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

KEITH CONRAD

Although the algebraic closure $\overline{\mathbf{Q}}_p$ is an infinite-degree extension of $\mathbf{Q}_p$, each finite subset $\{\alpha_1, \dots, \alpha_m\}$ of $\overline{\mathbf{Q}}_p$ lies in a finite extension of $\mathbf{Q}_p$, since the field $\mathbf{Q}_p(\alpha_1, \dots, \alpha_m)$ is a finite extension of $\mathbf{Q}_p$. It follows that every individual matrix in $\mathrm{GL}_n(\overline{\mathbf{Q}}_p)$ lies in $\mathrm{GL}_n(F)$ for some finite extension $F/\mathbf{Q}_p$: choose F to be the field generated over $\mathbf{Q}_p$ by all the entries of the matrix. The theorem we will discuss here is an analogue of this property for a compact group of matrices.

Theorem 1. *For each compact subgroup K of $\mathrm{GL}_n(\overline{\mathbf{Q}}_p)$, there is a finite extension $F/\mathbf{Q}_p$ such that $K \subset \mathrm{GL}_n(F)$.*

Proof. Our argument is due to W. Sinnott. Let $G = \mathrm{GL}_n(\overline{\mathbf{Q}}_p)$ and $\overline{\mathbf{Z}}_p$ be the integers of $\overline{\mathbf{Q}}_p$. For $r \geq 1$, set

$$G_r = I_n + p^r \mathrm{M}_n(\overline{\mathbf{Z}}_p).$$

This is an open subgroup of G and

$$G \supset G_1 \supset G_2 \supset G_3 \supset \cdots,$$

with G_r lying in an arbitrarily small neighborhood of I_n as $r \to \infty$. The elements of G_r have matrix entries p-adically termwise close to the entries of the $n \times n$ identity matrix. For each $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ we have $\sigma(G_i) = G_i$. For g and g' in G, the condition $g \equiv g' \bmod G_r$ means $g \in g'G_r = g'(I_n + p^r \mathrm{M}_n(\mathbf{Z}_p))$, so in a multiplicative sense the matrix entries of g and g' are p-adically close.

Since G_r is open in G, the intersection

$$K_r = K \cap G_r$$

is an open subgroup of K and

$$K \supset K_1 \supset K_2 \supset K_3 \supset \cdots,$$

with K_r lying in an arbitrarily small neighborhood of the identity matrix as $r \to \infty$. An open subgroup of a compact group is closed and has finite index, so K_r is compact and $[K : K_r]$ is finite. If some K_r is contained in $\mathrm{GL}_n(F)$ for some finite extension F of $\mathbf{Q}_p$, then K itself lies in $\mathrm{GL}_n(F')$ where F' is the field generated over F by the matrix entries from the finitely many (say, left) coset representatives for K/K_r in K. The entries of a matrix in K are all algebraic over $\mathbf{Q}_p$, so F' is a finite extension field of F. This means $[F' : \mathbf{Q}_p]$ is finite and $K \subset \mathrm{GL}_n(F')$, so we'd be done.

Assume, to the contrary, that for each finite extension $F/\mathbf{Q}_p$, no K_r is contained in $\mathrm{GL}_n(F)$. Since there are only a finite number of extensions of $\mathbf{Q}_p$ inside $\overline{\mathbf{Q}}_p$ with degree below a given bound, for each $d \geq 1$ the composite of all finite extensions of $\mathbf{Q}_p$ with degree $< d$ is a finite extension of $\mathbf{Q}_p$. Therefore our assumption implies that

(1) every K_r contains a matrix with an entry of arbitrarily large degree over $\mathbf{Q}_p$.

We will recursively find positive integers $d_1 < d_2 < \cdots$ and matrices $g_i \in K_{d_i}$ for each $i \geq 1$ such that

(a) some entry in g_i has degree at least i over $\mathbf{Q}_p$,

(b) for all $\sigma \in \operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, if $\sigma(g_i) \neq g_i$ then $\sigma(g_i) \not\equiv g_i \bmod G_{d_{i+1}}$, *i.e.*, $\sigma(g_i) \notin g_i G_{d_{i+1}}$.

Before we construct the integers d_i and matrices g_i, note that for each $g \in \operatorname{GL}_n(\overline{\mathbf{Q}}_p)$ the set of all possible $\sigma(g)$ as σ runs over $\operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ is finite since each entry of g has only finitely many $\mathbf{Q}_p$-conjugates.

