THE p-ADIC SOLENOID

NEEL MURTHY

1. Definitions and examples

We'll start with some preliminary definitions. See [4] and [6] for more information about them.

Definition 1.1. A *group* is a set S, closed under a binary operation $*$, satisfying the following axioms:

(1) Associativity of $*$; for all $a, b, c \in S$,
$$a * (b * c) = (a * b) * c$$
(2) Existence of identity element; there exists an $e \in S$ such that for all $x \in S$,
$$e * x = x * e = x$$
(3) Existence of inverses; for every $a \in S$, there exists an $a^{-1} \in S$ such that
$$a * a^{-1} = a^{-1} * a = e$$

Definition 1.2. An *abelian group* is a group $(S, *)$ such that $*$ is also commutative; for all $a, b \in S$,
$$a * b = b * a$$

Example. Common examples of abelian groups are $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, together with addition.

Definition 1.3. Let G be a group and let H be a subgroup of G. Then the cosets of H form G/H, the *quotient group* of G over H.

Example. The quotient group $\mathbb{Z}/2\mathbb{Z}$ can be thought of as $\{0, 1\}$ because the cosets of $2\mathbb{Z}$ are $0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

Definition 1.4. A *ring* is a set R with two binary operations $+$ and $*$ such that

(1) $(R, +)$ is an abelian group.
(2) $*$ is associative
(3) The left and right distributive laws hold:
$$a * (b + c) = a * b + a * c$$
$$(b + c) * a = b * a + c * a$$

Definition 1.5. Consider an inverse system with algebraic objects $(A_i)_{i \in I}$. Suppose we have a family of maps $f_{ij} : A_i \to A_j$ such that $f_{ik} = f_{ij} \circ f_{jk}$. Then the *inverse limit* of the system is
$$A = \{(a_1, a_2, a_3, \dots) \in \prod_{i \in I} A_i : f_{ij}(a_i) = a_j \forall i, j \in I\}$$

Example. There is one inverse limit, in particular, that we should be familiar with: $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$. Analogously, as we will learn, $\varprojlim_n \mathbb{R}/p^n\mathbb{Z} = S_p$.

Definition 1.6. Let $(A, *)$ and $(B, *')$ be two algebraic structures with binary operations. A *homomorphism* is a mapping $\phi : A \to B$ such that
$$\phi(x * y) = \phi(x) *' \phi(y).$$
If this mapping is bijective, it is called an *isomorphism.*

Proposition 1.7. *$\mathbb{R}/\mathbb{Z}$ under addition is isomorphic to the unit circle $C = \{z \in \mathbb{C} : |z| = 1\}$ under multiplication.*

Date: June 12, 2018.

Proof. To prove these two structures are isomorphic, we find a function that satisfies the properties in the above definition. Such a function is $\phi(x) = e^{2\pi i x}$. Since the domain of ϕ is $\mathbb{R}/\mathbb{Z}$, each x maps to a different element of C. Thus,

$$\phi(x) = \phi(y) \Longrightarrow x = y.$$

So ϕ is injective. Furthermore, C can be rewritten as $C = \{x \in \mathbb{C} : e^{ix}\}$. Therefore ϕ is surjective, and, as a result, bijective. Finally,

$$e^{2i(x+y)} = e^{2ix}e^{2iy}$$

establishing that ϕ is an isomorphism. ∎

Remark 1.8. Going forward, we shall continue to use C to denote the unit circle.

Definition 1.9. A topological space X is *connected* if there cannot exist nonempty open subsets Y and Z of X such that $Y \cup Z = X$ and $Y \cap Z = \varnothing$.

Definition 1.10. A subspace A of a topological space X is *compact* if every open cover of A has a finite subcover i.e. for every collection of open sets $\{U_i\}_{i \in I}$ such that $\bigcup_{i \in I} U_i \supseteq X$, there exists a finite set $J \subseteq I$ such that $\bigcup_{i \in J} U_i \supseteq X$.

Example. According to the Heine Borel Theorem, any closed and bounded set on $\mathbb{R}$ is compact. Furthermore any interval on $\mathbb{R}$ is connected. As we will learn, S_p is a connected *and* compact.

