CHAPTER 9: APPLICATIONS OF LOCAL FIELDS

PETE L. CLARK

The topological groups $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ have an inexhaustibly rich structure and importance in all parts of modern mathematics: analysis, geometry, topology, representation theory, number theory....The serious study of these groups was already begun in the 19th century by Lie and his contemporaries.

Somewhat more recently (say, about 1950) it has been realized that for a non-Archimedean locally compact field K, the groups $\mathrm{GL}_n(K)$ also have a rich and useful structure.

We will give some of this structure theory here: namely, we will classify the maximal compact subgroups of $\mathrm{GL}_n(K)$ for K a nondiscrete locally compact field. This has immediate applications to the structure of finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$, which are of intrinsic interest and are quite useful in areas like representation theory and modular and automorphic forms. Moreover, this material (actually, a small piece of it suffices) can be combined with a beautiful embedding theorem of J.W.S. Cassels to deduce a celebrated 1960 theorem of A. Selberg: for any field K of characteristic 0, a finitely generated subgroup of $\mathrm{GL}_n(K)$ is virtually torsionfree: i.e., has a finite index subgroup without any nontrivial elements of finite order.

1. General linear groups over locally compact fields

1.1. $\mathrm{GL}_n(K)$ **is a locally compact group.** Let K be a nondiscrete locally compact field, and let n be a positive integer. We consider the group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices with coefficients in K. We wish to endow $\mathrm{GL}_n(K)$ with a natural locally compact topology. There are in fact two natural ways to do this, which, happily, lead to the same result.

For any $n \in \mathbb{Z}^+$, we endow the Cartesian product K^n with the product topology, which of course makes it a locally compact topological group. We will sometimes refer to this topology on K^n and other topologies induced from it as the **analytic topology**, to distinguish it from the Zariski topology. (However, the reader need not know what the Zariski topology is in order to read these notes.)

Let $M_n(K)$ be the ring of $n \times n$ matrices with entries in K. As a K-vector space, $M_n(K) \cong K^{n^2}$, and we give it the topology pulled back from the analytic topology on K^{n^2} via the isomorphism. (Easy exercise: the topology we get on $M_n(K)$ is independent of the chosen basis.)

Now $\mathrm{GL}_n(K)$ is a subset of $M_n(K)$. We claim that in the induced (subspace) topology it is locally compact, and indeed this is foisted off on the reader in the

form of the following straightforward exercises.

Exercise 9.1: Let $P(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ be a polynomial, thought of as an algebraic object. Then P induces a function $P : K^n \to K$ in the usual way: $(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n)$. Show that P is continuous for the analytic topologies on K^n and K.

Exercise 9.2: Deduce that $\mathrm{GL}_n(K)$ is an open subset of $M_n(K)$.

Exercise 9.3: A subset A of a topological space X is **locally closed** if it can be written in the form $U \cap V$, where U is open and V is closed.
a) Show that A is locally closed iff A is open in its closure $\overline{A}$.
b) Suppose that X is a locally compact Hausdorff space and A is a locally closed subset of X. Show that A is locally compact in the subspace topology.
c) Does the converse of part b) hold?

So $\mathrm{GL}_n(K)$, being an open subset of a locally compact space, is locally compact.

Now we give a second definition of the topology which is closely related to the "multiplicative" topology on the unit group of a topological ring. (Indeed, $\mathrm{GL}_n(K)$ is the group of units of the noncommutative topological ring $M_n(K)$, but never mind.) This definition realizes $\mathrm{GL}_n(K)$ as a closed subset of a K-vector space of one higher dimension. Namely, consider the subset of K^{n^2+1} given as the zero locus of the single polynomial $D(t_1, \ldots, t_{n^2})t_{n^2+1} - 1 = 0$, where D is the degree n polynomial giving the discriminant of an $n \times n$ matrix. There is a bijection between this locus and $\mathrm{GL}_n(K)$ as follows: write the entries of a matrix $M \in \mathrm{GL}_n(K)$ in linear order, say, $m_1, \ldots, m_{n^2}$; then to M we associate the point $(m_1, \ldots, m_{n^2}, \frac{1}{\det M}) \in K^{n^2+1}$. Then we may endow $\mathrm{GL}_n(K)$ with the subspace topology; being a closed subspace of the locally compact space K^{n^2+1}, it is locally compact.

Remark: This description shows that $\mathrm{GL}_n(K)$ is an affine algebraic variety rather than merely a quasi-affine algebraic variety.

Exercise 9.4: Show that the two topologies defined on $\mathrm{GL}_n(K)$ coincide.

1.2. **The orthogonal group of a quadratic form.**

We suppose that the characteristic of K is not 2 and $q(x) = a_1x_1^2 + \ldots + a_nx_n^2$ is a nonsingular quadratic form. There is an associated bilinear form $\langle x, y\rangle = \frac{1}{2}(q(x+y) - q(x) - q(y))$ and thus an associated **orthogonal group**

$$O(q) = \{M \in \mathrm{GL}_n(K) \mid \forall x, y \in K^n, \langle Mx, My\rangle = \langle x, y\rangle\}.$$

Equivalently, in terms of the natural action of $\mathrm{GL}_n(K)$ on symmetric matrices by conjugation – i.e., $P \mapsto G^T PG$ – the orthogonal group of q is precisely the stabilizer of the Gram matrix of q. Either way, $O(q)$ is clearly defined by the satisfaction of a finite system of polynomial equations, so is a linear algebraic group. Note that when $q = x_1^2 + \ldots + x_n^2$ we recover the "standard orthogonal group"

$$O(n) = \{M \in \mathrm{GL}_n(K) \mid MM^T = 1\}.$$

The structure of $O(q)$ is quite different depending upon whether the quadratic form q is isotropic or anisotropic. Indeed, there is the following general result.

