SELF-DUALITY OF $\mathbb{Q}_p$ AND $\mathbb{R}$ VIA THE SOLENOID

CRIS POOR, JERRY SHURMAN, AND DAVID S. YUEN

ABSTRACT. Let p be prime. Because $\mathbb{Z}[1/p]$ is dense in $\mathbb{Q}_p$ and in $\mathbb{R}$, and because the unitary dual $\mathbb{Z}[1/p]^\vee$ is the projective limit $\lim_{k\geq 0}\mathbb{R}/p^k\mathbb{Z}$, which contains $\mathbb{Q}_p$ and $\mathbb{R}$, it follows readily that $\mathbb{Q}_p$ and $\mathbb{R}$ are unitarily self-dual.

Let S^1 denote the unit circle in the complex plane, a multiplicative group carrying the subspace topology from $\mathbb{C}$. For a topological ring R, let $R^\vee$ denote the unitary dual of R as an additive group, the group of continuous homomorphisms $f:(R,+)\longrightarrow S^1$. Let p be prime. With "=" denoting natural isomorphisms of topological groups here and throughout, two well known equalities are

$$\mathbb{Q}_p^\vee = \mathbb{Q}_p \qquad \text{and} \qquad \mathbb{R}^\vee = \mathbb{R}.$$

For example, these are special cases of Lemma 2.2.1 at the beginning of Tate's thesis [7], proved there and in ensuing expositions such as the Ramakrishnan–Valenza text [6] by using results about locally compact topological groups. Such an argument is an appropriate scalable approach, but this note follows other authors in proving these two equalities in a way that requires less background. A quick elementary proof of the first equality is in Washington's *Monthly* article [8]. A quick proof of the second equality, using integration, is in Theorem VII.9.11 of Conway's functional analysis text [2], and this approach also scales. An elementary approach to these matters is in an online writeup by Conrad [1] mainly focused on $\mathbb{Q}^\vee$. Here we prove the two equalities by using the fact that the localization $\mathbb{Z}[1/p]$ of $\mathbb{Z}$ is dense both in $\mathbb{Q}_p$ and in $\mathbb{R}$. When the localization has the discrete topology, its unitary dual $\mathbb{Z}[1/p]^\vee$ is the projective limit $\lim_{k\geq 0}\mathbb{R}/p^k\mathbb{Z}$, called the *solenoid* in online writeups by Garrett [4, 3]. The solenoid contains $\mathbb{Q}_p$ and $\mathbb{R}$ as the duals of $\mathbb{Z}[1/p]$ with the subspace topologies from $\mathbb{Q}_p$ and $\mathbb{R}$, and therefore as the duals $\mathbb{Q}_p^\vee$ and $\mathbb{R}^\vee$.

Section 1 skims how the definition of $\mathbb{Z}_p$ as a projective limit implies that $\mathbb{Q}_p$ is such a limit as well. Section 2 explains the p-adic exponential. Section 3 introduces the solenoid, denoted $\mathbb{S}_p$, and establishes one p-adic and one real solenoid property. Section 4 shows that the dual $\mathbb{Z}[1/p]^\vee$ is $\mathbb{S}_p$, so that the restriction of an element of $\mathbb{Q}_p^\vee$ or $\mathbb{R}^\vee$ to the dense subset $\mathbb{Z}[1/p]$ of $\mathbb{Q}_p$ or $\mathbb{R}$ can be viewed as a solenoid element. Section 5 uses this and the two established solenoid properties to show that $\mathbb{Q}_p^\vee = \mathbb{Q}_p$ and $\mathbb{R}^\vee = \mathbb{R}$ algebraically; the quick ease of these arguments is the point of this note. Section 6 shows that these equalities are also topological. We assume that the reader is amenable to p-adic ideas and to ideas of point set topology, and we hope that the reader will enjoy the utility of these ideas in action, in particular analysis at one prime proving a real result.

