MAXIMAL COMPACT SUBGROUPS OF $\mathrm{GL}_n(\mathbf{Q}_p)$

KEITH CONRAD

1. Introduction

It is a classical theorem that for $n \geq 1$, each compact subgroup of $\mathrm{GL}_n(\mathbf{R})$ is conjugate to a subgroup of the compact group $\mathrm{O}_n(\mathbf{R})$, the real orthogonal group:

$$\mathrm{O}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) : AA^\top = I_n\}. \tag{1.1}$$

This isn't be true with $\mathbf{R}$ replaced by $\mathbf{Q}_p$ because every matrix in $\mathrm{O}_n(\mathbf{Q}_p)$ has determinant ± 1 but the scalar diagonal matrices $\mathbf{Z}_p^\times I_n$ form a compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$ conjugate only to themselves (they're in the center) and most of them don't have determinant ± 1. Moreover, the groups $\mathrm{O}_n(\mathbf{Q}_p)$ are usually *not* compact (see the appendix).

The correct p-adic analogue of each compact subgroup of $\mathrm{GL}_n(\mathbf{R})$ being conjugate to a subgroup of $\mathrm{O}_n(\mathbf{R})$ is that each compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$ is conjugate to a subgroup of the compact group $\mathrm{GL}_n(\mathbf{Z}_p)$. Our exposition of this result will follow [1, pp. LG 4.30–LG 4.32] closely except for the proof of Lemma 2.6 below (its statement is [1, Lemma 1]).

It is worth briefly describing how all compact subgroups of $\mathrm{GL}_n(\mathbf{R})$ are proved to be conjugate to a subgroup of $\mathrm{O}_n(\mathbf{R})$, even though the real and p-adic proofs are different. The group $\mathrm{O}_n(\mathbf{R})$ can be characterized either as all $A \in \mathrm{GL}_n(\mathbf{R})$ such that $AA^\top = I_n$, as in (1.1), or more geometrically as all $A \in \mathrm{GL}_n(\mathbf{R})$ that preserve the dot product:

$$\mathrm{O}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) : Av \cdot Aw = v \cdot w \text{ for all } v \text{ and } w \text{ in } \mathbf{R}^n\}. \tag{1.2}$$

The dot product is just one example of an inner product on $\mathbf{R}^n$, and all inner products can be turned into the dot product by a linear change of variables. With this in mind, if we are given a compact subgroup H of $\mathrm{GL}_n(\mathbf{R})$, integration on H (with respect to an invariant measure) can be used to create an inner product $\langle \cdot, \cdot \rangle$ on $\mathbf{R}^n$ that is H-invariant: $\langle h(v), h(w) \rangle = \langle v, w \rangle$ for all $h \in H$. By a linear change of variables this inner product can be turned into the dot product on $\mathbf{R}^n$, and that linear change of variables is an $A \in \mathrm{GL}_n(\mathbf{R})$ that conjugates H into $\mathrm{O}_n(\mathbf{R})$.

The p-adic substitute for the *dot product* on $\mathbf{R}^n$ (which is preserved by $\mathrm{O}_n(\mathbf{R})$) is the *subgroup* $\mathbf{Z}_p^n$ of $\mathbf{Q}_p^n$. For each $A \in \mathrm{GL}_n(\mathbf{Q}_p)$, we can act A on $\mathbf{Z}_p^n = \sum_{i=1}^n \mathbf{Z}_p e_i$ (here and below, the e_i's are the standard basis of n-space) and get $A(\mathbf{Z}_p^n) = \sum_{i=1}^n \mathbf{Z}_p A(e_i)$, which may or may not be $\mathbf{Z}_p^n$ again.

Theorem 1.1. $\mathrm{GL}_n(\mathbf{Z}_p) = \{A \in \mathrm{GL}_n(\mathbf{Q}_p) : A(\mathbf{Z}_p^n) = \mathbf{Z}_p^n\}$.

This theorem, characterizing $\mathrm{GL}_n(\mathbf{Z}_p)$, is the p-adic analogue of (1.2).

Proof. Suppose $A(\mathbf{Z}_p^n) = \mathbf{Z}_p^n$. The standard basis of $\mathbf{Q}_p^n$ is inside $\mathbf{Z}_p^n$. so from $A(\mathbf{Z}_p^n) = \mathbf{Z}_p^n$ we get $A(e_i) \in \mathbf{Z}_p^n$ for all i, so the columns of A are in $\mathbf{Z}_p^n$. Also $\mathbf{Z}_p^n = A^{-1}(\mathbf{Z}_p^n)$, so the columns of A^{-1} are in $\mathbf{Z}_p^n$ too. Thus A and A^{-1} are both matrices with $\mathbf{Z}_p$-entries, so $A \in \mathrm{GL}_n(\mathbf{Z}_p)$.

Conversely, suppose $A \in \mathrm{GL}_n(\mathbf{Z}_p)$. Then A has $\mathbf{Z}_p$-entries, so $A(e_i) \in \mathbf{Z}_p^n$. Since $A(\mathbf{Z}_p^n)$ is the $\mathbf{Z}_p$-linear combinations of the vectors $A(e_i)$, $A(\mathbf{Z}_p^n) \subset \mathbf{Z}_p^n$. Also A^{-1} has $\mathbf{Z}_p$-entries, so $A^{-1}(\mathbf{Z}_p^n) \subset \mathbf{Z}_p^n$, or equivalently $\mathbf{Z}_p^n \subset A(\mathbf{Z}_p^n)$. Hence $A(\mathbf{Z}_p^n) = \mathbf{Z}_p^n$. ∎

Theorem 1.2. *The group* $\mathrm{GL}_n(\mathbf{Z}_p)$ *is compact and open in* $\mathrm{GL}_n(\mathbf{Q}_p)$.

Proof. We can view $\mathrm{GL}_n(\mathbf{Z}_p)$ as the intersection

$$\mathrm{GL}_n(\mathbf{Z}_p) = \mathrm{M}_n(\mathbf{Z}_p) \cap \left\{g \in \mathrm{M}_n(\mathbf{Q}_p) : \det g \in \mathbf{Z}_p^\times\right\}.$$

Inside $\mathrm{M}_n(\mathbf{Q}_p)$, $\mathrm{M}_n(\mathbf{Z}_p)$ is open (it is the sup-norm unit ball with respect to the standard basis of $\mathrm{M}_n(\mathbf{Q}_p)$), and since the determinant $\det\colon \mathrm{M}_n(\mathbf{Q}_p) \to \mathbf{Q}_p$ is continuous (it is a polynomial function of the matrix entries) and $\mathbf{Z}_p^\times$ is open in $\mathbf{Q}_p$ the set $\left\{g \in \mathrm{M}_n(\mathbf{Q}_p) : \det g \in \mathbf{Z}_p^\times\right\}$ is open in $\mathrm{M}_n(\mathbf{Q}_p)$. Therefore $\mathrm{GL}_n(\mathbf{Z}_p)$ is the intersection of two open sets in $\mathrm{M}_n(\mathbf{Q}_p)$, so it is open here. Then since $\mathrm{GL}_n(\mathbf{Z}_p) \subset \mathrm{GL}_n(\mathbf{Q}_p)$ and $\mathrm{GL}_n(\mathbf{Q}_p)$ is open in $\mathrm{M}_n(\mathbf{Q}_p)$ (since $\mathrm{GL}_n(\mathbf{Q}_p) = \det^{-1}(\mathbf{Q}_p^\times)$), $\mathrm{GL}_n(\mathbf{Z}_p)$ is open in $\mathrm{GL}_n(\mathbf{Q}_p)$.