Theorem 1. *Let K be a nondiscrete locally compact field, and q a nonsingular quadratic form. TFAE:*
(i) The orthogonal group $O(q)$ is compact.
(ii) The quadratic form q is anisotropic.

This result will be established in the Archimedean case in a sequence of exercises later in this section. We do not prove it in the non-Archimedean case here – nor will we use it – but the statement is sufficiently striking that we have presented it for the reader's edification.

1.3. **Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{R})$: orthogonal groups.** In the case of $K = \mathbb{R}$, a bilinear form $\langle , \rangle$ on $\mathbb{R}^n$ is said to be an **inner product** if it is positive-definite: for all $x \in \mathbb{R}^n$, $\langle x, x \rangle \geq 0$, with equality iff $x = 0$. Note that any two quadratic forms giving inner products are equivalent under the action of $\mathrm{GL}_n(K)$ (also called "isometric", but the formulation in terms of group actions will be convenient for us here), i.e., all inner products are conjugate to the standard inner product $\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1 y_1 + \ldots + x_n y_n$ coming from the sum of squares form $q(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2$.

Exercise 9.5:
a) Let G be a group acting on a set X. For $x \in X$, let $G_x = \{g \in G \mid gx = x\}$ be the stabilizer of x. Show that for any $g \in G$, $G_{gx} = gG_x g^{-1}$.
b) Deduce from part a) that in a transitive group action, all point stabilizers are conjugate subgroups of G.

Exercise 9.6:
a) Let $O(n)$ be the standard real orthogonal group, i.e., the orthogonal group associated to the standard inner product. Show that it is a compact subgroup $\mathrm{GL}_n(\mathbb{R})$.
b) Deduce from Exercise 9.5 that any orthogonal group associated to a positive definite quadratic form on $\mathbb{R}$ is conjugate to the standard orthogonal group $O(n)$.

Exercise 9.7:
a) If q is a quadratic form and $\alpha \in K^\times$, let αq be the quadratic form with coefficients scaled by α.[1] Show that $O(\alpha q) = O(q)$.
b) Conclude that the orthogonal group of any negative definite real quadratic form is also conjugate to $O(n)$, hence also compact.

Exercise 9.8: For $a, b \in \mathbb{N}$ with $a + b = n$, let $q_{a,b}$ be the diagonal quadratic form with a coefficients of $+1$ and b coefficients of -1. Let $O(a, b)$ be the orthogonal group of $q_{a,b}$.
a) Show that the orthogonal group of any nonsingular real quadratic form is conjugate to a unique $O(a, b)$ with $a \geq b$.
b) Show that if $a \geq b > 0$, $O(a, b)$ is *not compact*.

[1]Note: this not the same as acting on q by the scalar matrix αI_n: the latter gives $\alpha^2 q$, which is equivalent to q, whereas αq need not be.

Proposition 2. *A compact subgroup of* $\mathrm{GL}_n(\mathbb{R})$ *admits an invariant inner product.*

Proof. (Weyl) Start with any inner product $\langle , \rangle$, say the standard one. It need not be G-invariant, but we can make it G-invariant by "averaging" over the action of G. Namely, define a new inner product $\langle , \rangle_G$ by

$$\langle x, y \rangle_G := \int_G \langle gx, gy \rangle d\mu(g),$$

where $\mu(g)$ is the unit Haar measure on the compact group G. We leave it to the reader to check that this gives a G-invariant inner product. □

Remark: Some readers may remember this argument from courses in representation theory and/or functional analysis. It applies equally well to infinite-dimensional representations V of G and shows that they are all *orthogonalizable*. (More common is to consider complex representations and then the term *unitarizable* is more familiar. More on this coming up.) It follows from this that any G-invariant subspace W of V has a G-invariant complement, namely $W^\perp$ and thus any representation of a compact group is completely reducible. Note that in the case of a finite group this is known as Maschke's Theorem, and in this case the integral is just the usual sum over all values divided by $\#G$.

Theorem 3. *(Maximal compact subgroups of* $\mathrm{GL}_n(\mathbb{R})$*) Every compact subgroup is contained in the orthogonal group of a definite quadratic form. It follows that the maximal compact subgroups of* $\mathrm{GL}_n(\mathbb{R})$ *are precisely these definite orthogonal groups, that all maximal compact subgroups are conjugate, and that every compact subgroup is contained in a maximal compact subgroup.*

Proof. The first sentence is a restatement of Proposition 2. By Exercise 9.6, all definite orthogonal groups are conjugate. The rest follows immediately. □

1.4. Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{C})$: unitary groups.