CONTENTS

1. p-adic number field $\mathbb{Q}_p$ as a limit

For any subring R of $\mathbb{R}$, for a prime p, and with the natural projection map $\pi_{\ell,k} : R/p^\ell\mathbb{Z} \longrightarrow R/p^k\mathbb{Z}$ for $0 \le k \le \ell$ induced by the identity map on $\mathbb{R}$, the projective limit $\lim_{k\ge 0} R/p^k\mathbb{Z}$ is the abelian group of compatible vectors

$$v = (v_{p^k}) \in \prod_{k\ge 0} R/p^k\mathbb{Z}, \quad \pi_{\ell,k}(v_{p^\ell}) = v_{p^k} \text{ for } 0 \le k \le \ell,$$

also a ring if $\mathbb{Z}$ is an ideal of R. Here any v_{p^n} determines v_{p^k} for $0 \le k < n$. In particular, the p-adic integer ring $\mathbb{Z}_p$ is defined as this limit with $R = \mathbb{Z}$ and then its quotient p-adic number field $\mathbb{Q}_p$ is a localization of $\mathbb{Z}_p$,

$$\mathbb{Z}_p = \lim_{k\ge 0} \mathbb{Z}/p^k\mathbb{Z} \qquad \text{and} \qquad \mathbb{Q}_p = \mathbb{Z}_p[1/p].$$

Granting the natural-looking third equality to follow, $\mathbb{Q}_p$ as an abelian group is also a limit but with the localization $\mathbb{Z}[1/p]$ rather than $\mathbb{Z}$ as R,

$$\mathbb{Q}_p = \mathbb{Z}_p[1/p] = (\lim_{k\ge 0} \mathbb{Z}/p^k\mathbb{Z})[1/p] = \lim_{k\ge 0} \mathbb{Z}[1/p]/p^k\mathbb{Z}.$$

For the third equality, the mutually inverse maps between $(\lim_{k\ge 0} \mathbb{Z}/p^k\mathbb{Z})[1/p]$ and $\lim_{k\ge 0} \mathbb{Z}[1/p]/p^k\mathbb{Z}$ are

$$\begin{aligned} x = (x_{p^k} + p^k\mathbb{Z})_{k\ge 0}/p^n &\longmapsto y = (x_{p^{k+n}}/p^n + p^k\mathbb{Z})_{k\ge 0} \\ y = (y_{p^k} + p^k\mathbb{Z})_{k\ge 0} &\longmapsto x = (p^n y_{p^{k-n}} + p^k\mathbb{Z})_{k\ge n}/p^n. \end{aligned}$$

In the second map the element y of $\lim_{k\ge 0} \mathbb{Z}[1/p]/p^k\mathbb{Z}$ has a common denominator because $p^n y_1$ lies in $\mathbb{Z}$ for some n and then $p^n y_{p^k} \equiv p^n y_1 \bmod \mathbb{Z}$ lies in $\mathbb{Z}$ for all k. The first map makes no reference to the entries of x lower than $x_{p^n} + p^n\mathbb{Z}$, and the second map produces an x starting at $x_{p^n} + p^n\mathbb{Z}$, but as just explained the first map loses no information in creating y and the second map determines the rest of x.

2. Exponentials e_p and e

Because $\mathbb{Z}[1/p]$ is dense in $\mathbb{Q}_p$ and $\mathbb{Z}_p$ is open in $\mathbb{Q}_p$ and $\mathbb{Z}[1/p] \cap \mathbb{Z}_p = \mathbb{Z}$ there is a natural group isomorphism $\mathbb{Z}[1/p]/\mathbb{Z} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$, and this is further a homeomorphism when $\mathbb{Z}[1/p]$ carries the subspace topology from $\mathbb{Q}_p$. Thus the map

$$\mathrm{e} : \mathbb{Z}[1/p]/\mathbb{Z} \longrightarrow S^1, \qquad \mathrm{e}(q + \mathbb{Z}) = e^{2\pi i q}$$

defines a resulting continuous homomorphism

$$\mathrm{e}_p : \mathbb{Q}_p \longrightarrow S^1, \qquad \ker(\mathrm{e}_p) = \mathbb{Z}_p.$$

Specifically, $\mathrm{e}_p(x) = \mathrm{e}(q_x)$ where $x \in \mathbb{Q}_p$ decomposes (nonuniquely) as $x = q_x + x_o$ with $q_x \in \mathbb{Z}[1/p]$ and $x_o \in \mathbb{Z}_p$. And of course the usual map $\mathrm{e}(x) = e^{2\pi i x}$ from $\mathbb{R}$ to S^1 is a continuous homomorphism having kernel $\mathbb{Z}$.

