Arithmetic subgroups of $\mathrm{SL}(n,\mathbb{R})$

Dave Witte Morris
University of Lethbridge, Alberta, Canada
`http://people.uleth.ca/~dave.morris`
`Dave.Morris@uleth.ca`

Abstract

$\mathrm{SL}(2,\mathbb{Z})$ is an "arithmetic" subgroup of $\mathrm{SL}(2,\mathbb{R})$. The other arithmetic subgroups are not as obvious, but they can be constructed by using quaternion algebras. Replacing the quaternion algebras with larger division algebras yields many arithmetic subgroups of $\mathrm{SL}(n,\mathbb{R})$, with $n > 2$. In fact, a calculation of group cohomology shows that the only other way to construct arithmetic subgroups of $\mathrm{SL}(n,\mathbb{R})$ is by using unitary groups.

Definition of arithmetic subgroup

Interested in *integer points* of a group $G \subseteq \mathrm{SL}(N,\mathbb{R})$:
elements of G whose matrix entries are int's.
$G_{\mathbb{Z}} = G \cap \mathrm{SL}(N,\mathbb{Z})$.

Definition

Spse $G \subseteq \mathrm{SL}(N,\mathbb{R})$ (and a technical cond'n is satisfied).
Then $G_{\mathbb{Z}}$ is an ***arithmetic*** subgroup of G.

Example. $\mathrm{SL}(n,\mathbb{Z})$ is an arith subgroup of $\mathrm{SL}(n,\mathbb{R})$.

Remark. We usually ignore finite groups.
$G \doteq H$ means some finite-index subgroup of G
is equal to some finite-index subgroup of H.
In other words, G and H are commensurable.

The technical condition

Need to assume G is ***defined over*** $\mathbb{Q}$:
G is def'd by polynomial eq'ns with rat'l coeffs.

More precisely, there are polynomials
$f_1(x_{1,1},\ldots,x_{N,N}),\ \ldots,\ f_m(x_{1,1},\ldots,x_{N,N})$
with coefficients in $\mathbb{Q}$,

$$\text{s.t.}\quad G \doteq \left\{ \begin{matrix} (g_{i,j}) \\ \in \mathrm{SL}(N,\mathbb{R}) \end{matrix} \;\middle|\; \begin{matrix} f_k(g_{1,1},\ldots,g_{N,N}) = 0, \\ \text{for all } k \end{matrix} \right\}.$$

Equivalent if G is connected and $[G,G] = G$:
$G_{\mathbb{Q}}$ is dense in G, where $G_{\mathbb{Q}} = G \cap \mathrm{SL}(N,\mathbb{Q})$.

$\Rightarrow G_{\mathbb{Z}}$ is a lattice in G [Borel & Harish-Chandra, 1962]

Definition. Subgroup $G_{\mathbb{Q}}$ is called a "$\mathbb{Q}$-form" of G.

Example

$\mathrm{SO}(1,n)_{\mathbb{Z}}$ is a arithmetic subgroup of $\mathrm{SO}(1,n)$.

Proof.

$\mathrm{SO}(1,n) = \{\, g \in \mathrm{SL}(n+1,\mathbb{R}) \mid g\, I_{1,n}\, g^T = I_{1,n} \,\}$,

$$\text{where}\quad I_{1,n} = \begin{bmatrix} 1 & & & & \\ & -1 & & & \\ & & -1 & & \\ & & & \ddots & \\ & & & & -1 \end{bmatrix}.$$

Write $g\, I_{1,n}\, g^T = I_{1,n}$ in terms of mat entries $(g_{i,j})$.
Obtain $(n+1)^2$ polynomial eqns, with coeffs in $\mathbb{Q}$.
Therefore $\mathrm{SO}(1,n)$ is defined over $\mathbb{Q}$,
so $\mathrm{SO}(1,n)_{\mathbb{Z}}$ is an arithmetic subgroup. □

A Lie group G usually has *many* arithmetic subgrps, because there are many embeddings $G \hookrightarrow \mathrm{SL}(N,\mathbb{R})$, which yield very different arithmetic subgroups.

Finding all the arithmetic subgroups of G
(up to commensurability)
is the same as finding all the $\mathbb{Q}$-forms of G
(up to isomorphism).

The obvious $\mathbb{Q}$-form of $\mathrm{SL}(n,\mathbb{R})$ is $\mathrm{SL}(n,\mathbb{Q})$,
corresponding to the arith subgrp $\mathrm{SL}(n,\mathbb{Z})$.

These lectures:
how to find all of the others

Example

An arithmetic subgroup of $\mathrm{SL}(n,\mathbb{C})$.

We need to embed $\mathrm{SL}(n,\mathbb{C})$ in some $\mathrm{SL}(N,\mathbb{R})$:
$\mathbb{C} \cong \mathbb{R}^2$, so $\mathbb{C}^n \cong \mathbb{R}^{2n}$, so $\mathrm{SL}(n,\mathbb{C}) \hookrightarrow \mathrm{SL}(2n,\mathbb{R})$.
Then $\mathrm{SL}(n,\mathbb{C})_{\mathbb{Z}} = \mathrm{SL}(n,\mathbb{C}) \cap \mathrm{SL}(2n,\mathbb{Z})$.