Choose $d_1 \geq 1$ and $g_1 \in K_{d_1}$ arbitrarily. Condition a is obvious for $i = 1$. Since g_1 has only finitely many conjugates $\sigma(g_1)$, where $\sigma \in \operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, for sufficiently large r the open set $g_1 G_r$ doesn't contain a matrix of the form $\sigma(g_1)$ other than those that equal g_1. Let d_2 be such an r with $d_2 > d_1$. That makes condition b true for $i = 1$. Next, suppose $g_1, \ldots, g_j$ and $d_1, \ldots, d_{j+1}$ have been chosen to satisfy conditions a and b for $i = 1, \ldots, j$. By (1), $K_{d_{j+1}}$ contains a matrix g_{j+1} with an entry having degree at least $j+1$ over $\mathbf{Q}_p$. Since g_{j+1} has only finitely many conjugates by $\operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ we can choose $d_{j+2} > d_{j+1}$ to satisfy condition b for $i = j+1$ in the same way we chose d_2 after choosing d_1 and g_1.

We want to work with the infinite product $h := g_1 g_2 \cdots$. To check it converges and to approximate it using partial products, we switch our focus to the subgroups G_{d_i}, which shrink to the identity in a controlled way through the powers of p defining them. Since $g_i \in G_{d_i} \subset K$, $d_i \to \infty$, and K is closed in G, the product $h := g_1 g_2 \cdots$ converges in K. We are going to look at automorphisms $\sigma \in \operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ that fix h. For every such σ,

$$\sigma(g_1)\sigma(g_2)\cdots = g_1 g_2 \cdots .$$

Suppose $\sigma(g_i) \neq g_i$ for some i. Let ℓ be the least such integer (it depends on σ). Then $\sigma(g_i) = g_i$ for all $i < \ell$, which means

$$\sigma(g_\ell)\sigma(g_{\ell+1})\cdots = g_\ell g_{\ell+1} \cdots .$$

For all $i > \ell$, $g_i \in G_{d_i} \subset G_{d_{\ell+1}}$ and $\sigma(g_i) \in \sigma(G_{d_i}) = G_{d_i} \subset G_{d_{\ell+1}}$, so $\sigma(g_\ell) \equiv g_\ell \bmod G_{d_{\ell+1}}$. Then condition b implies $\sigma(g_\ell) = g_\ell$, which is a contradiction. Therefore $\sigma(g_i) = g_i$ for all i. In other words, the subgroup of $\operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ fixing h fixes every entry of every g_i, and condition a implies the subgroup fixing h has a fixed field that is an infinite extension of $\mathbf{Q}_p$. However, all the entries of h lie in a finite extension of $\mathbf{Q}_p$, so the subgroup of $\operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ fixing h has a fixed field that is a finite extension of $\mathbf{Q}_p$. We have reached a contradiction. □

Remark 2. Replacing $\overline{\mathbf{Q}}_p$ by its completion $\mathbf{C}_p$, it is *false* that a general compact subgroup of $\operatorname{GL}_n(\mathbf{C}_p)$ is in $\operatorname{GL}_n(F)$ for some finite extension $F/\mathbf{Q}_p$. For example, inside $\operatorname{GL}_1(\mathbf{C}_p) = \mathbf{C}_p^\times$ we can pick $x \notin \overline{\mathbf{Q}}_p$ where $|x-1|_p < 1$ and take $K = x^{\mathbf{Z}_p}$.

The proof of Theorem 1 is similar in spirit to one of the proofs [1, pp. 182–183], [2, p. 71] that $\overline{\mathbf{Q}}_p$ is not complete: consider an infinite series $\sum_{i \geq 0} c_i p^i$ where the c_i's are in $\overline{\mathbf{Q}}_p$, $|c_i|_p = 1$, and $[\mathbf{Q}_p(c_i) : \mathbf{Q}_p] \to \infty$. By a suitable choice of c_i's, if that infinite series converges in $\overline{\mathbf{Q}}_p$ then a contradiction can be reached by comparing the series with a p-adic expansion of the limit. Turning things around, we can use the ideas in the proof of Theorem 1 to prove something about compact subgroups of the additive group $\overline{\mathbf{Q}}_p$.

Corollary 3. *Every compact subgroup of $\overline{\mathbf{Q}}_p$ is inside a finite extension of $\mathbf{Q}_p$.*

Proof. Repeat the proof of Theorem 1 for additive groups, *e.g.*, when K is a compact subgroup of $\overline{\mathbf{Q}}_p$ the intersections $K_r = K \cap p^r\overline{\mathbf{Z}}_p$ are compact subgroups of $\overline{\mathbf{Q}}_p$ with finite index in K and it suffices to show some K_r is in a finite extension of $\mathbf{Q}_p$. Or, more quickly, we can embed $\overline{\mathbf{Q}}_p$ as a subgroup of $\mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ by $a \mapsto \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, which lets us think of a compact subgroup of $\overline{\mathbf{Q}}_p$ as a compact subgroup of $\mathrm{GL}_2(\overline{\mathbf{Q}}_p)$. Then we can appeal to Theorem 1 when $n = 2$. □

References

[1] F. Q. Gouvea, "p-adic Numbers: An Introduction," 2nd ed., Springer–Verlag, New York, 1997.

[2] N. M. Koblitz, "p-adic Numbers, p-adic Analysis, and Zeta-functions," 2nd ed., Springer-Verlag, New York, 1984.