3. Solenoid $\mathbb{S}_p$

Let $\mathbb{S}_p$ denote the projective limit $\lim_{k\geq 0} \mathbb{R}/p^k\mathbb{Z}$, consisting of the compatible vectors $s = (s_{p^k}) \in \prod_{k\geq 0} \mathbb{R}/p^k\mathbb{Z}$ with $\pi_{\ell,k}(s_{p^\ell}) = s_{p^k}$ for $0 \leq k \leq \ell$. This limit is denoted $\mathbb{S}_p$ and named the solenoid because of how its transition maps $\pi_{\ell,k}$ wrap circles. Each solenoid element uniquely takes the form

$$s = (r_{p^k} + p^k\mathbb{Z}), \quad \begin{pmatrix} r_{p^k} \in [-p^k/2, p^k/2) \subset \mathbb{R} \\ r_{p^\ell} \equiv r_{p^k} \bmod p^k\mathbb{Z} \end{pmatrix} \text{ for } 0 \leq k \leq \ell.$$

The solenoid $\mathbb{S}_p = \lim_{k\geq 0} \mathbb{R}/p^k\mathbb{Z}$ clearly contains $\mathbb{Q}_p = \lim_{k\geq 0} \mathbb{Z}[1/p]/p^k\mathbb{Z}$. It also contains a copy of $\mathbb{R}$, consisting of the vectors such that $r_{p^k} \equiv r \bmod p^k\mathbb{Z}$ for some $r \in \mathbb{R}$ and all k, and we freely refer to this copy as $\mathbb{R}$. Criteria to discern solenoid elements in $\mathbb{Q}_p$ and in $\mathbb{R}$ are as follows. For p-adic elements,

$$\text{for all } s = (r_{p^k} + p^k\mathbb{Z}) \in \mathbb{S}_p, \quad r_1 \in \mathbb{Z}[1/p] \implies s \in \mathbb{Q}_p.$$

Indeed, if $r_1 \in \mathbb{Z}[1/p]$ then the solenoid compatibility conditions give $r_{p^k} \in \mathbb{Z}[1/p]$ for all k and so $s \in \lim_k \mathbb{Z}[1/p]/p^k\mathbb{Z} = \mathbb{Q}_p$. As for real solenoid elements, we prove that

$$(*) \qquad \text{for all } s = (r_{p^k} + p^k\mathbb{Z}) \in \mathbb{S}_p, \quad \lim_{k\to\infty} r_{p^k}/p^k = 0 \implies s \in \mathbb{R}.$$

An induction argument shows that there exist k_o and $r \in \mathbb{R}$ such that $r_{p^k} = r$ for all $k \geq k_o$, as follows. The hypothesis $\lim_{k\to\infty} r_{p^k}/p^k = 0$ in $(*)$ says that there exists k_o such that for all $k \geq k_o$, $|r_{p^k}/p^k| < 1/(2p)$ and so $|r_{p_k}| < p^{k-1}/2$. Let $r = r_{p^{k_o}}$. The claimed equality $r_{p^k} = r$ holds for $k = k_o$ by the definition of r. Suppose inductively that it holds for some $k \geq k_o$. Because $k+1 \geq k_o$ we have $|r_{p^{k+1}}| < p^k/2$, and also $|r_{p^k}| \leq p^k/2$, and also $r_{p^{k+1}} \equiv r_{p^k} \bmod p^k$, and so $r_{p^{k+1}} = r_{p^k}$. The inductive hypothesis is $r_{p^k} = r$, and so $r_{p^{k+1}} = r$. This completes the inductive proof that $r_{p^k} = r$ for all $k \geq k_o$, and so certainly $r_{p^k} + p^k\mathbb{Z} = r + p^k\mathbb{Z}$ for such k. For $0 \leq k < k_o$ the solenoid condition $r_{p^k} + p^k\mathbb{Z} = r_{p^{k_o}} + p^k\mathbb{Z}$ and the equality $r_{p^{k_o}} = r$ give $r_{p^k} + p^k\mathbb{Z} = r + p^k\mathbb{Z}$ as well, and $(*)$ is proved. The converses of the two criteria hold easily as well, but we don't need them.

