Introduction to Rings and Modules

Lecture 21, Monday June 26 2023

Ari Feiglin

Definition 21.0.1:

Suppose R is an integral domain, then a **absolute value** on R is a function

$$|\cdot|\colon R \longrightarrow \mathbb{R}_{\geq 0}$$

which satisfies

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

(2) $|a \cdot b| = |a| \cdot |b|$ for every $a, b \in R$.

(3) $|a + b| \leq |a| + |b|$ for every $a, b \in R$.

This is a generalization of the concept of an absolute value in $\mathbb{R}$, or the modulus of $\mathbb{C}$. Of course both of these are valuations on these fields.
Another example would be

$$|a| = \begin{cases} 0 & a = 0 \\ 1 & a \neq 0 \end{cases}$$

We will focus now on absolute values over fields. We can construct an absolute value over the field $\mathbb{Q}$, as follows: let p be prime, then of course $|0|_p = 0$. Then suppose $0 \neq a \in \mathbb{Q}$, $a = \frac{m}{n}$. Then $m = p^b m'$ and $n = p^a n'$ where m' and n' are coprime with p, so

$$a = p^{b-c}\frac{m}{n}$$

and so we define

$$|a|_p = p^{c-b}$$

Or in other words, if

$$a = p^d \frac{m}{n}$$

where p is coprime with m and n and $d \in \mathbb{Z}$, then $|a|_p = p^{-d}$.
This is well-defined since if $a = \frac{m}{n} = \frac{x}{y}$ then suppose $m = p^d m'$ and $n = p^{d'} n'$ and $x = p^e x'$ and $y = p^{e'} y'$ then

$$p^{d-d'}\frac{m'}{n'} = p^{e-e'}\frac{x'}{y'}$$

and so

$$p^{d-d'} m' y' = p^{e-e'} x' n'$$

and since m', n', x', and y' are all coprime with p, we must have $d - d' = e - e'$ which means the absolute value is well-defined.

Definition 21.0.2:

The absolute value defined above is called the **p-adic absolute value**.

Proposition 21.0.3:

The p-adic absolute value is indeed an absolute value.

Proof:

Obviously $|a| = 0_p$ if and only if $a = 0$, and the absolute value is non-negative. Now suppose

$$a = p^d \frac{m_1}{n_1}, \quad b = p^e \frac{m_2}{n_2}$$

and so

$$ab = p^{d+e} \frac{m_1 m_2}{n_1 n_2}$$

and since $m_1 m_2$ and $n_1 n_2$ are still coprime with p, we have

$$|ab|_p = p^{-d-e} = p^{-d} p^{-e} = |a|_p |b|_p$$

as required.
Finally, for the triangle inequality, suppose without loss of generality that $d \leq e$. So

$$a + b = p^d \left(\frac{m_1}{n_1} + p^{e-d} \frac{m_2}{n_2} \right) = p^d \frac{m_1 n_2 + p^{e-d} m_2 n_1}{n_1 n_2} = p^d \frac{m_3}{n_1 n_2}$$

Now suppose $m_3 = p^f m_4$, then we have

$$a + b = p^{d+f} \frac{m_4}{n_1 n_2}$$

which means that

$$|a + b|_p = p^{-d-f} \leq p^{-d} = \max\{p^{-d}, p^{-e}\} = \max\left\{ |a|_p, |b|_p \right\} \leq |a|_p + |b|_p$$

as required. ■

We actually have proven a stronger property of the p-adic absolute value, that

$$|a + b|_p \leq \max\left\{ |a|_p, |b|_p \right\}$$

Such a property is called the *strong triangle inequality*.

Proposition 21.0.4:

Suppose R is an integral domain with an absolute value, then $|1_R| = 1$.

Let $0 \neq a \in R$ then $|a| \neq 0$ and $|a| = |a \cdot 1_R| = |a||1_R|$ and since $\mathbb{R}$ is a field, we have $|1_R| = 1$ as required.

