Absolute Values and p-adics

LA Math Circle

April 3, 2012

1 Absolute Values

1.1 Definitions

Definition 1. An *absolute value* on $\mathbb{Q}$ is a function $|\cdot| : \mathbb{Q} \to \mathbb{R}$ satisfying:

(i) $|x| \geq 0$ for all $x \in \mathbb{Q}$;

(ii) $|x| = 0$ if and only if $x = 0$;

(iii) $|xy| = |x||y|$ for all $x, y \in \mathbb{Q}$;

(iv) $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{Q}$.

Definition 2. Let p be a prime. For any $0 \neq x \in \mathbb{Q}$ we can write $x = p^v \frac{a}{b}$ for $a, b, v \in \mathbb{Z}, a \neq 0 \neq b$ and $p \nmid a, p \nmid b$. We call v the *p-adic valuation of x*, denoted $v_p(x)$.

Definition 3. Let p be a prime. We define a function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ by

$$|x|_p = \begin{cases} \left(\frac{1}{p}\right)^{v_p(x)} & x \neq 0 \\ 0 & x = 0. \end{cases}$$

This function is called the *p-adic absolute value*.

1.2 Exercises

1. Decide which of the four axioms of an absolute value are satisfied by each of the following functions.

   (a) $f(x) = x$

   (b) $f(x) = e^x$

   (c) $f(x) = x^2$

   (d) $f(x) = 100|x|$

   (e) $f(x) = \sqrt{x}$

   (f) $f(x) = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$

2. Let $x \in \mathbb{Q}$. Show that for ANY absolute value $|\cdot|$ we have $|1| = 1, |-x| = |x|$, and if $x \neq 0$ then $|1/x| = 1/|x|$.

3. Fill in the following table.

x	$v_2(x)$	$v_5(x)$	$v_{11}(x)$	$\|x\|_2$	$\|x\|_5$	$\|x\|_{11}$
1						
2						
110						
100^{27}						
$2^3 5^{14} 11^2$						
$2^a 5^b 11^c$						
$5/2$						
$22/5$						
$2/11$						

4. Verify that $|\cdot|_p$ is an absolute value.

5. For any $n \in \mathbb{Z}$ define $|\cdot|_n$ analogously to $|\cdot|_p$. Does this define an absolute value on $\mathbb{Q}$? Why or why not?

6. Can you find any other absolute values on $\mathbb{Q}$? If so, are they related to any of the absolute values defined above? How?

7. If $|\cdot|_1$ is an absolute value and we define $|\cdot|_2$ by $|x|_2 = |x|_1^c$ for some constant $c \geq 0$, is $|\cdot|_2$ necessarily an absolute value? Can you find examples where $|\cdot|_2$ is an absolute value? Can you find examples where $|\cdot|_2$ is not an absolute value?

2 Cauchy sequences and Completions

2.1 Definitions

Definition 4. A sequence of rational numbers $\{x_n\}$ is a *Cauchy sequence with respect to an absolute value* $|\cdot|$ if, for any $\varepsilon > 0$ there is some (large) N such that whenever $n, m \geq N$ we have $|x_n - x_m| < \varepsilon$.

Definition 5. There is a theorem that tells us that every element $\alpha \in \mathbb{Q}_p$ can be written uniquely in the form

$$\alpha = \sum_{i=k}^{\infty} d_i p^i,$$

where $k \in \mathbb{Z}$ (could be positive or negative) and $0 \leq d_i \leq p-1$ for all i. This expansion is called the *p-adic expansion* of α.

Definition 6. Two absolute values $|\cdot|_1, |\cdot|_2$ on $\mathbb{Q}$ are *equivalent* if there is a constant $c > 0$ such that $|x|_1 = |x|_2^c$ for all $x \in \mathbb{Q}$.

2.2 Exercises

1. Determine which of the following sequences $\{x_n\}$ are Cauchy with respect to each nontrivial absolute value on $\mathbb{Q}$.

   (a) $x_n = \frac{1}{2^n}$

   (b) $x_n = (-1)^n$

   (c) $x_n = p^n$ for a *fixed* prime p

   (d) $x_n = n$

   (e) $x_n = \begin{cases} n & n \text{ is a power of 10} \\ 1 & \text{otherwise} \end{cases}$

   (f) $x_n = \begin{cases} 1/n & n \text{ is a power of 10} \\ 0 & \text{otherwise} \end{cases}$

2. Show that if $|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values and $\{x_n\}$ is a Cauchy sequence with respect to $|\cdot|_1$, then $\{x_n\}$ is also a Cauchy sequence with respect to $|\cdot|_2$.