4. Localization dual $\mathbb{Z}[1/p]^\vee = \mathbb{S}_p$

The solenoid $\mathbb{S}_p$ is the unitary dual $\mathbb{Z}[1/p]^\vee$, where $\mathbb{Z}[1/p]$ carries the discrete topology. Indeed, $\mathbb{Z}[1/p]$ is the non-direct sum $\sum_{k\geq 0} \mathbb{Z}\cdot 1/p^k$, and so any f in $\mathbb{Z}[1/p]^\vee$ is determined by its values $f(1/p^k)$, these values satisfying compatibility conditions. The values are

$$f(1/p^k) = \mathrm{e}(s_{p^k}/p^k), \quad s_{p^k} \in \mathbb{R}/p^k\mathbb{Z}, \quad k = 0, 1, 2, \ldots,$$

each s_{p^k} uniquely of the form $r_{p^k} + p^k\mathbb{Z}$ as above. The compatibility conditions are $(f(1/p^\ell))^{p^{\ell-k}} = f(1/p^k)$ for $0 \leq k \leq \ell$, or $(\mathrm{e}(s_{p^\ell}/p^\ell))^{p^{\ell-k}} = \mathrm{e}(s_{p^k}/p^k)$, or $\mathrm{e}(s_{p^\ell}/p^k) = \mathrm{e}(s_{p^k}/p^k)$, or $r_{p^\ell}/p^k \equiv r_{p^k}/p^k \bmod \mathbb{Z}$, or

$$r_{p^\ell} + p^k\mathbb{Z} = r_{p^k} + p^k\mathbb{Z}, \quad 0 \leq k \leq \ell.$$

That is, the r_{p^k} are compatible with the transition maps of the solenoid. These steps are reversible, and so elements $f : 1/p^k \mapsto \mathrm{e}(r_{p^k}/p^k)$ of $\mathbb{Z}[1/p]^\vee$ and $s = (r_{p^k} + p^k\mathbb{Z})$ of $\mathbb{S}_p$ are naturally identified.

5. p-adic dual $\mathbb{Q}_p^\vee = \mathbb{Q}_p$ and real dual $\mathbb{R}^\vee = \mathbb{R}$

Every p-adic number r defines an element of $\mathbb{Q}_p^\vee$,

$$f_r : \mathbb{Q}_p \longrightarrow S^1, \qquad f_r(x) = \mathrm{e}_p(rx).$$

To show that these make up all of $\mathbb{Q}_p^\vee$, let $f \in \mathbb{Q}_p^\vee$ be given and let $s(f) = (r_{p^k} + p^k\mathbb{Z})$ be the solenoid element corresponding to its restriction to $\mathbb{Z}[1/p]$. Because $p^d\mathbb{Z}_p$ lies in any neighborhood of 0 in $\mathbb{Q}_p$ for large enough d, and f is continuous at 0, f maps some $p^d\mathbb{Z}_p$ into the open right half of S^1, which contains no nontrivial subgroup, and so $f(p^d\mathbb{Z}_p) = 1$; thus $(\mathrm{e}(r_1))^{p^d} = (f(1))^{p^d} = f(p^d) = 1$, giving $r_1 \in 1/p^d{\cdot}\mathbb{Z} \subset \mathbb{Z}[1/p]$. As explained in section 3, consequently $s(f)$ is a p-adic number r. For each $k \geq 0$ the congruence $r_{p^k} \equiv r \bmod p^k\mathbb{Z}_p$ gives $f(1/p^k) = \mathrm{e}(r_{p^k}/p^k) = \mathrm{e}_p(r/p^k) = f_r(1/p^k)$, and so $f = f_r$ on the dense subset $\mathbb{Z}[1/p]$ of $\mathbb{Q}_p$. Thus $f = f_r$.

