Valuations

Dave Mendes da Costa

November 18, 2009

1 Valuations on number fields

Everyone knows about the absolute value $|x|_\infty$ of a rational number $x \in \mathbb{Q}$. This is a very useful notion, giving us a measure of the size of a number, a metric and associated topology on $\mathbb{Q}$ and ulimately a way of completing $\mathbb{Q}$ to form $\mathbb{R}$. And we all like $\mathbb{R}$.

What is perhaps less well known is that the abolute value, $|\cdot|_\infty$, is not the only way to proceed. To see this we first need to define what we want a valuation to do:

Defintion : A **valution** (or **norm**) on a ring k is a funtion $|\cdot| : k \to \mathbb{R}$ such that:
(1) $|a| \geq 0$ $\forall x \in k$ $|x| = 0 \Leftrightarrow x = 0$
(2) $|ab| = |a|\,|b|$ $\forall x, y \in k$
(3) $\exists C \in \mathbb{R}$ such that $|a| \leq 1 \Rightarrow |a + 1| \leq C$

Examples :

1. The trivial valuation, $|x|_0 = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$. If k is finite then this is the only valuation on k. In this case we may take $C = 1$.
2. The absolute value, $|\cdot|_\infty$. Here we have $C = 2$.
3. If $|\cdot|_1$ is a valuation on k and $\lambda > 0$ then $|\cdot|_2 := |\cdot|_1^\lambda$ is also a valuation on k. In this case we say that $|\cdot|_1$ and $|\cdot|_2$ are *equivalent*. Equivalence is, of course, an equivalence relation and the equivalence classes are known as *places*.

This definition is due to Artin. It is sometimes formulated with (3) replaced by the more familiar Triangle Inequality:

(3') $|a + b| \leq |a| + |b|$ $\forall a, b \in k$.

It may be shown that (3') holds if and only if (3) holds with $C = 2$. Therefore every valution is equivalent to one satisfying the triangle inequality. In the case that (3) holds with $C = 1$ we get the stronger condition:

$|a + b| \leq \max\{|a|, |b|\}$ (*Ultrametric Inequality*)

If $|a| \neq |b|$ then we get an equality. We call valuations with $C = 1$ *non-achimedian* and the others are called *archimedian*.

So far the only example of a non-arch valuation on $\mathbb{Q}$ is $|\cdot|_0$, but we can do better than that. Let p be a prime number in $\mathbb{Z}$ and $a = p^e b \in \mathbb{Q}$ where $b = \frac{m}{n}$ with $\gcd(m, n, p) = 1$. Putting $|a|_p = \frac{1}{p^e}$ and setting $|0|_p = 0$ yields a non-arch valuation on $\mathbb{Q}$ called the *p-adic valuation*.

These are essentially the only non-trivial non-arch valuations of $\mathbb{Q}$:

Theorem(Ostrowski): Every non-trivial valuation on $\mathbb{Q}$ is equivalent to either $|\cdot|_p$ for some prime p or $|\cdot|_\infty$.

We may generalise the case of $\mathbb{Q}$ to a number field k. The arch valuations come from the real embeddings and the pairs of complex embeddings with the usual valuations on $\mathbb{R}$ and $\mathbb{C}$ respectively. For the non-arch (non trivial) valuations we proceed as follows: Let $\mathfrak{P}$ be a prime ideal of k and let $x \in k^*$. Then by the theorem on uniqueness of factorisation of ideals we get that the fraction ideal (x) may be expressed as

$$(x) = \mathfrak{P}^e \prod \mathfrak{P}_i^{e_i}$$

where the product is over the remaining prime ideals of k. We may then form the $\mathfrak{P}$-*adic valuation* by putting $|x|_{\mathfrak{P}} = \frac{1}{N(\mathfrak{P})^e}$ and $|0|_{\mathfrak{P}} = 0$ where $N(\mathfrak{P})$ is the norm of $\mathfrak{P}$.