2. Models of the p-adic solenoid

To describe the p-adic solenoid (which we shall denote S_p), we often use models to make it helpful in different contexts. Here are a few:

$$S_p = \{(s_0, s_1, s_2, s_3, \dots) \in C^{\mathbb{N}} : s_i = s_{i+1}^p\}$$
$$S_p = \{(s_0, s_1, s_2, s_3, \dots) \in (\mathbb{R}/\mathbb{Z})^{\mathbb{N}} : s_i = ps_{i+1}\}$$
$$S_p = \varprojlim_n \mathbb{R}/p^n\mathbb{Z} = \{(s_0, s_1, s_2, s_3, \dots) \in \prod_n \mathbb{R}/p^n\mathbb{Z} : s_i \equiv s_{i+1} \pmod{p^i}\}$$

where we define real numbers a and b to be congruent modulo m (we denote this as $a \equiv b \pmod{m}$, as in the convention with integers) if and only if $m|(a-b)$. [1] [3]

As a result of the isomorphism we proved in Proposition 1.9, the first two definitions of the solenoid are equivalent; they only differ in names. This can be very helpful; the first definition clearly demonstrates that the p-adic solenoid is an inverse limit of circles. However, for the most part, both definitions have the same information. For any given element of S_p, if you find s_n, you can find s_i for $i < n$. Furthermore, there are p choices for s_{n+1}, p^2 choices for s_{n+2}, p^3 choices for s_{n+3}, and so on. Finally, we must note that there are uncountably many elements of S_p, as each element of each tuple is selected from the interval $[0, 1)$. Useful as the first two definitions are, we shall opt to use the third one in order to describe how S_p relates to other algebraic objects. [3]

As a consequence of definition 3, the surjective homomorphisms $f_n : S_p \to \mathbb{R}/p^n\mathbb{Z}_p$ exist for $n \geq 0$. Furthermore, we have an injective homomorphism $f : \mathbb{R} \to S_p$ and surjective homomorphisms from $\mathbb{R}$ to each of the $\mathbb{R}/p^n\mathbb{Z}$'s. We summarize this in a commutative diagram, where dashed arrows denote injection and filled arrows denote surjection. [5]

$$\begin{tikzcd}
 & & & & \mathbb{R} \arrow[d, dashed] \arrow[ddlll] \arrow[ddll] \arrow[ddl] \arrow[ddr] \arrow[ddrr] & & \\
 & & & & S_p \arrow[dlll] \arrow[dll] \arrow[dl] \arrow[dr] \arrow[drr] & & \\
\cdots \arrow[r] & \mathbb{R}/p^n\mathbb{R} \arrow[r] & \mathbb{R}/p^{n-1}\mathbb{R} \arrow[r] & \mathbb{R}/p^{n-2}\mathbb{R} \arrow[r] & \cdots \arrow[r] & \mathbb{R}/p\mathbb{Z} \arrow[r] & \mathbb{R}/\mathbb{Z}
\end{tikzcd}$$

What does this all tell us? Apart from all the mappings, it gives us a coherent system of residue classes whereby we can classify any element of S_p: we can describe any element $x \in S_p$ as a x_0 modulo 1, x_1 modulo p, x_2 modulo p^2, and so on, such that x_m is congruent to x_n modulo p^n whenever $m > n$ [6].

3. Properties of the solenoid and its elements

We have investigated how to define the p-adic soleniod, and we have looked at how it maps between other algebraic objects. Now, we're going to establish some properties of the group itself.

Proposition 3.1. *Every element of S_p can be uniquely formed by an element of $\mathbb{Z}_p$ and a real number on the interval $[0,1)$. [2] [5]*

Proof. First, note that there exists a subset of S_p isomorphic to $\mathbb{Z}_p$. This is because S_p has a surjective homomorphism to $\mathbb{R}/p^n\mathbb{Z}$ for $n \geq 0$. It follows that S_p has a surjective mapping to $\mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$, since for each n, $\mathbb{Z}/p^n\mathbb{Z} \subset \mathbb{R}/p^n\mathbb{Z}$. Hence, we can represent any element of $\mathbb{Z}_p$ by mapping to an integer in $\mathbb{R}/p^n\mathbb{Z}$ for $n \geq 1$ and to 0 in $\mathbb{R}/\mathbb{Z}$.