Proposition 21.0.5:

Suppose $b \in R$ is invertible, then $\left|b^{-1}\right| = |b|^{-1}$.

Since $|b| \cdot \left|b^{-1}\right| = \left|bb^{-1}\right| = |1| = 1$, since $\mathbb{R}$ is a field we have $\left|b^{-1}\right| = |b|^{-1}$.

Proposition 21.0.6:

$|-a| = |a|$

Since $1 = |-1| \cdot |-1|$, we have that $|-1|$ is a unit in $\mathbb{R}_{\geq 0}$, meaning $|-1| = 1$.
Notice that if $n \in \mathbb{Z}$ such that $p \nmid n$, then n is coprime with p and thus $|n|_p = p^{-0} = 1$. And on the flipside, $|p^n| = p^{-n}$.
So let $\varepsilon > 0$ and d be the smallest integer such that $p^{-d} < \varepsilon$, thus p^{-d} is the largest exponent of p less than ε,

$$|a - b|_p < \varepsilon$$

if and only if $a - b = p^c \frac{m}{n}$ where $p^{-c} < \varepsilon$ and so $p^{-c} < p^{-d}$, meaning

$$|a - p|_p < \varepsilon \iff |a - b|_p < p^{-d}$$

Note 21.0.7:

If R is an integral domain with an absolute value, then we can define a metric on it by

$$d(a,b) = |a-b|$$

Obviously $d(a,b) \geq 0$ and is zero only when $a=b$, and it is symmetric. And finally

$$d(a,b)+d(b,c) = |a-b|+|b-c| \geq |(a-b)+(b-c)| = |a-c| = d(a,c)$$

Thus an absolute value defines a metricizable topology on R, generated by the basis of balls $B_\varepsilon(a)$.

Definition 21.0.8:

Two absolute values on the ring R are **equivalent** if they define the same topology on R.

Proposition 21.0.9:

Two absolute values on R, $|\cdot|_1$ and $|\cdot|_2$, are equivalent if and only if there exists an $n \in \mathbb{Z}$ such that for every $a \in R$, $|a|_1 = |a|_2^n$.

Proof:

Let us show that if the equality holds, they are equivalent. This is because

$$|a-b|_1 < \varepsilon \iff |a-b|_2^n < \varepsilon \iff |a-b|_2 < \varepsilon^{1/n}$$

and thus

$$B_\varepsilon^1(a) = B_{\varepsilon^{1/n}}^2(a)$$

Now suppose the two absolute values are equivalent. Now suppose that $a \in R$, then for any $\varepsilon > 0$ there exists a $\delta > 0$ such that $|a-b|_1 < \varepsilon$ if and only if $|a-b|_2 < \delta$.

Definition 21.0.10:

Let R be a ring, then for $n \in \mathbb{N}$, let $n_R = 1_R + \cdots + 1_R$ (n times). If $n \in \mathbb{Z}$ and $n < 0$ then $n_R = (-n)_R$.

Note that the unique ring homomorphism $\varphi\colon \mathbb{Z} \longrightarrow R$ is given by $\varphi(n) = n_R$.

Definition 21.0.11:

If R is an integral domain with an absolute value $|\cdot|$, the absolute value is **non-Archimedean** if

$$\{|n_R| \mid n \in \mathbb{N}\} \subseteq \mathbb{R}_{\geq 0}$$

is bounded from above.
The absolute value is **Archimedean** if it is not non-Archimedean.

Proposition 21.0.12:

An absolute value on a ring R is non-Archimedean if and only if it satisfies the strong triangle inequality.