An analogue of Ostrowski's Theorem holds for number fields. We denote the places of k by M_k, the arch places by M_k^∞ and the non-arch places by M_k^0. It is worth noting that since non-arch (resp. arch) places come from prime ideals they are referred to as prime (resp. infinite) places.

Finally, since $\mathbb{Q} \subset k$ we get a valuation on $\mathbb{Q}$ from each valuation on k by restriction. It is easy to see that the arch places on k descend to the arch place on $\mathbb{Q}$ and that if $\mathfrak{P}$ is a prime ideal lieing over the rational prime p then the $\mathfrak{P}$-adic valuation on k restricts to a valuation equivalent to the p-adic valuation on $\mathbb{Q}$.

2 Completions

Recall that a complete metric space is one where every Cauchy sequence converges. We all know that $\mathbb{Q}$ is not complete with respect to $|\cdot|_\infty$ and nor is it with repect to any of the p-adic valuations. However, every metric space has a completion (a complete metric space containing k as a **dense** subspace) which is essentially the space of equivalence classes of Cauchy sequences under the equivalence relation $(a_n) \equiv (b_n) \Leftrightarrow |a_n - b_n| \to 0$ as $n \to \infty$.

The completion of $\mathbb{Q}$ with repect to $|\cdot|_\infty$ is $\mathbb{R}$ and with respect to $|\cdot|_p$ the completion is denoted $\mathbb{Q}_p$ and is called the space of *p-adic numbers*. Note that we usualy write $\mathbb{R}$ as $\mathbb{Q}_\infty$ and refer to ∞ as the *infinite prime*.

We can also complete a number field k with respect a valuation ν, and we denote the completion by k_ν.

Theorem: Let $\nu \in M_k^\infty$, then k_ν is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.

3 The structure of (discrete) complete non-arch fields

In this section k will denote an arbitary complete non-arch field with vaulation $|\cdot|$.

The p-adic numbers were invented/discovered by Hensel in order to bring the might of power series to bear in number theory. He defined them as formal Laurent series in p and later the valuation approach which we are using here developed. We shall now recover the Hensellian picture.

Lemma: Let $(a_n) \subset k$ be a sequence. Then $\sum_{n=0}^\infty a_n$ converges if and only if $a_n \to 0$ as $n \to \infty$.

Definition: Let $R = \{x \in k : |x| \leq 1\}$ and $I = \{x \in R : |x| < 1\}$. We call R the *ring of integers* of k.

Since I is a maximal ideal in R we can define the *Residue Class Field* R/I.

Note that R is indeed a ring since $|\cdot|$ is non-arch. This clearly fails in the arch case. As an example let us look at $k = \mathbb{Q}$ with $|\cdot|_p$. Here $R = \{\frac{m}{n} : p \not| n\}$ and $I = pR$. Then $R/I \cong \mathbb{Z}/p\mathbb{Z}$. It may be shown that the residue class field remains unchanged under the process of completing a field and so we have for free that the residue class field of $\mathbb{Q}_p$ is also $\mathbb{Z}/p\mathbb{Z}$.

For $\mathbb{Q}_p$ we denote R by $\mathbb{Z}_p$ and we call it the ring of *p-adic integers*. It is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

Now, the valuations we have seen take their values on a discrete set of $\mathbb{R}_{>0}$ when restricted to k^*. These values form a cyclic group with generator $q \in \mathbb{R}$, say. We call such valuations *discrete* and we shall proceed with the assumption that we are working with such a valuation. Let R and I be as above and let $\pi \in I$ be such that $|\pi|$ is maximal. Then we have that $I = (\pi)$ since $y \in I$ implies $|y| \leq |\pi|$ and so $y = x\pi$ with $|x| \leq 1$. This shows that $x \in R$ and, moreover, $y \in (\pi)$. We call π a *uniformiser* of I. (When $k = \mathbb{Q}_p$ we may take $\pi = p$.)