Every real number r defines an element of $\mathbb{R}^\vee$,

$$f_r : \mathbb{R} \longrightarrow S^1, \qquad f_r(x) = \mathrm{e}(rx).$$

To show that these make up all of $\mathbb{R}^\vee$, let p be any prime, let $f \in \mathbb{R}^\vee$ be given, and let $s_p(f) = (r_{p^k} + p^k\mathbb{Z})$ be the solenoid element corresponding to its restriction to $\mathbb{Z}[1/p]$. Because $\lim_{k\to\infty} 1/p^k = 0$ in $\mathbb{R}$ and f is continuous at 0, $\lim_{k\to\infty} \mathrm{e}(r_{p^k}/p^k) = \lim_{k\to\infty} f(1/p^k) = f(0) = 1$ in S^1, giving $\lim_{k\to\infty} r_{p^k}/p^k = 0$ in $\mathbb{R}$. As explained in section 3, consequently $s_p(f)$ is a real number r. For each $k \geq 0$ the congruence $r_{p^k} \equiv r \bmod p^k\mathbb{Z}$ gives $f(1/p^k) = \mathrm{e}(r_{p^k}/p^k) = \mathrm{e}(r/p^k) = f_r(1/p^k)$, and so $f = f_r$ on the dense subset $\mathbb{Z}[1/p]$ of $\mathbb{R}$. Thus $f = f_r$.

6. Topology

As a projective limit of compact spaces, $\mathbb{S}_p = \lim_k \mathbb{R}/p^k\mathbb{Z}$ is compact, its limit topology being the subspace topology that it inherits from the product topology of $\prod_{k\geq 0} \mathbb{R}/p^k\mathbb{Z}$. In particular, a subbasis about 0 consists of the sets

$$T_{\ell,\varepsilon} = \{(r_{p^k} + p^k\mathbb{Z}) \in \mathbb{S}_p : |r_{p^\ell}/p^\ell| < \varepsilon\}, \quad \ell \in \mathbb{Z}_{\geq 0},\ \varepsilon > 0.$$

The unitary dual $\mathbb{Z}[1/p]^\vee$ carries the compact-open topology. Because the compact subsets of $\mathbb{Z}[1/p]$ are the finite sets, a compact-open subbasis about 1 in $\mathbb{Z}[1/p]^\vee$ consists of the sets

$$U_{\ell,\varepsilon} = \{f \in \mathbb{Z}[1/p]^\vee : f(1/p^\ell) \in \mathrm{e}((-\varepsilon, \varepsilon))\}, \quad \ell \in \mathbb{Z}_{\geq 0},\ \varepsilon > 0.$$

And because $f(1/p^\ell) = \mathrm{e}(r_{p^\ell}/p^\ell)$, these identify with the subsets $T_{\ell,\varepsilon}$ of $\mathbb{S}_p$. Thus the identification of $\mathbb{Z}[1/p]^\vee$ and $\mathbb{S}_p$ is a topological group isomorphism.

The map $r \mapsto f_r$ from $\mathbb{Q}_p$ to $\mathbb{Q}_p^\vee$ or from $\mathbb{R}$ to $\mathbb{R}^\vee$ is a group isomorphism, its homomorphic property and injectivity clear and its surjectivity now established. Further it is a topological isomorphism by a standard exercise in which the solenoid plays no role, as follows. In the compact-open topology of $\mathbb{Q}_p^\vee$, a subbasis at 1 consists of the sets

$$V_{K,\varepsilon} = \{f : f(K) \subset \mathrm{e}((-\varepsilon, \varepsilon))\}, \quad K \text{ compact in } \mathbb{Q}_p,\ \varepsilon > 0.$$