Proof:

Suppose the strong triangle inequality is satisfied, then inductively, we show that $|n_R| \leq 1$. For $n=1$ this is trivial, and otherwise

$$|(n+1)_R| = |n_R + 1_R| \leq \max\{|n_R|, |1_R|\} \leq \max\{1,1\} = 1$$

So the absolute value is non-Archimedean.
Now suppose the absolute value is non-Archimedean, suppose $M > 0$ is a bound for $\{|n_R|\}$. Let $a, b \in R$ and suppose

$|b| \leq |a|$. Then let $k \in \mathbb{N}$, so

$$\left|(a+b)^k\right| = \left|\sum_{i=0}^{k} \binom{n}{i}_R a^i b^{k-i}\right| \leq \sum_{i=0}^{k} M|a|^i|b|^{k-i} \leq (k+1)M|a|^k$$

Thus by taking the k-th root from both sides, we get

$$|a+b| \leq (k+1)^{1/k} \cdot M^{1/k} \cdot |a|$$

and then we can let $k \to \infty$, and $(k+1)^{1/k}$, $M^{1/k} \to 1$ and so

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

Thus $|\cdot|$ satisfies the strong triangle ienquality, as required. ■

Note then that the p-adic metric is non-Archimedean (this is not hard to prove directly).

Theorem 21.0.13 (Ostrowski's Theorem):

Every non-trivial absolute value on $\mathbb{Q}$ is equivalent either to a p-adic absolute value $|\cdot|_p$ or the normal absolute value, denoted $|\cdot|_\infty$.

Proof:

Suppose $|\cdot|$ is a non-trivial absolute value on $\mathbb{Q}$. If the absolute value is non-Archimedean, then it must satisfy the strong triangle inequality, and thus

$$|n| \leq \max\{|1|, \ldots, |1|\} = |1|$$

for every $0 \neq z \in \mathbb{Z}$. Let

$$I = \{n \in \mathbb{Z} \mid |n| < 1\}$$

then $I \trianglelefteq \mathbb{Z}$ is a prime ideal. $I \neq \mathbb{Z}$ since $|1| = 1$, and $0 \in I$. I is an ideal since if $a \in \mathbb{Z}$ and $n \in I$ then $|an| = |a||n| \leq |n| < 1$ so $an \in I$. And if $a, b \in I$ then $|a+b| \leq \max\{|a|, |b|\} < 1$ since the absolute value satisfies the strong triangle inequality. Now suppose $nm \in I$ then $|nm| = |n||m| < 1$. Since $|n|, |m| \leq 1$, if neither of them are in I then $|n|, |m| = 1$ and so $|nm| = 1$ in contradiction.
We will show that $I \neq (0)$. If $I = (0)$ then for every $\frac{a}{b} \in \mathbb{Q}$, we have that $\left|\frac{a}{b}\right| = \left|ab^{-1}\right| = |a||b|^{-1} = 1$, which is 1 if $a \neq 0$ and 0 if $a = 0$, meaning the absolute value is trivial, in contradiction.
Thus $I = p\mathbb{Z}$ for some prime p. We claim that the absolute value is equivalent to the p-adic absolute value. So we have that for every prime $q \neq p$, $q \notin I$ and thus $|q| = 1$. So suppose $n \in \mathbb{N}$, and so $n = p^d \cdot p_1^{n_1} \cdots p_k^{n_k}$ and so

$$|n| = |p|^d \cdot |p_1|^{n_1} \cdots |p_k|^{n_k} = |p|^d$$

And in general if $\frac{m}{n} \in \mathbb{Q}$, where $m = p^d m'$ and $n = p^{d'} n'$ then we have $|m| = |p|^d$ and $|n| = |p|^{d'}$ and so

$$\left|\frac{m}{n}\right| = |p|^{d-d'}$$

Now we know that

$$\left|\frac{m}{n}\right|_p = p^{d'-d}$$

Let $|p| = p^{-s}$ (or in other words $s = -\log_p |p|$)

$$\left|\frac{m}{n}\right| = \left(p^{-s}\right)^{d-d'} = \left(p^{d'-d}\right)^s = \left|\frac{m}{n}\right|_p^s$$

meaning the absolute value is equal to the the p-adic absolute value, raised to the sth power, which we showed means they are equivalent.