Now, take any $z \in S_p$. Suppose $z \equiv r \pmod 1$, where we take $0 \leq r < 1$. Then $z - r \equiv 0 \pmod 1$, and as a result $z - r \in \mathbb{Z}_p$. Thus we may write

$$z = x + r,$$

where $x \in \mathbb{Z}_p$ and $r \in [0,1)$. The proof of uniqueness is straightforward: let

$$z = x + r = x' + r' \tag{1}$$

where both $x \neq x'$ and $r \neq r'$. Since $r \neq r'$, then $r - r' \not\equiv 0 \pmod 1$, a contradiction. So in order for (1) to hold, we must have $r = r'$, and in turn, this forces $x = x'$. ∎

The form in which we wrote elements of S_p in the previous proposition tells us that we cannot use the p-adic metric. To see this, note that we can represent any element of S_p in the following base-p expansion:

$$z = \sum_{n=-\infty}^{\infty} a_n p^n = \ldots a_{-2}p^{-2} + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \ldots \tag{2}$$

where $a_i \in \{0, 1, 2, \ldots, p-1\}$. In order for z to be a representable quantity, we need the above series to converge in not only one direction, but *both* directions. This is just not possible, as $\lim_{n\to-\infty} d_p(a_n p^n, a_{n+1}p^{n+1}) = \infty$.

To fix the problem we introduce a new metric. Take two elements from S_p, x and y. Let $x - y = n + \xi$, where $n \in \mathbb{Z}_p$ and $\xi \in [0,1)$. Then $y - x = (-n-1) + (1-\xi)$, where $-n-1 \in \mathbb{Z}_p$ and $1 - \xi \in [0,1)$, and

$$d(x,y) = \min\{\ell(x-y), \ell(y-x)\}$$
$$\ell(x-y) = \max\{|n|_p, \xi\}$$
$$\ell(y-x) = \max\{|-n-1|_p, 1-\xi\}$$

This setup allows (2) to converge in both directions, as we use the p-adic metric for the integer terms, and the Euclidean metric for the terms between 0 and 1. In both directions, the terms get closer and closer together. Now we can use the form presented in (2) to describe the elements of S_p. [2]

But there is a problem with this form, however—it loses uniqueness. Note the following proposition:

Proposition 3.2. *In S_2, we have $0 = \ldots 11111.11111\ldots$*

Proof. We write $a = \ldots 11111$ and $b = 0.11111\ldots$ and sum the two.

$$\begin{aligned}
a &= \cdots + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 1 \\
&= \cdots + (2-1)2^4 + (2-1)2^3 + (2-1)2^2 + (2-1)2 + (2-1) \\
a + 1 &= 0 \\
a &= -1 \\
b &= 1\cdot 2^{-1} + 1\cdot 2^{-2} + 1\cdot 2^{-3} + \cdots \\
&= \frac{\frac{1}{2}}{1-\frac{1}{2}} \\
&= 1
\end{aligned}$$

Hence, $\ldots 11111.11111\cdots = a + b = 0$. ∎

Owing to Proposition 3.2, it would be most preferable to rewrite $z = x + r$ as $z = (x, r)$, since x and r are unique. This is acceptable, as the product $\mathbb{Z}_p \times [0, 1)$, with the metric defined above, is algebraically and topologically equivalent to S_p. [2]

We conclude our investigation of S_p by examining some properties of the object itself. One can think of the p-adic solenoid as gluing the real numbers together with the p-adic integers in order to make them continuous. By doing so, we encounter an object S_p, that can represent any element of $\mathbb{R}$, $\mathbb{Z}_p$, and $\mathbb{Q}_p$. It can represent e; this was a glaring deficiency of $\mathbb{Q}_p$. On the other hand, we lose multiplication, as S_p is an abelian group, rather than a ring. So for the sake of performing operations, there are probably better sets to work with.

But S_p still has some useful topological properties. For one thing, it is compact. We prove a second property below. This proof comes from [5], and it shall finish our exploration of the p-adic solenoid.

Proposition 3.3. *S_p is a connected topological space. [5]*

Proof. We utilize the fact that if A is a connected topological space, and $A \subset B \subset \overline{A}$, then B is connected as well. Define $A = \{(x, \xi) \in S_p : x + \xi \in \mathbb{R}, x \in \mathbb{Z}_p, \xi \in [0, 1)\}$. Then we have $A \subset S_p \subset \overline{A}$. It follows that S_p is a connected topological space. ∎

References

[1] Peter Becker-Kern. Explicit representation of roots on p-adic solenoids and non-uniqueness of embeddability into rational one-parameter subgroups. *Proceedings of the Indian Academy of Science*, 2006.

[2] D.V. Chistyakov. Fractal geometry for images of continuous map of p-adic numbers and p-adic solenoids into euclidean spaces. *Theoretical and Mathematical Physics*, 1996.

[3] Paul Garrett. Solenoids, September 2010.

[4] John B. Raleigh. *A first course in abstract algebra*. Addison-Wesley, 2003.

[5] Alain M. Robert. *A Course in p-adic Analysis*. Springer, 2000.

[6] Simon Rubinstein-Salzedo. p-adic analysis. Provided as part of the p-adic Analysis class.