Arithmetic Subgroups and Applications

By Mariam Almahdi Mohammed Mull'a, Amal Mohammed Ahmed Gaweash
& Hayat Yousuf Ismail Bakur

University of Kordofan

Abstract- Arithmetic subgroups are an important source of discrete groups acting freely on manifolds. We need to know that there exist many torsion-free $SL(2, \mathbb{R})$ is an "arithmetic" subgroup of $SL(2, \mathbb{R})$. 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 $SL(n, \mathbb{R})$, with $n>2$. In fact, a calculation of group cohomology shows that the only other way to construct arithmetic subgroups of $SL(n, \mathbb{R})$ is by using arithmetic groups. In this paper justifies Commensurable groups, and some definitions and examples, $\mathbb{R}$-forms of classical simple groups over $\mathbb{C}$, calculating the complexification of each classical group, Applications to manifolds. Let us start with $SS(n,\mathbb{C})$. This is already a complex Lie group, but we can think of it as a real Lie group of twice the dimension. As such, it has a complexification.

Keywords: lie group, commensurable groups, orthogonal group, symplectic group, subgroups, congruence subgroup, arithmetic subgroups, cohomology, equivalence class, automorphism.

ARITHMETICSUBGROUPSANDAPPLICATIONS

Strictly as per the compliance and regulations of:

Arithmetic Subgroups and Applications

Mariam Almahdi Mohammed Mull'a α, Amal Mohammed Ahmed Gaweash σ
& Hayat Yousuf Ismail Bakur ρ

Abstract- Arithmetic subgroups are an important source of discrete groups acting freely on manifolds. We need to know that there exist many torsion-free $SL(2,\mathbb{Z})$ is an "arithmetic" subgroup of $SL(2,\mathbb{R})$. 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 $SL(n,\mathbb{R})$, with $n > 2$. In fact, a calculation of group cohomology shows that the only other way to construct arithmetic subgroups of $SL(n,\mathbb{R})$ is by using arithmetic groups. In this paper justifies Commensurable groups, and some definitions and examples, $\mathbb{R}$-forms of classical simple groups over $\mathbb{C}$, calculating the complexification of each classical group, Applications to manifolds. Let us start with $SL(n,\mathbb{C})$. This is already a complex Lie group, but we can think of it as a real Lie group of twice the dimension. As such, it has a complexification.

Subject Areas: mathematical analysis, mathematical modern algebra and foundation of mathematics.

Keywords: lie group, commensurable groups, orthogonal group, symplectic group, subgroups, congruence subgroup, arithmetic subgroups, cohomology, equivalence class, automorphism.

I. Introduction

In This paper we will give a quite explicit description of the arithmetic subgroups of almost every classical Lie group G. (Recall that a simple Lie group G is "classical" if it is either a special linear group, an orthogonal group, a unitary group, or a symplectic group The key point is that all the $\mathbb{Q}$-forms of G are also classical, not exceptional, so they are fairly easy to understand. However, there is an exception to this rule, some 8-dimensional orthogonal groups have $\mathbb{Q}$-forms of so-called triality type, that are not classical and will not be discussed in any detail here given G, which is a Lie group over $\mathbb{R}$, we would like to know all of its $\mathbb{Q}$-forms (because, by definition, arithmetic groups are made from $\mathbb{Q}$-forms) [1,2,3]. However, we will start with the somewhat simpler problem that replaces the fields $\mathbb{Q}$ and $\mathbb{R}$ with the fields $\mathbb{R}$ and $\mathbb{C}$: finding the $\mathbb{R}$-forms of the classical Lie groups over $\mathbb{C}$. In this paper we construct methods by arithmetic groups. The associated symmetric space $SL_2(\mathbb{R}) = SO_2$ is the hyperbolic plane $\mathbb{H}^2$. There are uncountably many lattices in $SL_2(\mathbb{R})$ (with the associated locally symmetric spaces being nothing other than Riemann surfaces), but only countably many of them are arithmetic. But in higher rank Lie groups, there is the following truly