This depends on the identification $\varphi \colon \mathbb{R}^2 \xrightarrow{\cong} \mathbb{C}$:
For $\varphi(a,b) = a + bi$, we have $\varphi(\mathbb{Z}^2) = \mathbb{Z}[i]$,
so $\mathbb{Z}^{2n}$ is identified with $(\mathbb{Z}[i])^n \subset \mathbb{C}^n$.
Since $\mathrm{SL}(2n,\mathbb{Z}) = \{\, g \in \mathrm{SL}(2n,\mathbb{R}) \mid g\mathbb{Z}^{2n} = \mathbb{Z}^{2n} \,\}$,

$$\begin{aligned} \mathrm{SL}(n,\mathbb{C})_{\mathbb{Z}} &= \mathrm{SL}(n,\mathbb{C}) \cap \mathrm{SL}(2n,\mathbb{Z}) \\ &= \{\, g \in \mathrm{SL}(n,\mathbb{C}) \mid g(\mathbb{Z}[i])^n = (\mathbb{Z}[i])^n \,\} \\ &= \mathrm{SL}(n,\mathbb{Z}[i]). \end{aligned}$$

Exercise. *Another arithmetic subgroup of* $\mathrm{SL}(2,\mathbb{R})$.

The quaternions $\mathbb{H} = \mathbb{H}^{-1,-1}$ can be embedded in $\mathrm{Mat}_{2\times 2}(\mathbb{C})$:

$$1 \mapsto I,\ i \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ j \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ k \mapsto ij = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Choose square-free $a, b \in \mathbb{Z}^+$.
$\mathbb{H}_{\mathbb{Z}}^{a,b} = \mathbb{Z}I + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k \subset \mathrm{Mat}_{2\times 2}(\mathbb{R})$,

$$\text{where}\quad i = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix},\ j = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix},\ k = ij.$$

$\mathrm{SL}(2,\mathbb{R})$ acts on $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ by multiplication gA.
For $\varphi \colon \mathbb{R}^4 \cong \mathrm{Mat}_{2\times 2}(\mathbb{R})$ with $\varphi(\mathbb{Z}^4) = \mathbb{H}_{\mathbb{Z}}^{a,b}$,

$$\begin{aligned} \mathrm{SL}(2,\mathbb{R})_{\mathbb{Z}} &= \{\, g \in \mathrm{SL}(2,\mathbb{R}) \mid g\mathbb{H}_{\mathbb{Z}}^{a,b} = \mathbb{H}_{\mathbb{Z}}^{a,b} \,\} \\ &= (\mathbb{H}_{\mathbb{Z}}^{a,b})^{\times} \doteq \mathrm{SL}(1,\mathbb{H}_{\mathbb{Z}}^{a,b}). \end{aligned}$$

$\mathrm{SL}(1,\mathbb{H}_{\mathbb{Z}}^{a,b})$ is an arithmetic subgroup of $\mathrm{SL}(2,\mathbb{R})$

In general, $\mathrm{SL}(n,\mathbb{H}_{\mathbb{Z}}^{a,b})$ is arith subgrp of $\mathrm{SL}(2n,\mathbb{R})$.

Remark

- If $H_{\mathbb{Q}}^{a,b}$ is a **division algebra** $(\forall x \neq 0, \exists y, xy = 1)$,
  (b not norm in $\mathbb{Q}[\sqrt{a}]$; $b \neq \square - a\square$)
  then $\mathrm{SL}(n,\mathbb{H}_{\mathbb{Z}}^{a,b})$ not commens'ble to $\mathrm{SL}(2n,\mathbb{Z})$.
- D any (finite-dimensional) division algebra over $\mathbb{Q}$,
  and $D \otimes \mathbb{R} \cong \mathrm{Mat}_{d\times d}(\mathbb{R})$,
  $\Rightarrow \mathrm{SL}(n,D_{\mathbb{Z}})$ is an arith subgroup of $\mathrm{SL}(dn,\mathbb{R})$.

Summary: Some arithmetic subgroups of $\mathrm{SL}(n,\mathbb{R})$ can be constructed from **division algebras**.

All the others come from **unitary groups**.

How to find the $\mathbb{Q}$-forms of $\mathrm{SL}(n,\mathbb{R})$

Let $G = \mathrm{SL}(n,\mathbb{R})$. Suppose $\rho \colon G \hookrightarrow \mathrm{SL}(N,\mathbb{R})$,
such that $\rho(G)$ is defined over $\mathbb{Q}$.

Find $\rho(G)_{\mathbb{Q}}$ by using Galois theory:
$\mathbb{Q} = \{\, z \in \mathbb{C} \mid \sigma(z) = z,\ \forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \,\}$.

$$\mathrm{SL}(N,\mathbb{Q}) = \left\{ h \in \mathrm{SL}(N,\mathbb{C}) \;\middle|\; \begin{matrix} \sigma(h) = h, \\ \forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \end{matrix} \right\}.$$

$$\begin{aligned} \rho(G)_{\mathbb{Q}} &= \rho(G) \cap \mathrm{SL}(N,\mathbb{Q}) \\ &= \{\, \rho(g) \mid \sigma(\rho(g)) = \rho(g),\ \forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \\ &\cong \{\, g \in G_{\mathbb{C}} \mid \tilde{\sigma}(g) = g,\ \forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \\ &\qquad \text{where } \tilde{\sigma} = \rho^{-1}\sigma\rho \colon G_{\mathbb{C}} \to G_{\mathbb{C}}. \end{aligned}$$

Every $\mathbb{Q}$-form of G is the fixed points of
an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on $G_{\mathbb{C}}$.

Lecture 2

Recall

What are the **arithmetic subgrps** of $G = \mathrm{SL}(n,\mathbb{R})$?
Embed $G \hookrightarrow \mathrm{SL}(N,\mathbb{R})$. Find $G_{\mathbb{Z}} = G \cap \mathrm{SL}(N,\mathbb{Z})$.