To show $\mathrm{GL}_n(\mathbf{Z}_p)$ is compact, we first observe that $\mathrm{M}_n(\mathbf{Z}_p)$ is compact (it is the closed unit ball of $\mathrm{M}_n(\mathbf{Q}_p)$ in the sup-norm with respect to the standard basis of $\mathrm{M}_n(\mathbf{Q}_p)$). Then $\mathrm{GL}_n(\mathbf{Z}_p)$ is the inverse image of $\mathbf{Z}_p^\times$ for $\det\colon \mathrm{M}_n(\mathbf{Z}_p) \to \mathbf{Z}_p$. This is continuous and $\mathbf{Z}_p^\times$ is closed in $\mathbf{Z}_p$, so the inverse image $\mathrm{GL}_n(\mathbf{Z}_p)$ is closed in a compact space $\mathrm{M}_n(\mathbf{Z}_p)$ and therefore is compact. □

While $\mathrm{GL}_n(\mathbf{Z}_p)$ is like $\mathrm{O}_n(\mathbf{R})$ because both are compact, note that $\mathrm{O}_n(\mathbf{R})$ is not open in $\mathrm{GL}_n(\mathbf{R})$: spaces that are related to Euclidean space are usually not compact and open, while the totally disconnected nature of p-adic spaces makes compactness and openness fairly common properties together.

2. Lattices in $\mathbf{Q}_p^n$

In $\mathbf{R}^n$, a lattice is defined to be the $\mathbf{Z}$-span of a basis of $\mathbf{R}^n$, with the standard lattice of $\mathbf{R}^n$ being $\mathbf{Z}^n$. We are going to work with $\mathbf{Z}_p^n$ as the analogue in $\mathbf{Q}_p^n$ of $\mathbf{Z}^n$ in $\mathbf{R}^n$: $\mathbf{Z}_p^n$ is the $\mathbf{Z}_p$-span of the standard basis of $\mathbf{Q}_p^n$, just as $\mathbf{Z}^n$ is the $\mathbf{Z}$-span of the standard basis of $\mathbf{R}^n$.

Definition 2.1. A *lattice* in $\mathbf{Q}_p^n$ is the $\mathbf{Z}_p$-span of a basis of $\mathbf{Q}_p^n$.

The most basic example of a lattice in $\mathbf{Q}_p^n$ is $\mathbf{Z}_p^n$, which will be called the *standard lattice* in $\mathbf{Q}_p^n$.

Remark 2.2. In $\mathbf{Q}_p^2$, $\mathbf{Z}_p \times \{0\}$ is *not* a lattice. Note it does not contain a basis for $\mathbf{Q}_p^2$.

For $A \in \mathrm{GL}_n(\mathbf{Q}_p)$, $A(\mathbf{Z}_p^n)$ is the $\mathbf{Z}_p$-span of $A(e_1), \ldots, A(e_n)$, which is a basis of $\mathbf{Q}_p^n$, so $A(\mathbf{Z}_p^n)$ is a lattice in $\mathbf{Q}_p^n$.

Theorem 2.3. *In* $\mathbf{R}^n$*, all lattices are of the form* $A(\mathbf{Z}^n)$ *where* $A \in \mathrm{GL}_n(\mathbf{R})$*. In* $\mathbf{Q}_p^n$*, all lattices are of the form* $A(\mathbf{Z}_p^n)$ *where* $A \in \mathrm{GL}_n(\mathbf{Q}_p)$.

Proof. If $A \in \mathrm{GL}_n(\mathbf{R})$ is such that $A = [\mathbf{v}_1 \cdots \mathbf{v}_n]$ where each $\mathbf{v}_i$ represents a column of A, then the $\mathbf{v}_i$'s are linearly independent over $\mathbf{R}$ and

$$A(\mathbf{Z}^n) = A(\mathbf{Z}e_1 + \cdots + \mathbf{Z}e_n) = \mathbf{Z}\mathbf{v}_1 + \cdots + \mathbf{Z}\mathbf{v}_n = \sum_{i=1}^n \mathbf{Z}\mathbf{v}_i$$

is the $\mathbf{Z}$-span of a basis of $\mathbf{R}^n$. Conversely, if $L = \mathbf{Z}\mathbf{v}_1 + \cdots + \mathbf{Z}\mathbf{v}_n$ is the $\mathbf{Z}$-span of a basis of $\mathbf{R}^n$ then the matrix $A = [\mathbf{v}_1 \cdots \mathbf{v}_n]$ is in $\mathrm{GL}_n(\mathbf{R})$ and $L = \mathbf{Z}A(e_1) + \cdots + \mathbf{Z}A(e_n) = A(\mathbf{Z}^n)$.

If we replace $\mathbf{Z}$ with $\mathbf{Z}_p$, the proof goes through for the p-adic case in the same way. □

Since $\mathbf{Z}^n$ is discrete, Theorem 2.3 tells us every lattice L in $\mathbf{R}^n$ is discrete. Likewise, since $\mathbf{Z}_p^n$ is compact and open in $\mathbf{Q}_p^n$ every lattice in $\mathbf{Q}_p^n$ is compact and open. (If we use quotient vector spaces, the dichotomy between lattices in $\mathbf{R}^n$ and $\mathbf{Q}_p^n$ takes on a more appealing form: when V is $\mathbf{R}^n$ or $\mathbf{Q}_p^n$ and L is a lattice in V, L is discrete and V/L is compact for real V while L is compact and V/L is discrete for p-adic V; V/L being discrete is another way of saying L is open in V.)

The following definition, inspired by Theorem 1.1, gives the counterpart to lattices in $\mathbf{Q}_p^n$ of the role $\mathrm{GL}_n(\mathbf{Z}_p)$ plays for the standard lattice $\mathbf{Z}_p^n$.

Definition 2.4. For each lattice L in $\mathbf{Q}_p^n$, set

$$K_L = \{g \in \mathrm{GL}_n(\mathbf{Q}_p) : g(L) = L\}.$$

For example, $K_{\mathbf{Z}_p^n} = \mathrm{GL}_n(\mathbf{Z}_p)$. When $g(L) = L$, we will say "g fixes L," but that only means L is fixed as a set, not that g fixes every element of L. Because all lattices in $\mathbf{Q}_p^n$ can be obtained from the standard lattice via a matrix in $\mathrm{GL}_n(\mathbf{Q}_p)$ (Theorem 2.3), the K_L's for different L's are related to each other:

Theorem 2.5. *For a lattice L in $\mathbf{Q}_p^n$, there is some $g \in \mathrm{GL}_n(\mathbf{Q}_p)$ such that $K_L = g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}$. Conversely, for $g \in \mathrm{GL}_n(\mathbf{Q}_p)$ the group $g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}$ is K_L for some lattice L in $\mathbf{Q}_p^n$.*

In particular, K_L is compact and open in $\mathrm{GL}_n(\mathbf{Q}_p)$.