3. Can you find a sequence that is a Cauchy sequence with respect to every absolute value? Can you find a non-constant sequence that is a Cauchy sequence in at least two non-equivalent absolute values?

4. (Product formula) Show that for any $0 \neq x \in \mathbb{Q}$ we have

$$|x| \prod_p |x|_p = 1,$$

where $|\cdot|$ is the usual absolute value on $\mathbb{Q}$ and the product ranges over all prime numbers p. (Hint: Write the numerator and denominator of x as products of distinct prime powers.)

5. Find the expansions of the following rational numbers in $\mathbb{Q}_p$ for the specified prime p.

   (a) 20 in $\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5$

   (b) 1/2 in $\mathbb{Q}_2, \mathbb{Q}_3$

   (c) -1 in $\mathbb{Q}_5$

   (d) -3 in $\mathbb{Q}_5$

   (e) 6! in $\mathbb{Q}_3$

   (f) 1/3! in $\mathbb{Q}_3$

   (g) 6! - 4 in $\mathbb{Q}_3$

6. Is there an element $\alpha \in \mathbb{Q}_3$ such that $\alpha^2 = -1$?

3 Solutions to polynomial equations and Hensel's Lemma

3.1 Definitions and Theorems

Definition 7. Let $a, b \in \mathbb{Q}_p$ such that $|a|_p, |b|_p \leq 1$. For any $n \geq 1$ we say that a *is congruent to* b *modulo* p^n, denoted $a \equiv b \pmod{p^n}$, if $|a - b|_p \leq 1/p^n$.

Theorem 1 (Hensel's Lemma)**.** *Let* $f(x)$ *be a polynomial with integer coefficients. Let* $\alpha_0 \in \mathbb{Q}_p$ *such that* $|\alpha|_p \leq 1$ *and* $f(\alpha_0) \equiv 0 \pmod{p}$ *and* $f'(\alpha_0) \not\equiv 0 \pmod{p}$*. Then there is a unique element* $\alpha \in \mathbb{Q}_p$ *such that* $f(\alpha) = 0$ *and* $\alpha \equiv \alpha_0 \pmod{p}$*. Furthermore,* $|\alpha|_p \leq 1$*.*

3.2 Exercises

1. As a review of modular arithmetic, compute the following:

   (a) $35 + 98 - 144 \pmod{11}$

   (b) $2^{100} \pmod{7}$

   (c) $1/4 \pmod{5}$

   (d) $1/7 \pmod{2}$

   (e) $-37 + 1/6 \pmod{17}$

2. Determine if the following polynomials have a root in the specified $\mathbb{Q}_p$.

   (a) $f(x) = x^2 - 2$ over $\mathbb{Q}_5, \mathbb{Q}_7$

   (b) $f(x) = x^3 - 7x + 3$ over $\mathbb{Q}_3, \mathbb{Q}_7$

   (c) $f(x) = x^2 + x + 1$ over $\mathbb{Q}_2, \mathbb{Q}_3$

   (d) $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}_7$

3. For which p does $\mathbb{Q}_p$ have an element α such that $\alpha^2 = -1$?

4. Suppose we have an element $x \in \mathbb{Q}$ with the property that for every prime p there is an element $\alpha_p \in \mathbb{Q}_p$ such that $\alpha_p^2 = x$. Is there necessarily some $a \in \mathbb{Q}$ such that $a^2 = x$? Why or why not? If not, can you change the statement so that it becomes true? Prove your result.

5. An element $u \in \mathbb{Q}_p$ is called a *p-adic unit* if $|x|_p = 1$. Describe the p-adic expansion of a p-adic unit.

6. Find a necessary and sufficient condition on the p-adic expansion of a p-adic unit u to ensure that u is a square in $\mathbb{Q}_p$.

7. Does $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ have a root over $\mathbb{Q}_p$? (Hint: What do you get when you divide $x^p - 1$ by $x - 1$? You may use Fermat's Little Theorem that for any integer a such that $p \nmid a$ we have $a^p \equiv a \pmod{p}$. If you finish, try to prove Fermat's Little Theorem.)