Same problem: Find $G_{\mathbb{Q}}$. ("$\mathbb{Q}$-form")

Every $\mathbb{Q}$-form of G is the fixed points of
an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on $G_{\mathbb{C}}$.

$\mathrm{SL}(n,\mathbb{Q}) = \{\, g \in G_{\mathbb{C}} \mid \forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}),\ \sigma(g) = g \,\}$.

$G_{\mathbb{Q}} = \{\, g \in G_{\mathbb{C}} \mid \forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}),\ \tilde{\sigma}(g) = g \,\}$.

Every $\mathbb{Q}$-form of G is the fixed points of
an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on $G_{\mathbb{C}}$.

Let $\alpha_\sigma = \tilde{\sigma}\,\sigma^{-1} \colon G_{\mathbb{C}} \to G_{\mathbb{C}}$. (continuous automorphism)
So $\alpha_\sigma \in \mathrm{Aut}(G_{\mathbb{C}})$. Thus, $\alpha \colon \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \to \mathrm{Aut}(G_{\mathbb{C}})$.

Group cohomology

Function $c \colon \Gamma^k \to A$ is k-cochain $\in C^k(\Gamma;A)$.
Coboundary $\delta_k \colon C^k(\Gamma;A) \to C^{k+1}(\Gamma;A)$

- $\delta_0 a(g) = {}^{g}a - a$
- 1-cocycle $\Leftrightarrow \delta_1 c = 0 \Leftrightarrow c(gh) = c(g) + {}^{g}c(h)$

Note. $\alpha_\sigma = \rho^{-1}\sigma\rho\,\sigma^{-1} = \rho^{-1}\,{}^{\sigma}\rho$ looks like a cobdry
so it is a **1-cocycle**.
So it defines an element of $H^1\big(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(G_{\mathbb{C}})\big)$.

$G_{\mathbb{Q}} \mapsto [\alpha_\sigma]$ provides a 1-1 correspondence between
$H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(G_{\mathbb{C}}))$ and the set of $\mathbb{Q}$-forms.

Finding the arithmetic subgrps of G amounts to calculating the "Galois cohomology set"
$$H^1\big(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(G_{\mathbb{C}})\big).$$

This is a special case of a fairly general principle:

If X is an algebraic object defined over $\mathbb{Q}$, then

$$\begin{aligned} &H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(X_{\mathbb{C}})) \\ &\quad \overset{1\text{-}1}{\longleftrightarrow} \{\, \mathbb{Q}\text{-forms of } X \,\} \\ &\quad = \left\{ \begin{array}{c} \mathbb{Q}\text{-isomorphism classes of} \\ \mathbb{Q}\text{-defined objects whose} \\ \mathbb{C}\text{-points are isomorphic to } X_{\mathbb{C}} \end{array} \right\}. \end{aligned}$$

Example

Suppose V_1 and V_2 are two vector spaces over $\mathbb{Q}$,
and they are isomorphic over $\mathbb{C}$.
(I.e., $V_1 \otimes \mathbb{C} \cong V_2 \otimes \mathbb{C}$.)
Then $\dim V_1 = \dim V_2$,
so V_1 and V_2 are isomorphic over $\mathbb{Q}$.
Thus, the $\mathbb{Q}$-form of any vector space is unique,
so $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(V_{\mathbb{C}})) = 0$,
for any vector space V over $\mathbb{Q}$.
In other words, $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{GL}(n,\mathbb{C})) = 0$.

Similarly: $H^1\big(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{SL}(n,\mathbb{C})\big) = 0$

Warning. $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{PSL}(n,\mathbb{C})) \neq 0$.

$\mathbb{Q}$-forms from Galois cohomology

We will find all the $\mathbb{Q}$-forms of $\mathrm{SL}(n,\mathbb{R})$,
by calculating $H^1\Big(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}\big(\mathrm{SL}(n,\mathbb{C})\big)\Big)$.

Fact. Only <u>outer</u> automorphism of $G_{\mathbb{C}} = \mathrm{SL}(n,\mathbb{C})$ is
transpose-inverse $(\omega(g) = (g^{\mathsf{T}})^{-1})$.
So $\mathrm{Aut}(G_{\mathbb{C}}) = \mathrm{PSL}(n,\mathbb{C}) \rtimes \langle \omega \rangle$.

$\mathbb{Q}$-form $G_{\mathbb{Q}}$ $\rightsquigarrow$ $\alpha \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(G_{\mathbb{C}}))$

We consider two cases:

1. $\alpha \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{PSL}(n,\mathbb{C}))$.
2. Image of $\alpha \notin \mathrm{PSL}(n,\mathbb{C})$.

Case 1. Assume $\alpha \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{PSL}(n,\mathbb{C}))$.

Fact. Every $\mathbb{C}$-linear aut of algebra $\mathrm{Mat}_{n\times n}(\mathbb{C})$ is inner
— it is conjugation by a matrix in $\mathrm{GL}(n,\mathbb{C})$.
Scalars act trivially: $\mathrm{Aut}(\mathrm{Mat}_{n\times n}(\mathbb{C})) = \mathrm{PSL}(n,\mathbb{C})$.

$$\begin{aligned} &H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{PSL}(n,\mathbb{C})) \\ &\quad = H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{Aut}(\mathrm{Mat}_{n\times n}(\mathbb{C}))) \\ &\quad = \{\, \mathbb{Q}\text{-forms of } \mathrm{Mat}_{n\times n}(\mathbb{C}) \,\} \\ &\quad = \left\{ \begin{array}{c} \text{algebras } A \text{ over } \mathbb{Q}, \\ \text{such that } A \otimes \mathbb{C} \cong \mathrm{Mat}_{n\times n}(\mathbb{C}) \end{array} \right\}. \end{aligned}$$

A must be simple, so, by Wedderburn's Theorem,
$A \cong \mathrm{Mat}_k(D)$, where D is a division alg over $\mathbb{Q}$.
(and the center of D must be $\mathbb{Q}$)
The corresponding $\mathbb{Q}$-form $G_{\mathbb{Q}}$ is $\mathrm{SL}(k,D)$.