Proof. For a lattice L, by Theorem 2.3 we can write $L = g(\mathbf{Z}_p^n)$ for some $g \in \mathrm{GL}_n(\mathbf{Q}_p)$. Then

$$\begin{aligned} K_L &= \{h \in \mathrm{GL}_n(\mathbf{Q}_p) : h(L) = L\} \\ &= \left\{h \in \mathrm{GL}_n(\mathbf{Q}_p) : hg(\mathbf{Z}_p^n) = g(\mathbf{Z}_p^n)\right\} \\ &= \left\{h \in \mathrm{GL}_n(\mathbf{Q}_p) : g^{-1}hg(\mathbf{Z}_p^n) = \mathbf{Z}_p^n\right\} \\ &= \left\{h \in \mathrm{GL}_n(\mathbf{Q}_p) : g^{-1}hg \in \mathrm{GL}_n(\mathbf{Z}_p)\right\} \\ &= g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}. \end{aligned}$$

Conjugation by g on $\mathrm{GL}_n(\mathbf{Q}_p)$ is continuous with continuous inverse, so since $\mathrm{GL}_n(\mathbf{Z}_p)$ is compact and open in $\mathrm{GL}_n(\mathbf{Q}_p)$ by Theorem 1.2, its conjugate subgroup K_L is compact and open in $\mathrm{GL}_n(\mathbf{Q}_p)$.

Reading the above computations in reverse shows $g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1} = K_{g(\mathbf{Z}_p^n)}$. □

In the language of group actions, the group $\mathrm{GL}_n(\mathbf{Q}_p)$ acts on the set of all lattices in $\mathbf{Q}_p^n$ by $g \cdot L = g(L)$. Theorem 2.3 says this action has a single orbit, and Theorem 1.1 says the stabilizer subgroup of $\mathbf{Z}_p^n$ is $\mathrm{GL}_n(\mathbf{Z}_p)$, while K_L is defined as the stabilizer subgroup of L. Points in the same orbit of a group action have conjugate stabilizer subgroups (with a conjugating element being one that sends one point to the other), so Theorem 2.5 makes sense in terms of group actions.

To prove every compact subgroup H of $\mathrm{GL}_n(\mathbf{Q}_p)$ is inside a conjugate of $\mathrm{GL}_n(\mathbf{Z}_p)$, Theorem 2.5 says that is the same as showing H is inside a K_L, i.e., H fixes some lattice in $\mathbf{Q}_p^n$. That is what we are actually going to show. To create a lattice in $\mathbf{Q}_p^n$ fixed by H, we will start with a lattice and then make an H-fixed lattice by "averaging" (really, summing) over the lattices $h(L)$ for $h \in H$. Compactness of H will tell us $\#\{h(L) : h \in H\}$ is finite. To show a finite sum of lattices is a lattice, the following characterization of lattices is more convenient than the definition of a lattice.

Lemma 2.6. *A subgroup L of $\mathbf{Q}_p^n$ is a lattice if and only if L has a finite spanning set over $\mathbf{Z}_p$ and L contains a basis of $\mathbf{Q}_p^n$.*

This means: if there is a finite set of vectors whose $\mathbf{Z}_p$-span is L (not assuming it is a basis) and L contains a basis of $\mathbf{Q}_p^n$, then L is a lattice, and conversely.

Proof. ($\Rightarrow$): By the definition of a lattice, L is the $\mathbf{Z}_p$-span of a basis of $\mathbf{Q}_p^n$, so L has a finite spanning set over $\mathbf{Z}_p$ and contains a basis of $\mathbf{Q}_p^n$.

($\Leftarrow$): Since L has a finite spanning set, $L = \sum_{i=1}^m \mathbf{Z}_p v_i$ for some v_i's in $\mathbf{Q}_p^n$. The $\mathbf{Q}_p$-span of the v_i's has dimension at most m, and this span is $\mathbf{Q}_p^n$ since L contains a basis of $\mathbf{Q}_p^n$. Therefore $n \leq m$.

If $n < m$ then the v_i's have a nontrivial $\mathbf{Q}_p$-linear relation, say

$$c_1 v_1 + \cdots + c_m v_m = 0$$

with $c_i \in \mathbf{Q}_p$ not all 0. We can turn this into a $\mathbf{Z}_p$-linear relation by dividing this equation by the c_i with maximal absolute value. That gives such a relation with $\mathbf{Z}_p$-coefficients and the v_i-coefficient is 1. Therefore v_i is in the $\mathbf{Z}_p$-span of the other v_j's, so we can remove it and still have a spanning set of L over $\mathbf{Z}_p$. Repeating this process, the bound $n \leq m$ tells us that eventually we will reach $m = n$, and at that point our spanning set can't be linearly dependent over $\mathbf{Q}_p$ (otherwise we could shrink it still further, but we must have $n \leq m$). So we have reached a spanning set of L over $\mathbf{Z}_p$ that has size n and is linearly independent over $\mathbf{Q}_p$, and thus L is the $\mathbf{Z}_p$-span of a basis of $\mathbf{Q}_p^n$, so L is a lattice. □

Remark 2.7. In [1], Lemma 2.6 is proved using properties of modules over a PID. The proof above avoided relying on $\mathbf{Z}_p$ being a PID.

Lemma 2.8. *Let $L_1, \ldots, L_r$ be lattices in $\mathbf{Q}_p^n$ and let $L = L_1 + \cdots + L_r$. Then L is a lattice in $\mathbf{Q}_p^n$.*

Proof. We use Lemma 2.6. First, L contains a basis of $\mathbf{Q}_p$ since each L_i does. Each L_i has a finite spanning set over $\mathbf{Z}_p$, so L has one as well: just use the union of the spanning sets of the L_i's. □

3. Maximality properties of $\mathrm{GL}_n(\mathbf{Z}_p)$

Theorem 3.1. *Let H be a compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$. Then:*

(1) *There exists a lattice M in $\mathbf{Q}_p^n$ such that $H \subset K_M$.*
(2) *There exists $g \in \mathrm{GL}_n(\mathbf{Q}_p)$ such that $H \subset g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}$.*

Proof. (1): Choose a lattice L in $\mathbf{Q}_p^n$ (for example, $L = \mathbf{Z}_p^n$). The intersection $H_L = H \cap K_L$ is the subgroup of H that sends L onto L. Since K_L is open in $\mathrm{GL}_n(\mathbf{Q}_p)$, H_L is open in H. Hence H_L has finite index in H (every open subgroup of a compact group has finite index, because the coset decomposition by the subgroup is an open covering that has a finite subcovering). Therefore we can write

$$H = \bigcup_{\sigma \in S} \sigma H_L,$$

where S is a finite set. For $h \in H$, write $h = \sigma g$ for some $\sigma \in S$ and $g \in H_L$. Then $h(L) = \sigma(g(L)) = \sigma(L)$, so

$$\{h(L) : h \in H\} = \{\sigma(L) : \sigma \in S\}$$

is finite. Let

$$M = \sum_{\sigma \in S} \sigma(L),$$

which is a finite sum of lattices. By Lemma 2.8, M is a lattice. We now show M is fixed by H, so $H \subset K_M$. For $h \in H$, write $h\sigma = \sigma_h g_h$ for $\sigma_h \in S$ and $g_h \in H_L$. Then

$$h(M) = \sum_{\sigma \in S} h\sigma(L) = \sum_{\sigma \in S} \sigma_h g_h(L) = \sum_{\sigma \in S} \sigma_h(L) = M,$$

where in the last step we use the fact that $\{\sigma_h : \sigma \in S\}$ is a set of representatives for the left H_L-cosets of H.

