in which a basis for the neighborhoods of α are the *open balls*

$$B(\alpha, d) = \{x \in K : |x - \alpha| < d\}$$

for $d > 0$.

Lemma 4.1. *Equivalent valuations induce the same topology.*

Proof. If $|\cdot|_1 = |\cdot|_2^r$, then $|x-\alpha|_1 < d$ if and only if $|x-\alpha|_2^r < d$ if and only if $|x-\alpha|_2 < d^{1/r}$ so $B_1(\alpha, d) = B_2(\alpha, d^{1/r})$. Thus the basis of open neighborhoods of α for $|\cdot|_1$ and $|\cdot|_2$ are identical. □

A valuation satisfying the triangle inequality gives a metric for the topology on defining the distance from α to β to be $|\alpha - \beta|$.

Lemma 4.2. *A field with the topology induced by a valuation is a topological field, i.e., the operations sum, product, and reciprocal are continuous.*

Proof. For example (product) the triangle inequality implies that

$$|(\alpha+\varepsilon)(\beta+\delta) - \alpha\beta| \le |\varepsilon|\,|\delta| + |\alpha|\,|\delta| + |\beta|\,|\varepsilon|$$

is small when $|\varepsilon|$ and $|\delta|$ are small (for fixed α, β). □

Lemma 4.3. *Suppose two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field K induce the same topology. Then for any sequence $\{x_n\}$ in K we have*

$$|x_n|_1 \to 0 \iff |x_n|_2 \to 0.$$

Proof. It suffices to prove that if $|x_n|_1 \to 0$ then $|x_n|_2 \to 0$, since the proof of the other implication is the same. Let $\varepsilon > 0$. The topologies induced by the two absolute values are the same, so $B_2(0,\varepsilon)$ can be covered by open balls $B_1(a_i, r_i)$. One of these open balls $B_1(a,r)$ contains 0, and we see that there is $\varepsilon' > 0$ such that

$$B_1(0,\varepsilon') \subset B_1(a,r) \subset B_2(0,\varepsilon).$$

Since $|x_n|_1 \to 0$, there exists N such that for $n \geq N$ we have $|x_n|_1 < \varepsilon'$. For such n, we have $x_n \in B_1(0,\varepsilon')$, so $x_n \in B_2(0,\varepsilon)$, so $|x_n|_2 < \varepsilon$. Thus $|x_n|_2 \to 0$. □

Proposition 4.4. *If two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field induce the same topology, then they are equivalent in the sense that there is a positive real α such that $|\cdot|_1 = |\cdot|_2^{\alpha}$.*

Proof. If $x \in K$ and $i = 1, 2$, then $|x^n|_i \to 0$ if and only if $|x|_i^n \to 0$, which is the case if and only if $|x|_i < 1$. Thus Lemma 4.3 implies that $|x|_1 < 1$ if and only if $|x|_2 < 1$. On taking reciprocals we see that $|x|_1 > 1$ if and only if $|x|_2 > 1$, so finally $|x|_1 = 1$ if and only if $|x|_2 = 1$.

Let now $w, z \in K$ both nonzero and with $|w|_i, |z|_i \neq 1$. On applying the foregoing to

$$x = w^m z^n \qquad (m, n \in \mathbf{Z})$$

we see that

$$m \log |w|_1 + n \log |z|_1 \geq 0$$

according as

$$m \log |w|_2 + n \log |z|_2 \geq 0.$$

Dividing through by $\log |z|_i$, and rearranging, we see that for every rational number $\alpha = -n/m$,

$$\frac{\log |w|_1}{\log |z|_1} \geq \alpha \iff \frac{\log |w|_2}{\log |z|_2} \geq \alpha.$$

Thus

$$\frac{\log |w|_1}{\log |z|_1} = \frac{\log |w|_2}{\log |z|_2},$$

so

$$\frac{\log |w|_1}{\log |w|_2} = \frac{\log |z|_1}{\log |z|_2}.$$

Since this equality does not depend on the choice of z, we see that there is a constant c $(= \log |z|_1 / \log |z|_2)$ such that $\log |w|_1 / \log |w|_2 = c$ for all w. Thus $\log |w|_1 = c \log |w|_2$, so $|w|_1 = |w|_2^c$, which implies that $|\cdot|_1$ is equivalent to $|\cdot|_2$. □