Case 1. Assume $\alpha \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \mathrm{PSL}(n,\mathbb{C}))$.

Case 2. Assume image of $\alpha \notin \mathrm{PSL}(n,\mathbb{C})$.

α induces <u>nontrivial</u>
$\alpha\overline{\alpha} \colon \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \to \mathrm{Aut}\ \mathrm{Out}(G_{\mathbb{C}}) \cong \mathbb{Z}_2$.
Action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on $\mathbb{Z}_2$ is trivial, so $\overline{\alpha}$ is a homo.

Kernel of $\overline{\alpha}$ is a subgroup of index 2 in $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$,
so fixed field is a quadratic extension $\mathbb{Q}[\sqrt{r}\,]$ of $\mathbb{Q}$.

Consider any $g \in G_{\mathbb{Q}} = \{\, g \in G_{\mathbb{C}} \mid g^{\tilde{\sigma}} = g, \forall \sigma \,\}$.
For simplicity, assume α is trivial on $\ker \overline{\alpha}$.
(If not, there is a division algebra involved.)
If $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}[\sqrt{r}\,]) = \ker \overline{\alpha}$, then α_σ is trivial.
This means $\sigma = \tilde{\sigma}$, so $g^{\sigma} = g^{\tilde{\sigma}} = g$.
So $g \in \mathrm{SL}(n, \mathbb{Q}[\sqrt{r}\,])$.

$G_{\mathbb{Q}} \subseteq \mathrm{SL}(n, \mathbb{Q}[\sqrt{r}\,])$

Let $\mathrm{Gal}(\mathbb{Q}[\sqrt{r}\,]/\mathbb{Q}) = \{1, \eta\}$, so $\eta \notin \ker \overline{\alpha}$.
Then $\alpha_\eta = (\text{conj by } A)\,\omega$ for some $A \in \mathrm{GL}(n,\mathbb{R})$.

We have $g = \tilde{\eta}(g) = \alpha_\eta\,\eta(g) = A\left(({}^{\eta}g)^{\mathsf{T}}\right)^{-1} A^{-1}$,
so $g\,A\,({}^{\eta}g)^{\mathsf{T}} = A$.

If $\eta = {}^{-}$ and $A = I$, this means $gg^* = I$,
so $g \in \mathrm{SU}(n)_{\mathbb{Q}[\sqrt{r}]}$. (unitary group)

If $A = I_{m,n} = \mathrm{diag}(1,1,\ldots,1,-1,-1,\ldots,-1)$,
so $\vec{z}A\vec{z}^{\,*} = |z_1|^2 + \cdots + |z_m|^2$
$- |z_{m+1}|^2 - \cdots - |z_{m+n}|^2$,
then $g \in \mathrm{SU}(m,n)_{\mathbb{Q}[\sqrt{r}]}$.

In general, we have $g \in \mathrm{SU}(A, \eta; \mathbb{Q}[\sqrt{r}\,])$.

Corrections

Intermediate case

We seem to have shown that all arithmetic subgroups of $\mathrm{SL}(n,\mathbb{R})$ can be constructed from either division algebras (Case 1) or unitary groups (Case 2). However, the discussion in Case 2 assumes that the restriction of α to the kernel of $\overline{\alpha}$ is trivial. If we remove this restriction, then, by the argument of Case 1, the cocycle from $\mathrm{Gal}(\mathbb{C}/\mathbb{Q}[\sqrt{r}\,])$ into $\mathrm{PSL}(n,\mathbb{C})$ yields a simple algebra $\mathrm{Mat}_k(D)$ whose center is $\mathbb{Q}[\sqrt{r}\,]$. The Galois automorphism η of $\mathbb{Q}[\sqrt{r}\,]$ can be extended to an anti-automorphism $\hat{\eta}$ of D. Then, for some $A \in \mathrm{Mat}_k(D)$, the corresponding $\mathbb{Q}$-form is
$$G_{\mathbb{Q}} = \mathrm{SU}\big(A, \hat{\eta}; D\big) = \Big\{\, g \in \mathrm{SL}(k,D) \;\Big|\; gA(g^{\hat{\eta}})^{\mathsf{T}} = A \,\Big\}.$$
Note that this $\mathbb{Q}$-form is obtained by combining unitary groups with division algebras.

Cocompact arithmetic subgroups

One more technique (familiar from the case of $\mathrm{SL}(2,\mathbb{R})$) is needed in order to obtain all of the arithmetic subgroups of $\mathrm{SL}(n,\mathbb{R})$, because the above techniques do not suffice to construct some cocompact examples. The key point is that we need to slightly extend the definition of an arithmetic subgroup. Namely, instead of requiring Γ to be the integer points of G itself, it may be necessary to choose a compact group K, such that $G \times K$ is defined over $\mathbb{Q}$, and allow Γ to be the projection of $(G \times K)_{\mathbb{Z}}$ to G. Because of this, $G_{\mathbb{Q}}$ can be a unitary group over a (totally real) extension of $\mathbb{Q}$, rather than over $\mathbb{Q}$ itself. In other words, we need to consider arithmetic subgroups obtained from "Restriction of Scalars".