(2): By Theorem 2.5, $K_M = g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}$ for some $g \in \mathrm{GL}_n(\mathbf{Q}_p)$ (use any g such that $M = g(\mathbf{Z}_p^n)$). So $H \subset K_M = g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}$, as required. $\square$

Now we want to show $\mathrm{GL}_n(\mathbf{Z}_p)$ is a *maximal* compact subgroup: it is not strictly contained in a larger compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$. (In the $n = 1$ case this is clear: $\mathrm{GL}_1(\mathbf{Z}_p) = \mathbf{Z}_p^\times$ is a maximal compact subgroup of $\mathrm{GL}_1(\mathbf{Q}_p) = \mathbf{Q}_p^\times$ since each element of $\mathbf{Q}_p^\times$ not of absolute value 1 has unbounded powers. We don't have an absolute value on $\mathrm{GL}_n(\mathbf{Q}_p)$ for $n > 1$ to generalize that argument.) Since every compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$ is in some K_L, what we want is the same as showing there are no containment relations among different K_L's.

We need a lemma from linear algebra, having nothing to do with p-adic fields.

Lemma 3.2. *Let V be a nonzero finite-dimensional vector space over a field F and let $W \subset V$ be a subspace such that $A(W) = W$ for all $A \in \mathrm{Aut}_F(V) = \mathrm{GL}(V)$. Then $W = 0$ or $W = V$.*

Proof. Set $n = \dim V > 0$. We will prove the contrapositive: if W is not 0 or V then $A(W) \neq W$ for some $A \in \mathrm{GL}(V)$. Of course we can take $n > 1$.

Set $d = \dim W$ and suppose $0 < d < n$. Pick a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ of W and extend it to a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_d, \ldots, \mathbf{e}_n\}$ of V. Pick $\mathbf{f}_1 \in V - W$ and extend it to a basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ of V. Define $A : V \to V$ by

$$A\left(\sum c_j \mathbf{e}_j\right) = \sum c_j \mathbf{f}_j.$$

Since A sends a basis to a basis, $A \in \mathrm{GL}(V)$. We have $A(W) \neq W$ since $A(\mathbf{e}_1) = \mathbf{f}_1 \notin W$. $\square$

The proof of the following theorem contains most of the hard work in this discussion.

Theorem 3.3. *Let L and L' be two lattices in $\mathbf{Q}_p^n$ and suppose $K_L \subset K_{L'}$. Then there exists $\lambda \in \mathbf{Q}_p^\times$ such that $L = \lambda L'$, and $K_L = K_{L'}$.*

Proof. Let

$$L = \sum_{i=1}^n \mathbf{Z}_p \mathbf{e}_i \qquad \text{and} \qquad L' = \sum_{j=1}^n \mathbf{Z}_p \mathbf{f}_j$$

for some bases $\{\mathbf{e}_i\}$ and $\{\mathbf{f}_j\}$ of $\mathbf{Q}_p^n$. For $\lambda \in \mathbf{Q}_p^\times$, $K_{\lambda L'} = K_{L'}$, so replacing L' with a nonzero scalar multiple doesn't affect the hypotheses of the theorem. We will do two scalings on L' to make things easier to analyze. Neither replacement changes $K_{L'}$.

First we show that $\lambda L' \subset L$ for some $\lambda \in \mathbf{Q}_p^\times$. The $\mathbf{e}_i$'s and $\mathbf{f}_j$'s are bases of $\mathbf{Q}_p^n$, so we can write

$$\mathbf{f}_j = \sum_{i=1}^n a_{ij} \mathbf{e}_i$$

where $a_{ij} \in \mathbf{Q}_p$. Then for $\lambda \neq 0$ small, we have $\lambda a_{ij} \in \mathbf{Z}_p$ for all i, j. So $\lambda \mathbf{f}_j \in L$ for all j and thus $\lambda L' \subset L$. We may replace L' with $\lambda L'$ and thus can suppose $L' \subset L$.

Next we want to show by further scaling that we can also arrange $L' \not\subset pL$ while still having $L' \subset L$. We know that, being a lattice, L' is open in $\mathbf{Q}_p^n$. Then since $0 \in L'$, $p^N \mathbf{e}_i \in L'$ for all i and for some N. So $p^N L \subset L' \subset L$. Multiplication by p makes a lattice smaller (as a set), so $p^{N+1}L$ is a proper subset of L'. Since L' is inside $L = p^0 L$ but is not inside $p^{N+1}L$, there is a maximum $r \geq 0$ such that $L' \subset p^r L$; that is, $L' \subset p^r L$ but $L' \not\subset p^{r+1}L$. This implies

$$\frac{1}{p^r} L' \subset L \qquad \text{and} \qquad \frac{1}{p^r} L' \not\subset pL.$$

We replace L' with $(1/p^r)L'$, which does not change the stabilizer group ($K_{\frac{1}{p^r}L'} = K_{L'}$), so now we have $L' \subset L$ and $L' \not\subset pL$.

From the two relations on L and L',

$$pL \subsetneq L' + pL \subset L. \tag{3.1}$$

We are going to show $L' + pL = L$, and then use the containment $K_{L'} \subset K_L$ (which has yet to be applied) to show $L' = L$. Reduce (3.1) modulo pL: set $V = L/pL$ and $W = (L' + pL)/pL$, so $W \subset V$ and $W \neq 0$. Multiplication by p kills V and W, so V and W are naturally $\mathbf{F}_p$-vector spaces and $V = \oplus_{i=1}^n (\mathbf{Z}_p/p\mathbf{Z}_p)\bar{\mathbf{e}}_i$ is n-dimensional over $\mathbf{F}_p$. We want to prove $W = V$, so then $L' + pL = L$. Lemma 3.2 is the result we need.

For each $g \in K_L$, $g(L) = L$ and $g(pL) = p \cdot g(L) = pL$, so g makes sense as a function

$$\bar{g} : L/pL \longrightarrow L/pL$$

that is $\mathbf{F}_p$-linear. So we have a reduction map

$$K_L \longrightarrow \mathrm{Aut}_{\mathbf{F}_p}(L/pL) \cong \mathrm{GL}_n(\mathbf{F}_p) \tag{3.2}$$

by $g \mapsto \bar{g}$. It is a homomorphism: $\overline{g_1 g_2} = \bar{g}_1 \bar{g}_2$. We show (3.2) is onto (which in the $n = 1$ case is the familiar surjectivity of $\mathbf{Z}_p^\times \longrightarrow \mathbf{F}_p^\times$ by $a \mapsto a \bmod p$, unlike that of $\mathbf{Z}^\times \longrightarrow \mathbf{F}_p^\times$). Let $\varphi \in \mathrm{Aut}_{\mathbf{F}_p}(L/pL)$, so

$$\varphi : L/pL \longrightarrow L/pL$$

is $\mathbf{F}_p$-linear. Since

$$L/pL = \sum_{i=1}^n \mathbf{F}_p \bar{\mathbf{e}}_i,$$

we have

$$\varphi(\bar{\mathbf{e}}_j) = \sum_{i=1}^n \bar{a}_{ij} \bar{\mathbf{e}}_i,$$

where $a_{ij} \in \mathbf{Z}_p$ reduces to the coefficients of $\mathbf{e}_i$. Set $A = (a_{ij}) \in \mathrm{M}_n(\mathbf{Z}_p)$. Since

$$\det(\bar{A}) = \det(\bar{a}_{ij}) \not\equiv 0 \bmod p,$$

$\det A \in \mathbf{Z}_p^\times$, so $A \in \mathrm{GL}_n(\mathbf{Z}_p)$.