Consider now the case of $\mathrm{GL}_n(\mathbb{C})$. If $n \geq 2$, then a quadratic form q in n variables over $\mathbb{C}$ is necessarily isotropic, so by Theorem X.X $O(q)$ is not compact. Indeed, over $\mathbb{C}$ any nonsingular q is equivalent to $x_1^2 + \ldots + x_n^2$, so we may again restrict to matrices M satisfying $MM^T = 1$. But the locus $q(x) = x_1^2 + \ldots + x_n^2 = 1$ is unbounded over $\mathbb{C}$, since indeed we may choose the first $n-1$ coordinates arbitrarily, and if x is any such vector, then it is easy to see that x can serve as the first column of an orthogonal matrix.[2]

However, from linear algebra we learn that the appropriate analogue of a bilinear form over $\mathbb{C}$ is a Hermitian form, i.e., an $\mathbb{R}$-bilinear form on $\mathbb{C}^n$ which is $\mathbb{C}$-linear in the first variables and conjugate linear in the second variable. The standard sesqulinear form is

$$\langle x, y \rangle = x_1 \overline{y_1} + \ldots + x_n \overline{y_n},$$

and this is positive definite in the sense that $\langle x, x \rangle \geq 0$ for all $x \in \mathbb{C}^n$ and is zero only if $x = 0$. To a Hermitian form H we associate its **unitary group**

$$U(H) = \{ g \in \mathrm{GL}_n(\mathbb{C}) \mid \forall x, y \in \mathbb{C}^n H(gx, gy) = H(x, y) \}.$$

[2]More generally, if $V_{/\mathbb{C}}$ is any affine variety of positive dimension, then $V(\mathbb{C})$ is not compact.

The unitary group associated to the standard Hermitian form is denoted $U(n)$.

Exercise 9.9: The unitary group of a Hermitian form is compact iff the form is positive definite.

The analogy to the real case should now be clear. We leave to the reader the proofs of the following results.

Proposition 4. *Any compact subgroup G of $\mathrm{GL}_n(\mathbb{C})$ admits a G-invariant positive definite Hermitian form.*

Theorem 5. *(Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{C})$) Every compact subgroup is contained in the unitary group of a definite Hermitian form. It follows that the maximal compact subgroups of $\mathrm{GL}_n(\mathbb{C})$ are precisely these definite unitary groups, that all maximal compact subgroups are conjugate, and that every compact subgroup is contained in a maximal compact subgroup.*

1.5. Maximal compact subgroups of GL_n over a non-Archimedean field: lattice stabilizers.

We now turn to the case of a non-Archimedean locally compact field K. In this case the maximal compact subgroups of $\mathrm{GL}_n(K)$ look quite different from the Archimedean case. This can be seen already in the case $n = 1$, i.e., $K^\times$.

- The maximal compact subgroup of $\mathbb{R}^\times$ is $\{\pm 1\} = O(1)$.
- The maximal compact subgroup of $\mathbb{C}^\times$ is $S^1 = U(1)$.

In each of these cases, the maximal compact subgroup is closed (of course!) but not open, and thus of smaller dimension than $\mathrm{GL}_n(K)$ itself. However, $K^\times$ admits **open** compact subgroups, namely $R^\times$. Although we have not developed a theory of non-Archimedean analytic manifolds and their dimensions, in some intuitive sense it is clear that both $K^\times$ and $R^\times$ have dimension one. (And indeed, this can be formalized.) In general, in the non-Archimedean case we have the following procedure for producing compact subgroups:

Theorem 6. *Let K be a NA locally compact field with valuation ring R. For any closed subgroup G of $\mathrm{GL}_n(K)$, define $G(R) := G \cap \mathrm{GL}_n(R)$. Then $G(R)$ is compact and open in G.*

Proof. Since G is closed in $\mathrm{GL}_n(K)$, $G(R) = G \cap \mathrm{GL}_n(R)$ is closed in $\mathrm{GL}_n(R)$. Thus it is enough to show that $\mathrm{GL}_n(R)$ is compact and open. Recall that we may view $\mathrm{GL}_n(K)$ as the closed subset of K^{n^2+1} of all pairs $(M, \alpha) \in M_n(K) \times K$ satisfying $\det(M)\alpha = 1$. Under this interpretation, clearly $\mathrm{GL}_n(R)$ is the closed subset of R^{n^2+1} of all pairs in $M_n(R) \times R$ satisfying the same relation. Since R^{n^2+1} is compact, so is $\mathrm{GL}_n(R)$. □

Now we momentarily work in a slightly more general setting: let R be a PID with fraction field K. We are interested in finding sufficient condition for a subgroup G of $\mathrm{GL}_n(K)$ to be conjugate to a subgroup of $\mathrm{GL}_n(R)$. The next few results are taken from [Ser].

Lemma 7. *Let $n \in \mathbb{Z}^+$, and let M be an R-submodule of K^n. TFAE:*
(i) M is a finitely generated R-module and M generates K^n as a K-module.
(ii) $M \cong R^n$.

Proof. (i) $\implies$ (ii). Since M is an R-submodule of K^n, it is torsion free. A finitely generated module over a PID is free, say $M \cong R^m$. There is a natural map $M \otimes_R K \to K^n$, which is surjective since M generates K^n as a K-module: thus $m \geq n$. On the other hand, a basis for M is an R-linearly independent set, hence also K-linearly independent (clear denominators), so by linear algebra $m \leq n$. (ii) $\implies$ (i): if $M \cong R^n$, then evidently M is finitely generated. If M did not generate K^n as a K-module, then the elements $e_1, \ldots, e_n$ of a basis for R form a K-linearly independent subset of K^n which does not span, contradicting linear algebra. □

An R-module M satisfying the equivalent conditions of Lemma 7 will be called a **lattice** in K^n. (Note that this usage is roughly analogous but not identical to that of a $\mathbb{Z}$-lattice in $\mathbb{R}^n$.)