$\mathrm{SL}(n,\mathbb{R})$ vs. $\mathrm{SL}(n,\mathbb{C})$

To discuss Galois cohomology, we replaced $\mathbb{R}$ with the algebraically closed field $\mathbb{C}$. Thus, some of the groups we found might not be $\mathbb{Q}$-forms of $\mathrm{SL}(n,\mathbb{R})$ (although we know that their complexification is $\mathrm{SL}(3,\mathbb{C})$). For example, if $G_{\mathbb{Q}} = \mathrm{SU}\big(J,\eta;\mathbb{Q}[\sqrt{r}\,]\big)$, and $r < 0$, then $G_{\mathbb{R}}$ is $\mathrm{SU}(2,1)$, not $\mathrm{SL}(3,\mathbb{R})$.

- In practice, one can determine which of the groups we constructed are $\mathbb{Q}$-forms of $\mathrm{SL}(3,\mathbb{R})$.
- Abstractly, $\mathrm{SL}(3,\mathbb{R})$ is an $\mathbb{R}$-form of $\mathrm{SL}(3,\mathbb{C})$, so, by the general principle, it is represented by a cohomology class $\beta \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mathrm{Aut}(G_{\mathbb{C}}))$. There is a natural restriction homomorphism
  $r\colon H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{Q}),\mathrm{Aut}(G_{\mathbb{C}})) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mathrm{Aut}(G_{\mathbb{C}}))$,
  and the $\mathbb{Q}$-forms of $\mathrm{SL}(3,\mathbb{R})$ are represented by the elements of $r^{-1}(\beta)$.

$\mathbb{C}$ vs. $\overline{\mathbb{Q}}$

For Galois cohomology, we should really be using the algebraic closure $\overline{Q}$ of $\mathbb{Q}$, instead of $\mathbb{C}$, and $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), G_{\overline{\mathbb{Q}}})$ is defined to be the natural limit of the groups $H^1(\mathrm{Gal}(F/\mathbb{Q}), G_{\overline{\mathbb{Q}}})$, where F ranges over all finite extensions of $\mathbb{Q}$.

Why unitary groups are arithmetic

Proposition

- *η = Galois automorphism of $\mathbb{Q}(\sqrt{r}) \neq \mathbb{Q}$,*
  where $r \in \mathbb{Z}^+$ is square-free,
  which means $\eta(a + b\sqrt{r}) = a - b\sqrt{r}$,
- $J = \begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}$ *or, if you prefer,* $J = \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix}$
- $\Gamma_r = \mathrm{SU}\big(J,\eta;\mathbb{Q}\mathbb{Z}[\sqrt{r}\,]\big)$
  $= \Big\{ g \in \mathrm{SL}\big(3,\mathbb{Z}[\sqrt{r}\,]\big) \;\Big|\; gJ({}^{\eta}g)^{\mathsf{T}} = J \Big\}.$

Then Γ_r is an arithmetic subgroup of $\mathrm{SL}(3,\mathbb{R})$.

Theorem (Weil 1960) (or Siegel earlier?)

Suppose Γ is an arithmetic subgroup of $G = \mathrm{SL}(3,\mathbb{R})$. If G/Γ is <u>not</u> compact, then Γ is commensurable to either $\mathrm{SL}(3,\mathbb{Z})$ or Γ_r, for some r.

Remark

The value of r is unique: if $r_1 \neq r_2$, then no finite-index subgroup of Γ_{r_1} is isomorphic to a finite-index subgroup of Γ_{r_2}.

$$\begin{aligned} \mathbb{Q}[\sqrt{r_1}\,] \neq \mathbb{Q}[\sqrt{r_2}\,] &\implies \ker \overline{\alpha_1} \neq \ker \overline{\alpha_2} \\ &\implies \overline{\alpha_1} \neq \overline{\alpha_2} \implies \alpha_1 \not\sim \alpha_2 \\ &\implies \mathbb{Q}\text{-forms are different.} \end{aligned}$$

(But different A's sometimes give the same $\mathbb{Q}$-form.)

Want: Γ_r is an arithmetic subgroup of $G = \mathrm{SL}(3,\mathbb{R})$

Construct embedding $\rho\colon G \hookrightarrow \mathrm{SL}(6,\mathbb{R})$,
such that $\rho(G) \cap \mathrm{SL}(6,\mathbb{Z}) = \rho(\Gamma_r)$.

Note:

$$G \times G = \begin{bmatrix} * & * & * & & & \\ * & * & * & & & \\ * & * & * & & & \\ & & & * & * & * \\ & & & * & * & * \\ & & & * & * & * \end{bmatrix} \subset \mathrm{SL}(6,\mathbb{R}).$$

Let $\widehat{G} = \{\, (g,h) \in G \times G \mid gJh^{\mathsf{T}} = J \,\}$.

$\widehat{G} = \{\, (g,h) \in G \times G \mid gJh^{\mathsf{T}} = J \,\}$

Each g determines a unique h, so $\widehat{G} \cong G$.
We may let $\rho(G) = \widehat{G}$.