Now define $\Phi : \mathbf{Q}_p^n \longrightarrow \mathbf{Q}_p^n$ to have matrix A in the basis $\{\mathbf{e}_i\}$:

$$\Phi(\mathbf{e}_j) = \sum_{i=1}^n a_{ij} \mathbf{e}_i \in L.$$

Then $\Phi(L) \subset L$. With respect to the basis $\{\mathbf{e}_i\}$, the matrix representation of Φ is $(a_{ij}) \in \mathrm{GL}_n(\mathbf{Z}_p)$. Let $(b_{ij}) = (a_{ij})^{-1} \in \mathrm{GL}_n(\mathbf{Z}_p)$ and define $\Psi : \mathbf{Q}_p^n \longrightarrow \mathbf{Q}_p^n$ by

$$\Psi(\mathbf{e}_j) = \sum_{i=1}^n b_{ij} \mathbf{e}_i \in L.$$

Then Φ and Ψ are inverses on $\mathbf{Q}_p^n$ and $\Psi(L) \subset L$. Applying Φ to both sides gives $L \subset \Phi(L)$. Thus $\Phi(L) = L$, so $\Phi \in K_L$ and (by reducing coefficients) we have $\bar{\Phi} = \varphi$. This proves $K_L \to \mathrm{Aut}_{\mathbf{F}_p}(L/pL)$ is onto.

Now we're in a position to use Lemma 3.2. For each $\varphi \in \mathrm{Aut}_{\mathbf{F}_p}(L/pL) = \mathrm{GL}(V)$, there is a $\Phi \in K_L$ that reduces to φ. Since $K_L \subset K_{L'}$ (!), $\Phi(L') \subset L'$, so

$$\Phi(L' + pL) \subset L' + pL.$$

Reduce this containment modulo pL to get $\varphi(W) \subset W$. Since φ is invertible on V, φ preserves dimensions, so $\varphi(W) = W$. This holds for all $\varphi \in \mathrm{Aut}_{\mathbf{F}_p}(L/pL)$, so $W = 0$ or $W = V$ by Lemma 3.2. Since $W \neq 0$, $W = V$. Thus

$$(L' + pL)/pL = L/pL,$$

so $L' + pL = L$. Hence "mod p" we have $L' = L$, and we want to prove there is actual equality of the two lattices in $\mathbf{Q}_p^n$.

We already have $L' \subset L$, so we will show that $L \subset L'$. We will do this in two ways. The first way will use an approximation method of the same kind we used twice already to show a locally compact normed vector space over a locally compact valued field is finite-dimensional and to show $n = ef$ for p-adic fields (that was the argument that went from $\mathcal{O}_K \subset M + p\mathcal{O}_K$ to $\mathcal{O}_K = M$). The second way will involve no limits at all and will be purely algebraic (it in fact is the proof of a special case of Nakayama's lemma from commutative algebra).

Since $L = L' + pL$, we can feed L into the right side to get

$$L = L' + p(L' + pL) \subset L' + p^2 L,$$

and then by induction

$$L \subset L' + p^m L$$

for all $m \geq 1$. Thus to each $v \in L$ we can find a sequence of $v'_m \in L'$ with $v - v'_m \in p^m L$, so $v'_m \to v$ as $m \to \infty$ (use the sup-norm with respect to the basis $\{\mathbf{e}_j\}$ here to see this concretely). Thus L lies in the closure of L'. Being a lattice in $\mathbf{Q}_p^n$, L' is compact, and therefore closed, so $L \subset L'$.

For our second proof, recall

$$L = \sum_{i=1}^n \mathbf{Z}_p \mathbf{e}_i \qquad \text{and} \qquad L' = \sum_{j=1}^n \mathbf{Z}_p \mathbf{f}_j.$$

From $L = L' + pL$, we can write

$$\mathbf{e}_i = \sum_{j=1}^n a_{ij}\mathbf{f}_j + \sum_{j=1}^n b_{ij}\mathbf{e}_j$$

for all i, where a_{ij} and b_{ij} are p-adic integers with $|b_{ij}|_p < 1$. We now have the system of equations

$$\begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix} = (a_{ij}) \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_n \end{pmatrix} + (b_{ij}) \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix}.$$

Set $A = (a_{ij})$ and $B = (b_{ij})$, so $A \in \mathrm{M}_n(\mathbf{Z}_p)$ and $B \in \mathrm{M}_n(p\mathbf{Z}_p)$. Then

$$\begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix} = A \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_n \end{pmatrix} + B \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix},$$

so

$$(I_n - B) \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix} = A \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_n \end{pmatrix}. \tag{3.3}$$

The matrix $I_n - B$ is in $\mathrm{M}_n(\mathbf{Z}_p)$ and reduces modulo p to $I_n - B \equiv I_n \bmod p$, so $\det(I_n - B) \equiv 1 \bmod p$. Hence $I_n - B \in \mathrm{GL}_n(\mathbf{Z}_p)$. Multiplying both sides of (3.3) by $(I_n - B)^{-1}$ shows us that all the $\mathbf{e}_i$'s are in L', so $L \subset L'$ and we are done. $\square$

Theorem 3.4. *The group $\mathrm{GL}_n(\mathbf{Z}_p)$ is a maximal compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$, and the maximal compact subgroups of $\mathrm{GL}_n(\mathbf{Q}_p)$ are precisely the conjugates of $\mathrm{GL}_n(\mathbf{Z}_p)$. Furthermore, every compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$ is contained in a maximal compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$.*

Proof. Suppose $\mathrm{GL}_n(\mathbf{Z}_p)$ is contained in a compact subgroup H of $\mathrm{GL}_n(\mathbf{Q}_p)$. Theorem 1.2 shows that there exists a lattice M such that $H \subset K_M$. Hence $\mathrm{GL}_n(\mathbf{Z}_p) \subset K_M$, but $\mathrm{GL}_n(\mathbf{Z}_p) = K_{\mathbf{Z}_p^n}$, so by Theorem 3.3, $\mathrm{GL}_n(\mathbf{Z}_p) = K_M$. Then $H \subset K_M = \mathrm{GL}_n(\mathbf{Z}_p) \subset H$, so $H = \mathrm{GL}_n(\mathbf{Z}_p)$. Conjugation preserves containments, so every conjugate of $\mathrm{GL}_n(\mathbf{Z}_p)$ is a maximal compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$.

By Theorem 3.1, every compact subgroup H of $\mathrm{GL}_n(\mathbf{Q}_p)$ is contained in $g\,\mathrm{GL}_n(\mathbf{Z}_p)g^{-1}$ for some $g \in \mathrm{GL}_n(\mathbf{Q}_p)$, so the conjugates of $\mathrm{GL}_n(\mathbf{Z}_p)$ are maximal in $\mathrm{GL}_n(\mathbf{Q}_p)$ and every compact subgroup is contained in one of these maximal compact subgroups. $\square$

The proofs above generalize with essentially no change to $\mathrm{GL}_n(K)$ for a p-adic field K (which in fact is the setting that is handled in [1]):

Theorem 3.5. *The maximal compact subgroups of $\mathrm{GL}_n(K)$ are the conjugates of $\mathrm{GL}_n(\mathcal{O}_K)$ and every compact subgroup of $\mathrm{GL}_n(K)$ is contained in a conjugate of $\mathrm{GL}_n(\mathcal{O}_K)$.*

In the proof, lattices in K^n are used. A lattice in K^n, by definition, is the $\mathcal{O}_K$-span of a basis of K^n. There are two points worth making about how the proof over $\mathbf{Q}_p$ adapts to the more general case:

(1) Lemma 2.6 goes through in K^n by the same argument used in $\mathbf{Q}_p^n$, so a finite sum of lattices in K^n is a lattice by the same proof used for lattices in $\mathbf{Q}_p^n$ (Lemma 2.8).
(2) If L is a lattice in K^n, and π is a prime in $\mathcal{O}_K$, $L/\pi L$ is a vector space over the residue field $\mathbf{k} = \mathcal{O}_K/\pi\mathcal{O}_K$ of K (and not just an $\mathbf{F}_p$-vector space as before). Any element of $\mathrm{GL}_n(K)$ that sends L onto itself induces a $\mathbf{k}$-linear automorphism of $L/\pi L$ and all such automorphisms arise in this way. The proof of that is identical to the $\mathbf{Q}_p$-case.