Lemma 8. *For lattices $M_1, \ldots, M_k$ in K^n, $M = \langle M_1, \ldots, M_k \rangle_R$ is also a lattice.*

Proof. M is a finitely generated R-module whose K-span is K^n, so this follows immediately from Lemma 7. □

Fix $n \in \mathbb{Z}^+$, and let $\mathcal{L}$ denote the set of all R-lattices in K^n. Any element $\Lambda \in \mathcal{L}$ can be represented as $\langle v_1, \ldots, v_n \rangle_R$, where $(v_1, \ldots, v_n)$ is a K-basis for K^n. The natural (simply transitive) action of $\mathrm{GL}_n(K)$ on ordered bases of K^n induces a transitive action on $\mathcal{L}$. We claim that the stabilizer of the standard lattice $R^n \subset K^n$ is precisely the subgroup $\mathrm{GL}_n(R)$. Indeed, it is immediate that each element of $\mathrm{GL}_n(R)$ preserves R^n, and conversely, if $M \in \mathrm{GL}_n(K)$ preserves R^n then for all $1 \leq i \leq n$, $Me_1 \in R^n$, so $M \in M_n(R)$. The same holds for M^{-1}, so $M \in \mathrm{GL}_n(R)$.

Therefore:

Proposition 9.
a) We have an isomorphism of $\mathrm{GL}_n(K)$-sets $\mathrm{GL}_n(K)/\mathrm{GL}_n(R) \cong \mathcal{L}$.
b) For every $\Lambda \in \mathcal{L}$, the stabilizer G_Λ of Λ in $\mathrm{GL}_n(K)$ is of the form $g\,\mathrm{GL}_n(R)g^{-1}$ for some $g \in \mathrm{GL}_n(K)$.

Exercise 9.10: Prove Proposition 9.9.

Proposition 10. *Let G be a subgroup of $\mathrm{GL}_n(K)$ with the following property:*
(LF) There exists a lattice $\Lambda_1 \in \mathcal{L}$ such that the orbit $G.\Lambda_1$ is finite.
Then G is conjugate to a subgroup of $\mathrm{GL}_n(R)$.

Proof. By hypothesis, $G.\Lambda_1$ is a finite set, say $\{\Lambda_1, \ldots, \Lambda_m\}$. Put $\Lambda = \langle \Lambda_1, \ldots, \Lambda_m \rangle_R$. By Lemma 8, Λ is again a lattice. By construction, for any $g \in G$ and $x \in \Lambda$, $gx \in \Lambda$, i.e., $g\Lambda \subset \Lambda$. Applying this with g^{-1} as well gives $g\Lambda = \Lambda$, Thus G stabilizes Λ, so $G \subset G_\Lambda$, which is conjugate to $\mathrm{GL}_n(R)$. □

Certainly hypothesis (LF) is satisfied if G is finite, and we conclude:

Corollary 11. *Let R be a PID with fraction field K. Then any finite subgroup of $\mathrm{GL}_n(K)$ is conjugate to a subgroup of $\mathrm{GL}_n(R)$.*

Already the case $R = \mathbb{Z}$ is interesting and useful, as we shall see shortly.

Finally, we return to the case in which K is a non-Archimedean locally compact field and R is its valuation ring. In this case, the group $\mathrm{GL}_n(R)$ is compact and open in $\mathrm{GL}_n(K)$. By Proposition 9, the same holds for the stabilizer G_Λ of every lattice in K^n.

Theorem 12. *Let H be a compact subgroup of $\mathrm{GL}_n(K)$. Then there exists $\Lambda \in \mathcal{L}$ such that $g\Lambda = \Lambda$ for all $g \in H$. Equivalently, $H \subset G_\Lambda$.*

Proof. By Proposition 10 it will suffice to show that a compact subgroup has property (LF). Begin with any lattice Λ_1. Then $H_{\Lambda_1} := H \cap G_{\Lambda_1}$ is the subgroup of H consisting of elements preserving Λ_1. Since G_{Λ_1} is open in $\mathrm{GL}_n(K)$, H_{Λ_1} is open in H. Since the cosets of H_{Λ_1} in H give an open covering of the compact group H, we must have $[H : H_{\Lambda_1}] < \infty$. It follows that the orbit $H.\Lambda_1$ is finite, qed. □

2. Cassels Embedding Theorem

2.1. Statement of the Theorem.

Theorem 13. *(Cassels* [Cas]*) Let K be a finitely generated field of characteristic 0, and let $x_1, \ldots, x_n \in K^\times$. Then there exist infinitely many prime numbers p such that there is a field embedding $\iota_p : K \hookrightarrow \mathbb{Q}_p$ such that for all $1 \leq i \leq n$, $|\iota_p(x_i)|_p = 1$.*