$(1,1)$ and $(\sqrt{r}, -\sqrt{r})$ are linearly independent,
so they form a basis of $\mathbb{R}^2$.
Thus, $\exists$ invertible linear trans of $\mathbb{R}^6$ that maps $\mathbb{Z}^6$ to
$\Lambda = \{\, (x,y,z,x^{\eta},y^{\eta},z^{\eta}) \mid x,y,z \in \mathbb{Z}[\sqrt{r}\,] \,\}$.
Since $\mathrm{SL}(6,\mathbb{Z}) = \{\, a \in \mathrm{SL}(6,\mathbb{R}) \mid a\mathbb{Z}^6 = \mathbb{Z}^6 \,\}$,
this means we may pretend (after a change of basis)

$$\begin{aligned} &(G \times G) \cap \mathrm{SL}(6,\mathbb{Z}) \\ &\quad = \{\, (g,h) \in G \times G \mid (g,h)\Lambda = \Lambda \,\} \\ &\quad = \Big\{ (g,g^{\eta}) \;\Big|\; g \in \mathrm{SL}\big(3,\mathbb{Z}[\sqrt{r}\,]\big) \Big\}. \end{aligned}$$

Want: $\rho(G) \cap \mathrm{SL}(6,\mathbb{Z}) = \rho(\Gamma_r)$.
Know: $\rho(G) = \widehat{G} = \{\, (g,h) \in G \times G \mid gJh^{\mathsf{T}} = J \,\}$,
and $(G \times G) \cap \mathrm{SL}(6,\mathbb{Z})$
$= \Big\{ (g,g^{\eta}) \;\Big|\; g \in \mathrm{SL}\big(3,\mathbb{Z}[\sqrt{r}\,]\big) \Big\}$.

Then
$\rho(\Gamma_r) = \{\, (g,g^{\eta}) \mid g \in \Gamma_r \,\}$,
and

$$\begin{aligned} \rho(G) \cap \mathrm{SL}(6,\mathbb{Z}) &= \widehat{G} \cap \big((G \times G) \cap \mathrm{SL}(6,\mathbb{Z})\big) \\ &= \left\{ (g,g^{\eta}) \;\middle|\; \begin{array}{c} g \in \mathrm{SL}\big(3,\mathbb{Z}[\sqrt{r}\,]\big), \\ gJ(g^{\eta})^{\mathsf{T}} = J \end{array} \right\} \\ &= \Big\{ (g,g^{\eta}) \;\Big|\; g \in \mathrm{SU}\big(J,\eta;\mathbb{Z}[\sqrt{r}\,]\big) \Big\} \\ &= \rho(\Gamma_r). \end{aligned}$$

$\boxed{\rho(G) \cap \mathrm{SL}(6,\mathbb{Z}) = \rho(\Gamma_r)}$

Conclude Γ_r is arith subgrp <u>if</u> $\rho(G)$ def'd over $\mathbb{Q}$.

Can be done directly (find polynomials with coeffs in $\mathbb{Q}$),
but it is confusing – need to work in a strange basis.

Instead, we will verify that $G_{\mathbb{Q}}$ is dense in G.

$$\begin{aligned} G_{\mathbb{Z}} = \Gamma_r &= \mathrm{SU}\big(J,\eta;\mathbb{Z}[\sqrt{r}\,]\big) \\ &= \Big\{ g \in \mathrm{SL}\big(3,\mathbb{Z}[\sqrt{r}\,]\big) \;\Big|\; gJ(g^{\eta})^{\mathsf{T}} = J \Big\}. \\ \Rightarrow\quad G_{\mathbb{Q}} &= \mathrm{SU}\big(J,\eta;\mathbb{Q}[\sqrt{r}\,]\big) \\ &= \Big\{ g \in \mathrm{SL}\big(3,\mathbb{Q}[\sqrt{r}\,]\big) \;\Big|\; gJ(g^{\eta})^{\mathsf{T}} = J \Big\}. \end{aligned}$$

$$G_{\mathbb{Q}} = \left\{ g \in \mathrm{SL}\big(3, \mathbb{Q}[\sqrt{r}\,]\big) \;\middle|\; gJ(g^{\eta})^{\mathsf{T}} = J \right\}$$

So $\left\{ \begin{bmatrix} 1 & x & t\sqrt{r} - \dfrac{x\,x^{\eta}}{2} \\ & 1 & -x^{\eta} \\ & & 1 \end{bmatrix} \;\middle|\; \begin{matrix} x \in \mathbb{Q}[\sqrt{r}\,], \\ t \in \mathbb{Q} \end{matrix} \right\} \subset G_{\mathbb{Q}}.$

This is dense in $U = \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix}$.

$G_{\mathbb{Q}}$ also contains a dense subgroup of U^{T}.
(In fact, it is easy to verify that $(G_{\mathbb{Q}})^{\mathsf{T}} = G_{\mathbb{Q}}$.)

Since $\langle U, U^{\mathsf{T}} \rangle = \mathrm{SL}(3,\mathbb{R}) = G$,
this implies $G_{\mathbb{Q}}$ is dense in G.

Lecture 3

How to make ~~arithmetic subgroups~~ $\mathbb{Q}$-forms of $\mathrm{SL}(n,\mathbb{R})$
1) division algebras 2) unitary groups
3) combination of the two

1. Division algebras

division algebra D over $\mathbb{Q}$, such that $D \otimes \mathbb{R} \cong \mathrm{Mat}_{d\times d}(\mathbb{R})$
$\rightsquigarrow$ $\mathbb{Q}$-form $\mathrm{SL}(n,D)$ of $\mathrm{SL}(dn,\mathbb{R})$.