Let $0 \in S \subset R$ be a set of representatives of each residue class. Then we have the following:

Theorem: Let k be a complete, non-arch field with respect to a discrete valuation. Let R, I, S, π be as above. Then:

1. Let $(a_n) \subset S$ be a sequence. Then $\sum_{n=0}^{\infty} a_n \pi^n$ converges in R and, moreover, every element $r \in R$ has a unique expression in this form.
2. If $0 \neq r \in R$ then $r = \sum_{n=0}^{\infty} a_n \pi^n$ with at least one $a_n \neq 0$ and we have $|r| = |\pi|^m$ where m is the smallest integer such that $a_m \neq 0$.
3. Any $x \in k^*$ can be expressed uniquely in the form $x = \sum_{n=M}^{\infty} a_n \pi^n$ for some integer M with $a_M \neq 0$. We have that $|x| = |\pi|^M$.

When applied to $\mathbb{Q}_p$, this theorem tells us that every non-zero $x \in \mathbb{Q}_p$ can be expressed uniquely as $\sum_{n=M}^{\infty} a_n p^n$ where $a_i \in \{0, 1, \ldots, p-1\}$. This recovers Hensel's original formulation of $\mathbb{Q}_p$.

An immediate corollary is that $\mathbb{Q}_p$ is uncountable via a diagonal argument identical to the one used to show $\mathbb{R}$ is uncountable.

We end this section with a result concerning the topology of R:

Theorem: R is compact if and only if R/I is finite.

Corollary: $\mathbb{Z}_p$ is open and compact.

4 The algebraic viewpoint

So far we have taken what may be called the 'analytic approach' to the p-adic numbers. We now consider the algebraic construction of $\mathbb{Q}_p$.

Let $r \in \mathbb{Z}_p$ so we have an expression $r = \sum_{n=0}^{\infty} a_n p^n$ with $a_n \in \{0, 1, \ldots, p-1\}$. If can look at the partial sums $s_n = \sum_{k=0}^{n} a_k p^k$ then we see that they can be thought of as elements of $\mathbb{Z}/p^{n+1}\mathbb{Z}$ (Thinking of them in this way is actually quite shrewd since it takes account of the fact that the a_i are only meant to be representatives of residue classes.) Moreover we see that we have the congruence relation:

$$s_n \equiv s_{n-1} (\text{mod } p^n)$$

We may thus express r as a sequence $(\ldots, s_2, s_1, s_0)$ with the above conjugacy conditions.

Consider the sequence (*inverse system*) of abelian groups:

$$\overset{\varphi_{n+1}}{\to} \mathbb{Z}/p^{n+1}\mathbb{Z} \overset{\varphi_n}{\to} \mathbb{Z}/p^n\mathbb{Z} \overset{\varphi_{n-1}}{\to} \dots \overset{\varphi_0}{\to} \mathbb{Z}/p\mathbb{Z}$$

with $\varphi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ being the homomorphism which takes $\alpha \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ to its residue mod p^n.

We define the *inverse limit* of this sequence to be the set of all sequences $(\dots, a_2, a_1, a_0)$ with $a_n \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ and $\varphi_n(a_n) = a_{n-1}$ and denote it by $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

From our previous comments we see that $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. The algebraic construction takes the inverse limit as the definition of $\mathbb{Z}_p$ and defines $\mathbb{Q}_p$ to be its field of fractions.

5 Hasse's Principle

The p-adic numbers have a key application to the study of Diophantine equations. This is due to the fact that $\mathbb{Q}_p$ contains a copy of $\mathbb{Q}$ and so a polynomial $f \in \mathbb{Q}[X]$ can be seen as a polynomial in $\mathbb{Q}_p[X]$. If there are no solutions in $\mathbb{Q}_p$, then there cannot be any solutions in $\mathbb{Q}$. Handy. An obvious question is whether we can go the other way, that is does the existence of a solution to a Diophantine equation in every completion of $\mathbb{Q}$ (including $\mathbb{R}$) imply a solution in $\mathbb{Q}$ itself? Such equations satisfy a local-global principle, or *Hasse's Principle*. A useful tool in the study of this problem is the following:

Theorem (Hensel's Lemma): Let $f \in \mathbb{Z}[X]$, $2 \leq k \in \mathbb{Z}$, p a rational prime. Suppose that we have $r \in \mathbb{Z}$ such that $f(r) \equiv 0 (\text{mod } p^{k-1})$. Then if $f'(r) \not\equiv 0 (\text{mod } p)$ we have that there exists $\overline{r}$ such that $f(\overline{r}) \equiv 0 (\text{mod } p^k)$ and with $\overline{r} \equiv r (\text{mod} p^{k-1})$.

The importance of this theorem to us is that it allows us to lift solutions to equations in finite fields to solutions in $\mathbb{Z}_p$. Indeed, if we look at the inverse limit definition of $\mathbb{Z}_p$ we see that a solution in $\mathbb{Z}_p$ corresponds to a solution in every ring $\mathbb{Z}/p^n\mathbb{Z}$.

Hasse's Principle holds for quadratic forms (Hasse-Minkowski Theorem) but fails in general for polynomials of higher degree. A famous example is

$$3x^3 + 4y^3 + 5z^3 = 0$$

which has a non-trivial solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p but has no non-trivial solution in $\mathbb{Q}$.

6 Adèles

We have seen that we can glue together the rings $\mathbb{Z}/p^n\mathbb{Z}$ to form $\mathbb{Z}_p$. This is a dandy thing to do since we can talk about all of the rings at once in a meaningful way. But why stop there?

We define the *(ring of) Adèles* of a number field k to be $\mathbb{A}_k = \prod'_\nu k_\nu$ where $\prod'$ means that for each adle $a = (a_\nu)_\nu \in \mathbb{A}_k$ all but finitely many of the entries of a_ν for $\nu \in M_k^0$ are integers (this is a *restricted topological product*). This restriction is to ensure that the adèles form a locally compact topological group which is a key property if we want to do abstract Fourier analysis on the adèles (à la Tate).

So why do we like the adèles? Well, an immediate reason is that since we can embed k diagonally into $\mathbb{A}_k$ we can study k in all of its completions simultaneously and thus without taking any of them to be of special importance over the others. This socialist view is necessary in order to gain a unified sense algebraic number theory.

Since we can view k as lieing inside $\mathbb{A}_k$ and since k is dense in each of its completions (by definition) it seems natural to ask about the density of k in $\mathbb{A}_k$. The two key results in this area are Weak

and Strong Approximation:

Theorem (Weak Approximation): Let $|\cdot|_j$ for $1 \leq j \leq n$ be pairwise inequivalent valuations on k. Let $a_1 \ldots, a_n$ be arbitrary elements in k and let $\epsilon > 0$. Then there exists an $x \in k$ such that $|x - a_i|_i < \epsilon$ for $1 \leq i \leq n$.

Weak Approximation means that if we restrict $\mathbb{A}_k$ to finitely many places then k is dense in the restriction. This may be alternatively stated as: k is dense is $\prod_\nu k_\nu$ with the (unrestricted) product topology.

This seems to be strong evidence that k is dense in $\mathbb{A}_k$ however this is not the case. Let us look at the case $k = \mathbb{Q}$. Consider $(a_p)_p = (1, 2, 3, 5, 7, 11, 13, \ldots) \in \mathbb{A}_\mathbb{Q}$. Now we cannot have $b \in \mathbb{Q}$ is such that $|b - a_p|_p < 1$ for every $p \in M_\mathbb{Q}$ since $|b - a_p|_p = \max\{|a_p|_p, |b|_p\} = 1$ for almost all p. A similar argument shows in fact that $\mathbb{Q}$ is discrete in $\mathbb{A}_\mathbb{Q}$. The best we can get is:

Theorem (Strong Approximation): Let P be a finite set of non-arch places on a number field k. Let $\epsilon > 0$ and $a_\nu \in k_\nu$ for each $\nu \in P$ be arbitrarily chosen. Then there is an $x \in k$ such that $|x - a_\nu|_\nu < \epsilon$ for each $\nu \in P$ and $|x|_\nu \leq 1$ for each non-arch place $\nu \notin P$. Further, if $a_i \in \mathcal{O}_\nu$ for each $\nu \in P$ then $x \in \mathcal{O}_k$.