2.2. Three Lemmas.

Lemma 14. *Let R be an infinite integral domain, and let $f_1, \ldots, f_m \in R[t_1, \ldots, t_n]$ be nonzero polynomials. Then there exist $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ such that for all $1 \leq i \leq m$, $f_i(a_1, \ldots, a_n) \neq 0$.*

Proof. We go by induction on n. The case of $n = 1$ is trivial, since a nonzero univariate polynomial over a domain has only finitely many roots, so we may select any element a of R in the complement of a finite set. Assume the result holds for all polynomials in $n-1$ variables. Put $S = R[t_1]$ – an infinite integral domain – so that $R[t_1, \ldots, t_n] = S[t_2, \ldots, t_n]$. By induction, there exist $a_2(t_1), \ldots, a_m(t_1) \in S$ such that for all i, $f_i(t_1, a_2(t_1), \ldots, a_n(t_1)) \neq 0$. Now we apply the $n = 1$ case. □

Lemma 15. *Let $f(t) \in \mathbb{Z}[t]$ be a nonconstant polynomial. Then there exist infinitely many prime numbers p such that the reduction mod p of f has a $\mathbb{Z}/p\mathbb{Z}$-rational root.*

Proof. We give two proofs. First, we may plainly assume that f is irreducible over $\mathbb{Q}[t]$. Put $K = \mathbb{Q}[t]/(f)$ and let L be its normal closure. Then, by the Cebotarev Density Theorem, the set of prime numbers p which split completely in L has positive density, and for such primes the mod p reduction of f splits completely.

However, it is possible to give a completely elementary argument. Namely, write $f(t) = a_n t^n + \ldots + a_1 t + a_0$. Clearly we may assume that $a_0 \neq 0$, otherwise 0 is a root of every mod p reduction. Suppose for the sake of contradiction that there exists a finite set S of prime numbers such that if p is a prime not lying in S, then the mod p reduction of f has no $\mathbb{F}_p$-rational root. Let $c \in \mathbb{Z}$ be an integer divisible by all primes in S. Then

$$f(ca_0) = a_0 r(c) = a_0(a_n a_0^{n-1} c^n + a_{n-1} a_0^{n-2} c^{n-1} + \ldots + 1).$$

Since f is nonconstant, we may choose c such that $r(c) \neq \pm 1$; do so, and let ℓ be prime dividing $r(c)$. Since $r(c) \equiv 1 \pmod{p}$ for all $p \in S$, ℓ is a prime outside of S such that f has a rational root modulo ℓ. □

Lemma 16. *For any prime p, the transcendence degree of $\mathbb{Q}_p$ over $\mathbb{Q}$ is uncountable.*

Proof. Indeed, since $\mathbb{Q}_p$ has continuum cardinality, this is clear. (But since we are following Cassels' proof so closely, we did not want to meddle with his auspicious number of preliminary lemmas.) □

2.3. **The proof of the Cassels Embedding Theorem.**

Let K be a finitely generated field of characteristic zero, and let S be a finite set of nonzero elements of K. At the cost of replacing S with a larger finite set, we may assume that C is closed under inversion, i.e., $s \in S \implies s^{-1} \in S$, and then it suffices to find, for infinitely many primes p, embeddings $\iota_p : K \hookrightarrow \mathbb{Q}_p$ such that for all $s \in S$, $\iota_p(s) \in \mathbb{Z}_p$.

The case in which K is algebraic over $\mathbb{Q}$ is easy: then $K \cong \mathbb{Q}[t]/(f(t))$ is a number field, and applying Lemma 15 to $f(t)$, we get infinitely many primes p such that there exists a degree one prime ideal $\mathfrak{p}$ of K lying over p, and thus $K \hookrightarrow K_{\mathfrak{p}} \cong \mathbb{Q}_p$. Moreover, any element of K is a $\mathfrak{p}$-adic integer except at finitely many prime ideals of $\mathbb{Z}_K$, so we need only exclude this finite set of primes.

Therefore we may assume that the transcendence degree of K over $\mathbb{Q}$ is positive, say n, and let $x_1, \ldots, x_n$ be a transcendence basis for $K/\mathbb{Q}$, i.e., such that $K/\mathbb{Q}(x_1, \ldots, x_n)$ is finite. Since we are in characteristic 0, the primitive element theorem applies, and there exists $y \in K$ such that $K = \mathbb{Q}(x_1, \ldots, x_n, y)$. Therefore each element c of C may be written in the form

$$c = \frac{U_c(y, x_1, \ldots, x_n)}{V_c(y, x_1, \ldots, x_n)}$$

for nonzero polynomials $U_c, V_c \in \mathbb{Z}[t, x_1, \ldots, x_n]$. Moreover, a simple denominator-clearing argument shows there is a polynomial

$$H(t) = H(t, x_1, \ldots, x_n) \in \mathbb{Z}[t, x_1, \ldots, x_n]$$

which is irreducible over $\mathbb{Q}(x_1, \ldots, x_n)$ and such that $g(y) = 0$. We write

$$H(t) = h_s(x_1, \ldots, x_n)t^s + \ldots + h_1(x_1, \ldots, x_n)t + h_0(x_1, \ldots, x_n),\ h_i \in \mathbb{Z}[x_1, \ldots, x_n],$$

with $h_s \neq 0$. Let $\Delta = \Delta(x_1, \ldots, x_n)$ be the discriminant of $H(t)$, which is a nonzero element of $\mathbb{Z}[x_1, \ldots, x_n]$.