Example: Quaternions

$\mathbb{H}_{\mathbb{Q}}^{a,b} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ $\quad (i^2 = a,\ j^2 = b,\ k = ij = -ji)$
$= F + Fj \qquad F = \mathbb{Q} + \mathbb{Q}i = \mathbb{Q}[\sqrt{a}]$
$j^2 = b,\ \ jx = x^{\eta} j,\ \ \langle \eta \rangle = \mathrm{Gal}(F/\mathbb{Q})$

Division algebra if b is not a norm in F
$b \neq x\,x^{\eta} = \square - a\square$

$\mathbb{H}_{\mathbb{Q}}^{a,b} = F + Fj,$
$|F:\mathbb{Q}| = 2,\ \ j^2 = b \in \mathbb{Q},\ \ jx = x^{\eta} j,\ \ \langle \eta \rangle = \mathrm{Gal}(F/\mathbb{Q})$

How to make a division algebra over $\mathbb{Q}$

$D = F + Fj + Fj^2 + \cdots + Fj^{d-1}$ (cyclic)
$|F:\mathbb{Q}| = d,\ j^d = b \in \mathbb{Q},\ jx = x^{\eta} j,\ \ \langle \eta \rangle = \mathrm{Gal}(F/\mathbb{Q})$

Eg. Choose $p \equiv 1 \pmod{d}$. $\quad \exists\, e \in \mathbb{Z}_p^{\times}$ of order $(p-1)/d$.
Let $\zeta = \sqrt[p]{1}$, and $F = \mathbb{Q}[\zeta^{e} + \zeta^{e^2} + \cdots + \zeta^{e^{(p-1)/d}}]$.

Division algebra if b^m not a norm in F, for $m < d$.
$b^m \neq x\,x^{\eta}\,x^{\eta^2} \cdots x^{\eta^{d-1}}$ $\qquad (m = 1$ if d is prime$)$

$G_{\mathbb{Q}} = \mathrm{SL}(k,D). \qquad G_{\mathbb{Z}} \doteq \mathrm{SL}(k, D_{\mathbb{Z}}).$

$F = \mathbb{Q}[\varphi]$, where φ is alg'ic int, and let $\mathcal{O} = \mathbb{Z}[\varphi]$.
Then $D_{\mathbb{Z}} = \mathcal{O} + \mathcal{O}j + \mathcal{O}j^2 + \cdots + \mathcal{O}j^{d-1}$, $\quad$ if $b \in \mathbb{Z}$.

---

1. Division algebras

2. Unitary groups

$F = \mathbb{Q}[\sqrt{r}]$, and $\langle \eta \rangle = \mathrm{Gal}(F/\mathbb{Q})$.
$A \in \mathrm{GL}(n,F)$ Hermitian $\ ((A^{\eta})^{\mathsf{T}} = A)$
Can assume $A = \mathrm{diag}(a_1,\ldots,a_n)$, $\quad a_i \in \mathbb{Q}^{\times}$.
$G_{\mathbb{Q}} = \mathrm{SU}(A,\eta;F) = \{ g \in \mathrm{SL}(n,F) \mid g\,A\,(g^{\eta})^{\mathsf{T}} = A \}$.
$G_{\mathbb{Z}} \doteq \mathrm{SU}(A,\eta;\mathbb{Z}[\sqrt{r}])$

Note: F is uniquely determined by $G_{\mathbb{Q}}$.
But $\mathrm{SU}(A,\eta;F) \cong \mathrm{SU}(B,\eta;F)$ if $B = XA(X^{\eta})^{\mathsf{T}}$.
$\Rightarrow$ can make A diagonal

3. Combination

$F = \mathbb{Q}[\sqrt{r}]$, and $\langle \eta \rangle = \mathrm{Gal}(F/\mathbb{Q})$.
$A \in \mathrm{GL}(n,F)$ Hermitian $\ ((A^{\eta})^{\mathsf{T}} = A)$
$G_{\mathbb{Q}} = \mathrm{SU}(A,\eta;F) = \{ g \in \mathrm{SL}(n,F) \mid g\,A\,(g^{\eta})^{\mathsf{T}} = A \}$.

3. Combine division algebras with unitary groups

$F = \mathbb{Q}[\sqrt{r}]$, and $\langle \eta \rangle = \mathrm{Gal}(F/\mathbb{Q})$.
Division algebra D over **F**, such that
η extends to antiaut $\boldsymbol{\eta}$ of D: $\ (ab)^{\boldsymbol{\eta}} = b^{\boldsymbol{\eta}}\,a^{\boldsymbol{\eta}}$.
$A \in \mathrm{GL}(n,D)$ Hermitian $\ ((A^{\boldsymbol{\eta}})^{\mathsf{T}} = A)$
(Can assume $A = \mathrm{diag}(a_1,\ldots,a_n)$, $\quad a_i \in D^{\times},\ a_i{}^{\boldsymbol{\eta}} = a_i$.)
$G_{\mathbb{Q}} = \mathrm{SU}(A,\eta;D), \qquad G_{\mathbb{Z}} = \mathrm{SU}(A,\eta;D_{\mathbb{Z}})$

Same methods apply to other groups

Galois cohomology finds arithmetic subgroups of any simple Lie group, not just $\mathrm{SL}(n,\mathbb{R})$.

Illustration: find the simple Lie groups (over $\mathbb{R}$).

Simple Lie groups over $\mathbb{C}$

Type A, B, C, D, E, F, G.

- E, F, and G are *exceptional* groups — ignore.
- A – D are *classical*.

Type A: $G_{\mathbb{C}} = \mathrm{SL}(n,\mathbb{C})$.
Obvious $\mathbb{R}$-form is $\mathrm{SL}(n,\mathbb{R})$.
Previous discussion: $\alpha \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{Aut}(G_{\mathbb{C}}))$.

Case 1. $\alpha \in H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{Inn}(G_{\mathbb{C}}))$. "Inner form"
Comes from division algebra over $\mathbb{R}$.
Only division algebra is $\mathbb{H}$: $G_{\mathbb{R}} = \mathrm{SL}(k,\mathbb{H})$.