Corollary (Alternate Statement of S.A.): Let $\mathbb{A}_{k,\nu_0}$ be $\mathbb{A}_k$ restricted to all places except ν_0. Then k is dense in $\mathbb{A}_{k,\nu_0}$.

So we have weak and strong approximation for number fields k. The real meat of these notions comes though when we look at varieties defined over k. Our discussion so far can be interpretted as looking at the affine line $X(\overline{k}) = \{(x, y) \in \overline{k}^2 : y = 0\}$ and the question of the density of $X(k)$ in $X(\mathbb{A}_k)$. In this case we get both weak and strong approximation.

Weak approximation and the Hasse principle are related: if X is a variety defined over k and $X(k_\nu) \neq \emptyset$ for all $\nu \in M_k$ then the density of $X(k)$ in $X(\prod_\nu k_\nu)$ (where $\prod_\nu k_\nu$ has the unrestricted product topology) implies that $X(k) \neq \emptyset$ since the empty set is not dense in a non-empty set. The failure of the Hasse Principle on some varieties imples that weak approximation is not a trivial concept.

7 Extending valuations

It is clear that if L/k is an extension of number fields then every valuation on L restricts to a valuation on k, but given a valuation on k how far can we extend it to a valuation on L? It is obvious how the arch valuations extend so let us concentrate on the non-arch ones.

Proposition: Let L/k be a finite field extension on degree n and suppose theat k is equipped with a non-arch valuation $|\cdot|_1$ with respect to which k is complete. Then $|\cdot|_1$ extends to a unique valuation $|\cdot|_2$ on L given by

$$|x|_2 = \left|N_{L/k}(x)\right|_1^{\frac{1}{n}}$$

This proposition clearly fails when k is not complete since if $k = \mathbb{Q}$ then $L = \mathbb{Q}(i)$ is a finite extension of $\mathbb{Q}$ but we have $(2) = (1 + i)(1 - i)$ in $\mathbb{Z}[i]$ and thus both the $(1 + i) - adic$ and $(1 - i) - adic$ valuation extend the $2 - adic$ valuation.

Let us suppose that k is equipped with a non-arch valuation $|\cdot|$ which does not make it complete. Denote the completion of k by $\widehat{k}$. Then since L and $\widehat{k}$ both contain k we may consider $L \otimes_k \widehat{k}$. Now there is an $a \in L$ such that $L = k(a)$ and this has minimum polynomial $f(x) \in k[x]$. Thus we have $L = \frac{k[x]}{(f(x))}$. This polynomial may well become irreducible over $\widehat{k}$ so that $f = g_1 \ldots g_r$ with $g_i \in \widehat{k}[x]$. In which case we have that

$$L \otimes_k \widehat{k} \cong \oplus_r^{i=1} \frac{\widehat{k[x]}}{(g_i(x))} =: \oplus_{i=1}^r \widehat{L}_i$$

With a bit of work we are able to prove:

Theorem: Let L/k be a finite extension and $|\cdot|$ be a non-arch valuation on k. Then there are r non-equivalent extensions of $|\cdot|$ to L (with r as above). Moreover, if $|\cdot|_i$ is such an extension and L_i is the completion of L with respect to it then $L_i \cong \widehat{L}_i$ (after a suitable reordering).

A corollary of this result is that if $k/\mathbb{Q}$ is a number field and $\mathfrak{P}$ is a prime ideal of k lieing over the rational prime p then $k_{\mathfrak{P}}$ is a finite extension of $\mathbb{Q}_p$ of degree at most $[k : \mathbb{Q}]$.