Now we begin! By Lemma 14, we may choose integers $a_1, \ldots, a_n$ such that

$$\Delta(a_1, \ldots, a_n) \neq 0$$

$$h_s(a_1, \ldots, a_n) \neq 0$$

and

$$\forall c \in C,\ V_c(a_1, \ldots, a_n) \neq 0.$$

Apply Lemma 15 to the polynomial $H(t, a_1, \ldots, a_n) \in \mathbb{Z}[t]$: there exist infinitely many primes p and integers b_p such that

$$H(b_p, a_1, \ldots, a_n) \equiv 0 \pmod{p}. \tag{1}$$

By excluding finitely many primes, we may also assume that none of $\Delta(a_1, \ldots, a_n)$ and $V_c(a_1, \ldots, a_n)$ are congruent to 0 mod p. For each such prime number p, we will construct the desired embedding ι_p.

Now by Lemma 16, let $\theta_1, \ldots, \theta_n$ be elements of $\mathbb{Q}_p$ which are algebraically independent over $\mathbb{Q}$. By replacing each θ_i by $p^m\theta_i$ if necessary (this certainly does not disturb the algebraic independence), we may assume that $0 < |\theta_i|_p < 1$ for all i. For all i, put

$$\xi_i = \theta_i + a_i.$$

Thus the ξ_i's are algebraically independent over $\mathbb{Q}$ such that for all i,

$$|\xi_i - a_i|_p < 1. \tag{2}$$

By (1) and (2) we have

$$|H(b_p, \xi_1, \ldots, \xi_n)|_p < 1.$$

Since the discriminant of H is a p-adic unit, it has distinct roots modulo p, and Hensel's Lemma applies to show that there exists $\eta \in \mathbb{Z}_p$ such that

$$H(\eta, \xi_1, \ldots, \xi_n) = 0.$$

It follows that for all $c \in C$,

$$U_c(\eta, \xi_1, \ldots, \xi_n),\ V_c(\eta, \xi_1, \ldots, \xi_n) \in \mathbb{Z}_p$$

and

$$|V_c(\eta, \xi_1, \ldots, \xi_n)|_p = 1.$$

So we may define an embedding $\iota_p : K \hookrightarrow \mathbb{Q}_p$ by:

$$\forall i,\ \iota_p : x_i \mapsto \xi_i,$$

and

$$\iota_p : y \mapsto \eta.$$

Moreover, for all $c \in C$,

$$|\iota_p(c)|_p = |U_c(\eta, \xi_1, \ldots, \xi_n)/V_c(\eta, \xi_1, \ldots, \xi_n))|_p = |U_c(\eta, \xi_1, \ldots, \xi_n)|_p \leq 1,$$

QED.

Exercise 9.11: Try to to prove the following positive characteristic analogue of Cassels' Theorem.

Theorem? 17. *Let K be a finitely generated field of characteristic $p > 0$, with constant subfield $\mathbb{F}_q$. (I.e., let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in K.) Let C be a finite set of nonzero elements of K. Then there exists a field embedding $\iota : K \hookrightarrow \mathbb{F}_q((t))$ such that for all $c \in C$, $\iota(c) \in \mathbb{F}_q[[t]]^\times$.*

3. Applications to subgroups of matrix groups

A group G is said to be **torsionfree** if the only element of finite order is the identity. A group is **virtually torsionfree** if it has a finite index torsionfree subgroup. Some elementary properties are established in the following exercise.

Exercise 9.12:
a) Show that every subgroup of a torsion free group is torsion free.
b) Show that every finite group is virtually torsion free.

c) Give an example of a group which is not virtually torsion free.
d) Let G be a finitely generated virtually torsionfree group. Show that G has a finite index **normal** subgroup which is torsion free. (Hint: a finitely generated groups has only finitely many subgroups of any given index.)

One reason to be interested to be interested in whether a group is virtually torsion-free is the following simple result.

Proposition 18. *Suppose that a group G has a torsionfree subgroup of finite index n. Then the order of any finite subgroup of G divides n.*

Exercise 9.13: Prove Proposition 18.

Exercise 9.14: Suppose that a group G has a torsionfree subgroup of index dividing $n < \infty$. Show that the same holds for each subgroup of G.

An important class of examples of virtually torsionfree groups are the groups $\mathrm{GL}_n(\mathbb{Z}_p)$. In view of Proposition 18, it is useful to have an explicit upper bound on the index of a torsionfree subgroup, and the following result achieves this.

Theorem 19. *Let p be a prime number.*
a) For $p > 2$, $\mathrm{GL}_n(\mathbb{Z}_p)$ has a torsionfree normal subgroup of index $\prod_{i=1}^n (p^n - p^{i-1})$.
b) $\mathrm{GL}_n(\mathbb{Z}_2)$ has a torsionfree normal subgroup of index $2^{n^2} \prod_{i=1}^n (2^n - 2^{i-1})$.