Case 2. $\overline{\alpha}$: $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathrm{Out}(G_{\mathbb{C}})$ nontriv. "Outer form"

- Unitary group: $G_{\mathbb{R}} = \mathrm{SU}(m,n)$.
- Combine unitary group with division algebra over $F = \mathbb{R}[\sqrt{r}] = \mathbb{C}$. $\quad \nexists$ div alg over $\mathbb{C}$.

Type B: $G_{\mathbb{C}} = \mathrm{SO}(n,\mathbb{C})$, with n odd.
Out$(G_{\mathbb{C}})$ trivial, so all $\mathbb{R}$-forms are inner.
$G_{\mathbb{R}} = \mathrm{SO}(p,q)$.

Type C:
$G_{\mathbb{C}} = \mathrm{Sp}(2n,\mathbb{C}) = \{ g \in \mathrm{SL}(2n,\mathbb{C}) \mid gJg^{\mathsf{T}} = J \}$

where $J = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & -1 & & & \\ -1 & & & & \end{bmatrix}$.

Obvious $\mathbb{R}$-form is $\mathrm{Sp}(2n,\mathbb{R})$.

Out$(G_{\mathbb{C}})$ is trivial (so forms inner), but can use $\mathbb{H}$:
$G_{\mathbb{R}} = \mathrm{SU}(I_{p,q},\eta;\mathbb{H}) = \mathrm{Sp}(p,q)$.
$\eta(a + bi + cj + dk) = a - bi - cj - dk$

Type D: $G_{\mathbb{C}} = \mathrm{SO}(2n,\mathbb{C})$. Obvious $G_{\mathbb{R}} = \mathrm{SO}(p,q)$.
Out$(G_{\mathbb{C}}) \cong \mathbb{Z}_2$ (if $2n \neq 8$), but inner in $\mathrm{O}(2n,\mathbb{C})$.
Can use quaternions:
$G_{\mathbb{R}} = \mathrm{SU}(I,\tilde{\eta};\mathbb{H}) = \mathrm{SO}(n,\mathbb{H}) = \mathrm{SO}^*(n)$.
$\tilde{\eta}(a + bi + cj + dk) = a + bi - cj + dk$

Arithmetic groups of classical type

$G_{\mathbb{Q}} = \mathrm{SL}(n,F),\ \mathrm{SL}(n,D),\ \mathrm{SU}(A,\eta;F),\ \mathrm{SU}(A,\boldsymbol{\eta};D)$
$\Rightarrow G_{\mathbb{R}} = \mathrm{SL}(n,\mathbb{R}),\ \mathrm{SL}(n,\mathbb{C}),\ \mathrm{SL}(n,\mathbb{H}),\ \mathrm{SU}(p,q)$,
or product of these

$G_{\mathbb{Q}} = \mathrm{SO}(A,F) \quad \Rightarrow G_{\mathbb{R}} = \mathrm{SO}(p,q),\ \mathrm{SO}(n,\mathbb{C})$ or product

$G_{\mathbb{Q}} = \mathrm{SU}(A,\tilde{\eta},\mathbb{H}_F^{a,b}) \qquad \Rightarrow G_{\mathbb{R}} = \mathrm{SO}(n,\mathbb{H})$,
or preceding orthogonal groups or product

$G_{\mathbb{Q}} = \mathrm{Sp}(n,F),\ \mathrm{SU}(A,\eta,\mathbb{H}_F^{a,b})$
$\Rightarrow G_{\mathbb{R}} = \mathrm{Sp}(n,\mathbb{R}),\ \mathrm{Sp}(n,\mathbb{C}),\ \mathrm{Sp}(p,q)$ or product

$$G_{\mathbb{Q}} = \mathrm{SL}(n,F),\ \ \mathrm{SL}(n,D),\ \ \mathrm{SU}(A,\eta;F),\ \ \mathrm{SO}(A,F),$$
$$\mathrm{SU}(A,\tilde{\eta},\mathbb{H}_F^{a,b}),\ \ \mathrm{Sp}(n,F),\ \ \mathrm{SU}(A,\eta,\mathbb{H}_F^{a,b})$$

This lists **all** $\mathbb{Q}$-forms of classical simple Lie groups
(SL, SO, SU, Sp)
except some outer forms of
$\mathrm{SO}(8,\mathbb{C}),\ \ \mathrm{SO}(p,8-p),\ \ \mathrm{SO}(4,\mathbb{H})$.

Missing: $\left|\mathrm{Out}(\widetilde{\mathrm{SO}}(8,\mathbb{C}))\right| = 6$:
Image of $\overline{\alpha}$ can be $\mathbb{Z}_3$ or S_3. (not trivial or $\mathbb{Z}_2$)
"**triality**" groups

References

V. Platonov and A. Rapinchuk,
Algebraic Groups and Number Theory,
Academic Press, New York, 1994. MR1278263

(See §2.2–§2.3 for the use of Galois cohomology to find $\mathbb{Q}$-forms of simple algebraic groups.)

Dave Witte Morris,
Introduction to Arithmetic Groups (in preparation).
`http://arxiv.org/abs/math/0106063`

(*Examples of Lattices* chapter includes sections on lattices in $\mathrm{SL}(3,\mathbb{R})$ and, more generally, $\mathrm{SL}(n,\mathbb{R})$.

Arithmetic Lattices in Classical Groups chapter describes the arithmetic subgrps of all classical Lie grps, not just $\mathrm{SL}(n,\mathbb{R})$.