Replacing $\mathrm{GL}_n(K)$ with other matrix groups over K, there could be more than one conjugacy class of maximal compact subgroups. For example, although in $\mathrm{SL}_n(\mathbf{R})$ all maximal compact subgroups are conjugate to a subgroup of $\mathrm{SO}_n(\mathbf{R})$, the group $\mathrm{SL}_n(K)$ has n conjugacy classes of maximal compact subgroups. Taking $n = 2$, the two conjugacy classes of maximal compact subgroups of $\mathrm{SL}_2(K)$ are $\mathrm{SL}_2(\mathcal{O}_K)$ and $\left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)\mathrm{SL}_2(\mathcal{O}_K)\left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$, where π is a prime of K.

Appendix A. Orthogonal groups over $\mathbf{Q}_p$

The group $\mathrm{O}_n(\mathbf{R})$ is compact because in $\mathrm{M}_n(\mathbf{R})$ it is closed (the condition $AA^\top = I_n$ is a finite system of polynomial equations on the matrix entries) and bounded (the rows of A are mutually orthogonal unit vectors, or equivalently the columns of A are mutually orthogonal unit vectors since $A^\top A = I_n$ is also a defining property of $\mathrm{O}_n(\mathbf{R})$). If we work over $\mathbf{C}$ instead of $\mathbf{R}$, the group $\mathrm{O}_1(\mathbf{C}) = S^1$ is compact, but $\mathrm{O}_n(\mathbf{C})$ for $n \geq 2$ is *not* compact because matrix entries can be unbounded: for arbitrary $z \in \mathbf{C}$, we can solve $w^2 = 1 - z^2$ for some w in $\mathbf{C}$, and the matrix $\left(\begin{smallmatrix} z & w \\ w & -z \end{smallmatrix}\right)$ is in $\mathrm{O}_2(\mathbf{C})$. For $n \geq 3$, using that 2×2 matrix as the upper left block with 1's on the rest of the main diagonal gives us matrices in $\mathrm{O}_n(\mathbf{C})$ with unbounded entries.

When $n = 1$, $\mathrm{O}_n(\mathbf{Q}_p) = \{\pm 1\}$ is compact (and it's smaller than the maximal compact subgroup $\mathbf{Z}_p^\times$ of $\mathrm{GL}_1(\mathbf{Q}_p) = \mathbf{Q}_p^\times$). The compactness of $\mathrm{O}_2(\mathbf{Q}_p)$ depends on $p \bmod 4$.

Theorem A.1. *If $p \not\equiv 1 \bmod 4$ then $\mathrm{O}_2(\mathbf{Q}_p)$ is compact and is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$.*

Proof. The group $\mathrm{O}_2(\mathbf{Q}_p)$ is closed since its defining condition $AA^\top = I_2$ is polynomial equations on the matrix entries. It remains to show the entries of a matrix in $\mathrm{O}_2(\mathbf{Q}_p)$ are bounded.

The rows (and columns) of a matrix in $\mathrm{O}_2(\mathbf{Q}_p)$ have entries x and y in $\mathbf{Q}_p$ that satisfy $x^2 + y^2 = 1$. We'll show when $p \not\equiv 1 \bmod 4$ that such x and y must be in $\mathbf{Z}_p$. If $y \in \mathbf{Z}_p$ then $x \in \mathbf{Z}_p$ since $x^2 = 1 - y^2 \in \mathbf{Z}_p$, and if $x \in \mathbf{Z}_p$ then $y \in \mathbf{Z}_p$. So if x or y is not in $\mathbf{Z}_p$ then neither is in $\mathbf{Z}_p$, and $|x|_p = |y|_p$ by $x^2 + y^2 = 1$ and the non-Archimedean triangle inequality.

Writing $|x|_p = |y|_p = p^r$ where $r \geq 1$, $x = u/p^r$ and $y = v/p^r$ where $u, v \in \mathbf{Z}_p^\times$. Then $1 = x^2 + y^2 = (u^2 + v^2)/p^{2r}$, so $u^2 + v^2 = p^{2r} \equiv 0 \bmod p^2$. Therefore $-1 \equiv (u/v)^2 \bmod p^2$, which for prime p forces $p \equiv 1 \bmod 4$ (it doesn't hold for $p = 2$ since $-1 \bmod 4$ is not a square even though $-1 \mod 2$ is a square). So when $p \not\equiv 1 \bmod 4$, all matrices in $\mathrm{O}_2(\mathbf{Q}_p)$ have entries in $\mathbf{Z}_p$ and thus these matrices are bounded. Since the determinant of an orthogonal matrix is ± 1, we have shown $\mathrm{O}_2(\mathbf{Q}_p) \subset \mathrm{GL}_2(\mathbf{Z}_p)$. $\square$

Theorem A.2. *If $p \equiv 1 \bmod 4$ then $\mathrm{O}_2(\mathbf{Q}_p)$ is not compact.*

Proof. We are going to think of $\mathrm{O}_2(\mathbf{Q}_p)$ in the sense of (1.2), as matrices preserving the dot product on $\mathbf{Q}_p^2$:

$$\mathrm{O}_2(\mathbf{Q}_p) = \{A \in \mathrm{GL}_2(\mathbf{Q}_p) : Av \cdot Aw = v \cdot w \text{ for all } v \text{ and } w \text{ in } \mathbf{Q}_p^2\}.$$

For $p \equiv 1 \bmod 4$, -1 is a square in $\mathbf{Z}_p^\times$, say $-1 = a^2$. The vectors $v = \binom{a}{1}$ and $w = \binom{-a}{1}$ in $\mathbf{Q}_p^2$ are a basis and $v \cdot v = 0$, $w \cdot w = 0$, and $v \cdot w = -a^2 + 1 = 2$, so for x and y in $\mathbf{Q}_p$,

$$(xv + yw) \cdot (xv + yw) = x^2(v \cdot v) + 2xyv \cdot w + y^2(w \cdot w) = 4xy.$$

For each $c \in \mathbf{Q}_p^\times$, the linear map $A_c \colon \mathbf{Q}_p^2 \to \mathbf{Q}_p^2$ where $A_c(xv + yw) = cxv + (1/c)yw$ (the matrix of A_c in the basis $\{v, w\}$ is $\left(\begin{smallmatrix} c & 0 \\ 0 & 1/c \end{smallmatrix}\right)$) preserves the dot product:

$$A_c(xv + yw) \cdot A_c(xv + yw) = 4(cx)((1/c)y) = 4xy = (xv + yw) \cdot (xv + yw),$$

so $A_c \in \mathrm{O}_2(\mathbf{Q}_p)$ (in fact, $A_c \in \mathrm{SO}_2(\mathbf{Q}_p)$ since $\det(A_c) = 1$), and since c is unbounded the group $\mathrm{O}_2(\mathbf{Q}_p)$ is not compact. $\square$

The compactness or noncompactness of $\mathrm{O}_n(\mathbf{Q}_p)$ for $n \geq 3$ is as follows, and will be explained below:

- for $n = 3$ and 4, $\mathrm{O}_n(\mathbf{Q}_2)$ is compact and $\mathrm{O}_3(\mathbf{Z}_2) \subset \mathrm{GL}_3(\mathbf{Z}_2)$, but $\mathrm{O}_4(\mathbf{Z}_2) \not\subset \mathrm{GL}_4(\mathbf{Z}_2)$,
- $\mathrm{O}_n(\mathbf{Q}_2)$ is noncompact when $n \geq 5$,
- for $p \neq 2$ and $n \geq 3$, $\mathrm{O}_n(\mathbf{Q}_p)$ is not compact.