Proof. a) Suppose p is odd, and consider the subgroup U^1 of $\mathrm{GL}_n(\mathbb{Z}_p)$ consisting of matrices of the form $1 + pM_n(\mathbb{Z}_p)$; equivalently, the kernel of the reduction map $r : \mathrm{GL}_n(\mathbb{Z}_p) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.[3] Evidently U^1 is normal and of finite index. We claim that U^1 has no elements of finite order. Indeed, assuming to the contrary it would have some element of prime order ℓ ($\ell = p$ is allowed). But for $B \in M_n(\mathbb{Z}_p) \setminus 0$, we have

$$(1 + pB)^\ell = 1 + \ell pB + \ldots + p^\ell B^\ell.$$

But now we apply the principle of domination: the entry of ℓpB of minimal p-adic norm has strictly smaller p-adic norm then the entries of all the other nonzero terms $\binom{\ell}{i} p^i B^i$: note that when $\ell = p$ we are using that $p \mid \binom{\ell}{2}$, which is valid since $p > 2$. Therefore the sum $\ell pB + \ldots + p^\ell B^\ell$ has at least one entry of nonzero p-adic norm, so is not the zero matrix, contradicting the statement that $1 + pB$ has order ℓ.
b) When $p = 2$, the above argument does not go through. To remedy it, we need to use U^2 instead, the kernel of the reduction map $r : \mathrm{GL}_n(\mathbb{Z}_2) \to \mathrm{GL}_n(\mathbb{Z}/2^2\mathbb{Z})$. We leave it to the reader to check that U^2 has no nontrivial elements of finite order by modifying the above argument. Moreover, we have $[\mathrm{GL}_n(\mathbb{Z}_2) : U^2] = \#\,\mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z})$. To compute the latter quantity, we use the short exact sequence

$$1 \to 1 + (2)M_n(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z}) \to 1,$$

noting that $\#(1 + (2)M_n(\mathbb{Z}/4\mathbb{Z}) = 2^{n^2}$. □

Theorem 20. *(Selberg* [Sel]*) Let K be a field of characteristic zero, $n \in \mathbb{Z}^+$, and let G be a finitely generated subgroup of $\mathrm{GL}_n(K)$. Then G is virtually torsionfree.*

[3]Note that when $n = 1$, this is indeed the first higher unit group considered in Chapter 5.

Proof. Let S be a finite, symmetric set of generators of G, i.e., if $x \in S$, then $x^{-1} \in S$. The subfield K' obtained by adjoining to $\mathbb{Q}$ all the matrix entries of the elements of S is finitely generated, and since S is a generating set for G, we have $G \subset \mathrm{GL}_n(K')$. By Theorem 13, there exists a prime number p and an embedding $\iota : K' \to \mathbb{Q}_p$ such that every entry of each matrix in S gets mapped into $\mathbb{Z}_p$. Thus ι induces an embedding $\iota : M_n(K') \hookrightarrow M_n(\mathbb{Q}_p)$ such that$\iota(G) \subset M_n(\mathbb{Z}_p)$, and since $\iota(G)$ is a group we must have $\iota(G) \subset \mathrm{GL}_n(\mathbb{Z}_p)$. By Theorem 19, $\mathrm{GL}_n(\mathbb{Z}_p)$ is virtually torsionfree, hence by Exercise 9.14 so is $G \cong \iota(G)$. □

Let $n \in \mathbb{Z}^+$, and let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$. By Corollary 11, G is conjugate to a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ hence *a fortiori* to a finite subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ for all primes p. Combining Proposition 18, Exercise 9.14 and Theorem 19, we get:

$$\#G \mid \gcd((2^{n^2}\prod_{i=1}^{n}(2^n - 2^{i-1}), \{\prod_{i=1}^{n}(p^n - p^{i-1})\}_{p>2}).$$

In practice, this gcd is attained by looking only at very small odd primes. For example, when $n = 2$, it is easy to see that the gcd is equal to 48, which is also $\#\,\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$: all the other orders are proper multiplies of 48, eg. $\#\,\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) = 96$, $\#\,\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) = 480$.

Is this upper bound sharp, i.e., is 48 indeed the least common multiple of all orders of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ (or equivalently, $\mathrm{GL}_2(\mathbb{Z})$)? Close, but not quite. There are well-known matrices of order 4 and 6 in $\mathrm{SL}_2(\mathbb{Z})$, namely

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

Moreover, put

$$S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

so that S has determinant -1 and order 2. Then we have

$$SAS^{-1} = A^{-1}, SBS^{-1} = B^{-1},$$

so that as subgroups of $\mathrm{GL}_2(\mathbb{Z})$ we have

$$\langle A, S\rangle \cong D_4, \langle B, S\rangle \cong D_6,$$

of orders 8 and 12 respectively. Thus the lcm of all orders of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ is a multiple of 24.