Let $\{f_{r_n}\}$ go to 1 in $\mathbb{Q}_p^\vee$. Given a positive integer m, there exists n_o such that for all $n \geq n_o$, $f_{r_n} \in V_{p^{-m}\mathbb{Z}_p,\pi/2}$ and so $\mathrm{e}_p(r_n p^{-m}\mathbb{Z}_p)$ is a subgroup of $\mathrm{e}((-\pi/2,\pi/2))$, making it 1, from which $r_n \in p^m\mathbb{Z}_p$; thus $\{r_n\}$ goes to 0 in $\mathbb{Q}_p$. Conversely, let $\{r_n\}$ go to 0 in $\mathbb{Q}_p$. Given K compact in $\mathbb{Q}_p$ and $\varepsilon > 0$, there exists $n_o = n_o(m,\varepsilon)$ such that for all $n \geq n_o$, $r_n K \subset \mathbb{Z}_p$ and so $\mathrm{e}_p(r_n K) = \{1\} \subset \mathrm{e}((-\varepsilon,\varepsilon))$, from which $f_{r_n} \in V_{K,\varepsilon}$; thus $\{f_{r_n}\}$ goes to 1 in $\mathbb{Q}_p^\vee$. In the compact-open topology of $\mathbb{R}^\vee$, a subbasis at 1 consists of the sets

$$W_{K,\varepsilon} = \{f : f(K) \subset \mathrm{e}((-\varepsilon,\varepsilon))\}, \quad K \text{ compact in } \mathbb{R},\ \varepsilon > 0.$$

Let $\{f_{r_n}\}$ go to 1 in $\mathbb{R}^\vee$. Given $\varepsilon > 0$, there exists n_o such that for all $n \geq n_o$, $f_{r_n} \in W_{[-1,1],\varepsilon}$ and so $r_n[-1,1] \subset (-\varepsilon,\varepsilon)$ and so $|r_n| < \varepsilon$; thus $\{r_n\}$ goes to 0 in $\mathbb{R}$. Conversely, let $\{r_n\}$ go to 0 in $\mathbb{R}$. Given K compact in $\mathbb{R}$ and $\varepsilon > 0$, there exists $\delta > 0$ such that $K \subset [-\delta,\delta]$ and then $n_o = n_o(\delta,\varepsilon)$ such that for all $n \geq n_o$, $|r_n|\delta < \varepsilon$ and so $f_{r_n} \in W_{K,\varepsilon}$; thus $\{f_{r_n}\}$ goes to 1 in $\mathbb{R}^\vee$.

7. Rational dual

As a final comment we state without proof that the localization unitary dual $\mathbb{Z}[1/p]^\vee = \mathbb{S}_p = \lim_{k\geq 0} \mathbb{R}/p^k\mathbb{Z}$ is $(\mathbb{R} \times \mathbb{Q}_p)/\mathbb{Z}[1/p]$, and that beyond the scope of this note, the rational unitary dual $\mathbb{Q}^\vee$ is the larger solenoid $\mathbb{S} = \lim_{n\geq 1} \mathbb{R}/n\mathbb{Z} = \prod_p \lim_{k\geq 0} \mathbb{R}/p^k\mathbb{Z} = \prod_p \mathbb{S}_p = \mathbb{A}/\mathbb{Q}$ where $\mathbb{A}$ denotes the rational adele ring; this ring $\mathbb{A} = \bigcup_{N\geq 1} \frac{1}{N}(\mathbb{R} \times \prod_p \mathbb{Z}_p)$ is not the full product $\mathbb{R} \times \prod_p \mathbb{Q}_p$. See Garrett's writeup [5] for these matters, or Conrad's writeup [1] for a treatment of $\mathbb{Q}^\vee$ that is solenoid-free.

References

[1] Keith Conrad. The character group of $\mathbb{Q}$. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/characterQ.pdf`.

[2] John B. Conway. *A course in functional analysis*, volume 96 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[3] Paul Garrett. Bigger diagrams for solenoids, more automorphisms, colimits. `https://www-users.cse.umn.edu/~garrett/m/mfms/notes/03_more_autos.pdf`.

[4] Paul Garrett. Solenoids. `https://www-users.cse.umn.edu/~garrett/m/mfms/notes/02_solenoids.pdf`.

[5] Paul Garrett. The ur-solenoid and the adeles. `https://www-users.cse.umn.edu/~garrett/m/mfms/notes/04_ur_solenoid.pdf`.

[6] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[7] J. T. Tate. Fourier analysis in number fields, and Hecke's zeta-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347. Academic Press, London, 1967.

[8] Lawrence Washington. On the self-duality of $\mathbb{Q}_p$. *Amer. Math. Monthly*, 81:369–371, 1974.