To prove compactness of $\mathrm{O}_n(\mathbf{Q}_2)$ for $n = 3$ and $n = 4$, we'll use the following lemma about 2-adic absolute values of sums of 2, 3, and 4 squares in $\mathbf{Q}_2$.

Lemma A.3. *On $\mathbf{Q}_2$, let $|\cdot|$ denote $|\cdot|_2$. For x and y in $\mathbf{Q}_2$,*

$$|x^2 + y^2| = \begin{cases} |x^2|, & \text{if } |x| > |y|, \\ \frac{1}{2}|x^2|, & \text{if } |x| = |y|. \end{cases}$$

For $x, y, z \in \mathbf{Q}_2$,

$$|x^2 + y^2 + z^2| = \begin{cases} |x^2|, & \text{if } |x| > |y|, |z| \quad \text{or} \quad \text{if} \quad |x| = |y| = |z|, \\ \frac{1}{2}|x^2|, & \text{if } |x| = |y| > |z|. \end{cases}$$

For $x, y, z, w \in \mathbf{Q}_2$,

$$|x^2+y^2+z^2+t^2| = \begin{cases} |x^2|, & \text{if } |x| > |y|, |z|, |t| \text{ or if } |x| = |y| = |z| > |t|, \\ \frac{1}{2}|x^2|, & \text{if } |x| = |y| > |z|, |t|, \\ \frac{1}{4}|x^2|, & \text{if } |x| = |y| = |z| = |t|. \end{cases}$$

Proof. If $|x| > |y|$, then $|x^2| > |y^2|$, so $|x^2 + y^2| = |x^2| = |x|^2$ by the non-Archimedean triangle inequality.

If $|x| = |y|$, first assume the common value is 0, *i.e.*, x and y are 0. Then $x^2 + y^2 = 0$, so $|x^2 + y^2| = 0 = \frac{1}{2}|x^2|$. If the common value is not 0, let it be $1/2^r$. Then $x = 2^r u$ and $y = 2^r v$ for u and v in $\mathbf{Z}_2^\times$, so $x^2+y^2 = 4^r(u^2+v^2)$. Since $u^2, v^2 \equiv 1 \bmod 4$, $|u^2+v^2| = 1/2$. Thus $|x^2 + y^2| = (1/4^r)(1/2) = \frac{1}{2}|x^2|$.

Now we look at a sum of three squares. If $|x|$, $|y|$, and $|z|$ have a maximum uniquely at $|x|$, then $|x^2 + y^2 + z^2| = |x^2|$ by the non-Archimedean triangle inequality.

If $|x|$, $|y|$, and $|z|$ have a maximum at x and y but not at z, then $|x^2 + y^2| = \frac{1}{2}|x^2|$ by the case of sums of two squares, and we'll show $\frac{1}{2}|x^2| > |z^2|$: it is obvious if $z = 0$, and if $z \neq 0$ then $|x| = |y| \geq 2|z|$ (since nonzero 2-adic absolute values are integral powers of 2), so $|x^2| \geq 4|z^2|$, so $\frac{1}{2}|x^2| \geq 2|z^2| > |z^2|$. Thus $|x^2+y^2| > |z^2|$, so $|x^2+y^2+z^2| = |x^2+y^2| = \frac{1}{2}|x^2|$.

If $|x| = |y| = |z| = 0$, then $|x^2 + y^2 + z^2| = 0 = |x^2|$. If $|x| = |y| = |z| \neq 0$, then $x = 2^r u$, $y = 2^r v$, and $z = 2^r w$ for some $r \in \mathbf{Z}$ and u, v, and w in $\mathbf{Z}_2^\times$, so $x^2+y^2+z^2 = 4^r(u^2+v^2+w^2)$. Since $u^2 + v^2 + w^2 \equiv 1 + 1 + 1 \equiv 3 \bmod 4$, $|x^2 + y^2 + z^2| = 1/4^r = |x^2|$.

The last case is a sum of four squares. If $|x|$, $|y|$, $|z|$, and $|t|$ have a maximum uniquely at $|x|$, then $|x^2 + y^2 + z^2 + t^2| = |x^2|$ by the non-Archimedean triangle inequality.

Suppose the maximum absolute value is only at x and y. Then $|z|, |t| \leq (1/2)|x|$, so $|z^2 + t^2| \leq (1/4)|x^2| < (1/2)|x^2| = |x^2 + y^2|$ by the formula for a sum of two squares. Thus $|x^2 + y^2 + z^2 + t^2| = |x^2 + y^2| = \frac{1}{2}|x^2|$.

Suppose the maximum absolute value is at x, y, and z but not at t. Then $|x^2+y^2+z^2| = |x^2| > |t^2|$ by the case of a sum of three squares, so $|x^2+y^2+z^2+t^2| = |x^2+y^2+z^2| = |x^2|$.

Finally, suppose $|x| = |y| = |z| = |t|$. If the common absolute value is 0, so all the numbers are 0, then $|x^2 + y^2 + z^2 + t^2| = 0 = \frac{1}{4}|x^2|$. If the common absolute value is not 0, then we can write $x = 2^r u$, $y = 2^r v$, $z = 2^r w$, and $t = 2^r s$ for some $r \in \mathbf{Z}$ and u, v, w, s in $\mathbf{Z}_2^\times$. Thus

$$x^2 + y^2 + z^2 + t^2 = 4^r(u^2 + v^2 + w^2 + s^2)$$

and $u^2+v^2+w^2+s^2 \equiv 1+1+1+1 \equiv 4 \bmod 8$, so $|x^2+y^2+z^2+t^2| = (1/4^r)(1/4) = \frac{1}{4}|x^2|$. □

Theorem A.4. *The groups $\mathrm{O}_3(\mathbf{Q}_2)$ and $\mathrm{O}_4(\mathbf{Q}_2)$ are compact, with $\mathrm{O}_3(\mathbf{Z}_3) \subset \mathrm{GL}_3(\mathbf{Z}_2)$ and $\mathrm{O}_4(\mathbf{Z}_2) \not\subset \mathrm{GL}_4(\mathbf{Z}_2)$, respectively.*

Proof. The groups $\mathrm{O}_3(\mathbf{Q}_2)$ and $\mathrm{O}_4(\mathbf{Q}_2)$ are closed in $\mathrm{M}_3(\mathbf{Q}_2)$ and $\mathrm{M}_4(\mathbf{Q}_2)$, since the matrix entries are solutions to some polynomial equations. We'll show the matrix entries are all bounded, so the orthogonal groups are compact. It will turn out matrices in $\mathrm{O}_3(\mathbf{Q}_2)$ have entries in $\mathbf{Z}_2$ and matrices in $\mathrm{O}_4(\mathbf{Q}_2)$ have entries in $\frac{1}{2}\mathbf{Z}_2$.