To show that 24 is sharp, we will use information coming from the Archimedean place of $\mathbb{Q}$! Namely, we can also embed $\mathrm{GL}_2(\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{R})$, so that by Theorem 3 every finite (hence compact) subgroup of $\mathrm{GL}_2(\mathbb{Q})$ is conjugate to a subgroup of the standard orthogonal group $O(2)$. But $O(2)$ has a very agreeable structure: the determinant map induces a short exact sequence

$$1 \to SO(2) \to O(2) \stackrel{\det}{\to} \{\pm 1\} \to 1,$$

where the special orthogonal group $SO(2)$ of all orthogonal matrices of determinant one is just the circle group:

$$SO(2) = S^1 = \{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mid \theta \in \mathbb{R}\}.$$

At first sight this seems unhelpful, because of course $SO(2)$ contains finite subgroups of all orders, namely the nth roots of unity. Conversely, it is easy to see that any finite subgroup of $SO(2)$ is generated by any element of minimal argument θ, so that the cyclic groups C_n generated by the nth roots of unity are the only finite subgroups of $SO(2)$. However, very few of the groups C_n have rational entries: indeed, C_n contains the matrix

$$\left[\begin{array}{cc} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{array} \right]$$

of trace $2\cos(\frac{2\pi}{n}) = \zeta_n + \zeta_n^{-1}$, which generates the real subfield of the nth cyclotomic field so for all $n > 2$ has degree $\frac{\varphi(n)}{2}$. Thus this is rational iff $\varphi(n) = 2$ iff $n = 3, 4, 6$. Thus, up to conjugacy, the only matrices in $\mathrm{GL}_2(\mathbb{R})$ with finite order and rational trace are ± 1, A and B. This shows that the least common multiple of all orders of finite subgroups of $\mathrm{SL}_2(\mathbb{Q})$ is 12 and thus that of $\mathrm{SL}_2(\mathbb{Q})$ is 24.

If we put $M(n)$ to be the least common multiple of all orders of finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$, the above work gives an explicit upper bound on $M(n)$ for a given n. In fact, the exact value of $M(n)$ for all n was computed by Minkowski.

Theorem 21. *(Minkowksi, 1887) For all $n \in \mathbb{Z}^+$,*

$$M(n) = \prod_{\ell} \ell^{\lfloor \frac{n}{\ell-1} \rfloor + \lfloor \frac{n}{\ell(\ell-1)} \rfloor + \lfloor \frac{n}{\ell^2(\ell-1)} \rfloor + \cdots},$$

where the product extends over all prime numbers ℓ.

Rather remarkably, the efficacy of the argument of looking at the completion at an Archimedean place and restricting to matrices with rational trace also holds for all $n \geq 2$, as the following theorem shows:

Theorem 22. *(Schur, 1905) Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a finite subgroup of matrices such that $\mathrm{tr}(g) \in \mathbb{Q}$ for all $g \in G$. Then $\#G \mid M(n)$.*

For modern (and novel) proofs of Theorems 20 and 21, we heartily recommend the recent paper of Guralnick and Lorenz [GL].

For fixed n, it is also interesting to ask for the **maximum** order of a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$, say $m(n)$. Evidently $m(n) \mid M(n)$. E.g. we found that $m(2) = 12$. This is achieved by the following remarkable theorem of Walter Feit.

Theorem 23. *(Feit, 1998) Let n be a positive integer, $n \neq 2, 4, 6, 7, 8, 9, 10$.*
a) Then $m(n) = 2^n n!$.
b) Let $G \subset \mathrm{GL}_n(\mathbb{Q})$ be a subgroup of order $2^n n!$. Then G is conjugate to the subgroup of signed permutation matrices, i.e., the subgroup generated by all permutation matrices and all diagonal matrices with diagonal entries ± 1.

Exercise 9.15: Show that for all $n \geq 1$, the group of signed permutation matrices is $O_n(\mathbb{Z}) := O_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{Z})$.

Feit's theorem relies upon a 1984 manuscript of B. Weisfeiler [Wei]. Weisfeiler's manusript is remarkable in that it uses the classification of finite simple groups,

one of the first to do so in an essential way to derive a significant theorem. However, there is an even more remarkable, and sad, story concerning Weisfeiler himself.

Boris Weisfeiler has been "missing" in Chile since January 4, 1985. In March of 1985 the local Chilean court ruled that Weisfeiler had died by accidental drowning. However, it has long been suspected that Weisfeiler was a *desaparecido*, i.e., that his death was one of the secret murders committed by the Pinochet regime. As of 2010, the matter is still not entirely settled, but has recently been heard by the *Comisión Asesora para la calificación de Detenidos Desaparecidos, Ejecutados Polticos y Vctimas de Prisin Poltica y Tortura*. A ruling is expected by early 2011 and it is expected that Weisfeiler's disappearance will be officially recognized as a human rights violation. For more information on Weisfeiler's life and his mathematics, see

http://boris.weisfeiler.com/

References

[Cas] J.W.S. Cassels, *An embedding theorem for fields*. Bull. Austral. Math. Soc. 14 (1976), 193-198.

[Fei] W. Feit, *Orders of finite linear groups*. Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996), 9–11, Univ. West Indies, Kingston, 199?.

[GL] R.M. Guralnick and M. Lorenz, *Orders of finite groups of matrices*. (English summary) Groups, rings and algebras, 141–161, Contemp. Math., 420, Amer. Math. Soc., Providence, RI, 2006.

[Sel] A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*. 1960 Contributions to function theory (internat. Colloq. Function Theory, Bombay, 1960) pp. 147–164 Tata Institute of Fundamental Research, Bombay

[Ser] J.-P. Serre, *Lie algebras and Lie groups*. Lectures given at Harvard University, 1964 W. A. Benjamin, Inc., New York-Amsterdam 1965 vi+247 pp.

[Wei] B. Weisfeiler, *On the size and structure of finite linear groups*, unpublished 1984 manuscript, available at `http://boris.weisfeiler.com`.