As in the proof of Lemma A.3, we'll use $|\cdot|$ for $|\cdot|_2$.

The 3×3 case. Each column of a matrix in $\mathrm{O}_3(\mathbf{Q}_2)$ is a triple (x, y, z) where $x^2+y^2+z^2 = 1$, so $|x^2 + y^2 + z^2| = 1$. Without loss of generality, let $\max(|x|, |y|, |z|) = |x|$.

From Lemma A.3, if $|x|$, $|y|$, and $|z|$ have a maximum at 1 or 3 of these numbers then $1 = |x^2 + y^2 + z^2| = |x^2|$, so all three of x, y, and z are in $\mathbf{Z}_2$.

If the maximum absolute value occurs at exactly two of the numbers, then $1 = \frac{1}{2}|x^2|$, so $|x^2| = 2$, which is impossible. Thus $\mathrm{O}_3(\mathbf{Z}_2) \subset \mathrm{M}_3(\mathbf{Z}_2)$. Since orthogonal matrices have determinant ± 1, and $\pm 1 \in \mathbf{Z}_2^\times$, $\mathrm{O}_3(\mathbf{Q}_2) \subset \mathrm{GL}_3(\mathbf{Z}_2)$.

The 4×4 case. The matrix

$$\begin{pmatrix} 1/2 & 1/2 & -1/2 & 1/2 \\ 1/2 & 1/2 & 1/2 & -1/2 \\ 1/2 & -1/2 & -1/2 & -1/2 \\ 1/2 & -1/2 & 1/2 & 1/2 \end{pmatrix}$$

is in $\mathrm{O}_4(\mathbf{Q}_2)$, so $\mathrm{O}_4 \not\subset \mathrm{GL}_4(\mathbf{Z}_2)$. To show all entries of matrices in $\mathrm{O}_4(\mathbf{Q}_2)$ are in $\frac{1}{2}\mathbf{Z}_2$, we'll show that if $|x^2+y^2+z^2+t^2| = 1$ then $x, y, z, t \in \frac{1}{2}\mathbf{Z}_2$.

If $|x^2+y^2+z^2+t^2| = 1$ and $\max(|x|, |y|, |z|, |t|) = |x|$, then by the formula in Lemma A.3 for $|x^2+y^2+z^2+t^2|$ we have either (i) $|x^2| = 1$ or (ii) $\frac{1}{4}|x^2| = 1$ (the equation $\frac{1}{2}|x^2| = 1$ is impossible). For (i), we have $|y|, |z|, |t| \leq |x| = 1$, so $x, y, z, t \in \mathbf{Z}_2$. For (ii), we have $|y|, |z|, |t| \leq |x| = 2$, so $x, y, z, t \in \frac{1}{2}\mathbf{Z}_2$. □

Here is an application of this theorem to matrix groups over $\mathbf{Q}$.

Corollary A.5. *Every entry of a matrix in $\mathrm{O}_3(\mathbf{Q})$ has an odd denominator, and every entry of a matrix in $\mathrm{O}_4(\mathbf{Q})$ has a denominator that is odd or an odd multiple of 2.*

Proof. Since $\mathrm{O}_3(\mathbf{Q})$ is contained in $\mathrm{O}_3(\mathbf{Q}_2)$, every matrix in $\mathrm{O}_3(\mathbf{Q})$ has entries in $\mathbf{Z}_2$ and thus the entries are rational numbers with odd denominators. Similarly, since $\mathrm{O}_4(\mathbf{Q}) \subset \mathrm{O}_4(\mathbf{Q}_2)$, the entries of a matrix in $\mathrm{O}_4(\mathbf{Q}_2)$ are in $\frac{1}{2}\mathbf{Z}_2$, so the denominators are divisible by 2 at most once. □

Our last task is to prove $\mathrm{O}_n(\mathbf{Q}_2)$ is noncompact for $n \geq 5$ and $\mathrm{O}_n(\mathbf{Q}_p)$ is noncompact when $p \neq 2$ and $n \geq 3$. This is explained in a common way by the next theorem.

Theorem A.6. *If $Q(x_1, \ldots, x_n)$ is a nondegenerate quadratic form on $\mathbf{Q}_p^n$ and there is a nonzero solution to $Q(v) = 0$, then $\mathrm{O}_Q(\mathbf{Q}_p)$ is noncompact.*

Proof. See https://mathoverflow.net/questions/370940. □

Apply this theorem to $x_1^2 + x_2^2 + \cdots + x_n^2$, which is a nondegenerate quadratic form on $\mathbf{Q}_p^n$ (both for $p = 2$ and $p \neq 2$) and it has a nontrivial zero if $p = 2$ and $n \geq 5$ and also if $p \neq 2$ and $n \geq 3$:[1] for $p = 2$, $-7 = \alpha^2$ for some $\alpha \in \mathbf{Z}_2^\times$ and $\alpha^2 + 2^2 + 1 + 1 + 1 = 0$ (pad the solution with extra 0's on the left if $n > 5$), while for $p \neq 2$, $x^2 + y^2 + 1 = 0$ for some x and y in $\mathbf{Z}_p$ (pad with extra 0's if $n > 3$) since the congruence $-1 \equiv x_0^2 + y_0^2 \bmod p$ has a solution where $x_0 \not\equiv 0 \bmod p$, and this can be lifted to a p-adic solution by Hensel's lemma.

Here is an analogous compactness theorem for orthogonal groups over $\mathbf{Q}_p$.

Theorem A.7. *If $Q(x_1, \ldots, x_n)$ is a nondegenerate quadratic form on $\mathbf{Q}_p^n$ and the only solution to $Q(v) = 0$ on $\mathbf{Q}_p^n$ is $v = \mathbf{0}$, then $\mathrm{O}_Q(\mathbf{Q}_p)$ is compact.*

Proof. See https://mathoverflow.net/questions/90117. □

The quadratic form $x_1^2 + x_2^2 + \cdots + x_n^2$ on $\mathbf{Q}_p^n$ fits the conditions of Theorem A.7 if $p = 2$ and $n \leq 4$, if $p \equiv 3 \bmod 4$ and $n \leq 2$, and if $p \equiv 1 \bmod 4$ and $n = 1$. So this theorem recovers the compactness of $\mathrm{O}_2(\mathbf{Q}_p)$ for $p \not\equiv 1 \bmod 4$ in Theorem A.1 and the compactness of $\mathrm{O}_3(\mathbf{Q}_2)$ and $\mathrm{O}_4(\mathbf{Q}_2)$ in Theorem A.4, but it doesn't tell us the more refined information about when $\mathrm{O}_n(\mathbf{Q}_p) \subset \mathrm{GL}_n(\mathbf{Z}_p)$ in Theorems A.1 and A.4.

References

[1] J.-P. Serre, "Lie Algebras and Lie Groups," 2nd ed., Springer-Verlag, New York, 1965.

[1] Also if $p \equiv 1 \bmod 4$ and $n = 2$ since -1 is a square in $\mathbf{Z}_p^\times$.