Author α: Department of Mathematics, University of Hafr Al-Batin (UoHB), Hafr Albatin, KSA, University of Kordofan, El-Obeid, North Kordofan, Sudan. e-mail: marimdx2014@gmail.com

Author σ: Department of Mathematics, University of Taif , KSA, University of Aldalling, Sudan. e-mail: amal.gaweash@gmail.com

Author ρ: Department of Mathematics, University of Jazan, KSA. University of Kordofan, El-Obeid, North Kordofan, Sudan.
e-mail: hayatdxdy@gmail.com

remarkable theorem known as Margulis arithmeticity. Let G be a connected semi simple Lie group with trivial centre and no compact factors, and assume that the real rank of G is at least two. Then every irreducible lattice $\Gamma \subset G$ is arithmetic [4, 5, 6]. These groups play a fundamental role in number theory, and especially in the study of automorphic forms, which can be viewed as complex valued functions on a symmetric domain which are invariant under the action ofan arithmetic group. Appeared that some arithmetic groups are the symmetry groups of several string theories. This is probably why this survey fits into these proceedings[7].

II.   COMMENSURABLE GROUPS

Subgroups H_1 and H_2 of a group are said to be commensurable if $H_1 \cap H_2$ is of finiteindex in both H_1 and H_2.The subgroups $a\mathbb{Z}$ and $b\mathbb{Z}$ of $\mathbb{R}$ are commensurable if and only if $\frac{a}{b} \in \mathbb{Q}$. For example, $6\mathbb{Z}$ and $4\mathbb{Z}$are commensurable because they intersect in $12\mathbb{Z}$, but $1\mathbb{Z}$ and $\sqrt{2}\mathbb{Z}$ are not commensurable because they intersect in $\{0\}$. More generally, lattices $L$and L'in a realvector space $V$are commensurable if and only if they generate the same $\mathbb{Q}$-subspace of V.Commensurability is an equivalence relation, it is reflexive and symmetric, and if H_1, H_2 and $H_2, H_3$are commensurable, one shows easily that $H_1 \cap H_2 \cap H_3$ is offinite index in H_1, H_2 and H_3 [8,9].

a) Definition

Let H_1 and H_2 be subgroups of a group G. We say that H_1 and H_2 are commensurable if $[H_1 : K], [H_2 : K] < \infty$, where $K = H_1 \cap H_2$, [6,10]

b) Remark

"Being commensurable" is an equivalence relation [11].

c) Examples

G finite: any two H_1 and H_2 are commensurable. $G = Z$: H_1 and H_2 are commensurable iff they are isomorphic [13].

d) The geometry topology

Let H_1 and H_2 as fundamental groups.For instance, let $G = PSL(2, \mathbb{C})$ acting on H_3 and let H_1 and H_2 be lattices which are fundamental groups of hyperbolic manifolds (or, more generally, or bifolds). if $H_1$and $H_2$are commensurable X/H_1 and $\frac{X}{H_2}$have a common finite cover. Since (orbifold) fundamental groups are defined as subgroups of G only up to conjugacy, it is natural to allow subgroups to have a finite index intersection only up to conjugacy[5,4].

e) Definition

Let H_1 and H_2 be subgroups of a group G. We say that $H_1$and H_2 are weakly commensurable if there is a g in G suchthat $[H_1 : K], [H_2 : K] < \infty$, where $K = H_1 \cap gH_2g^{-1}$[9]

f) Remark

"Weak commensurability" is also an equivalence relation [13].

Ref

9. HELGASON, S. 1978. Differential geometry, Lie groups, and symmetric spaces, volume 80 of Pure and Applied Mathematics. Academic Press Inc., New York.

g) *The Geometry Topology in dimension 2*

Let S_g denote the fundamental group of the genus g close orientable surface. of course $S_g \subset S_2$ for all $g \geq 2$. On the other hand one can find discrete surface groups H_1 and H_2 inside $G = PSL(2,R)$ which are not (weakly) commensurable[14].

h) *Definition*

Let H_1 and H_2 be groups. We say that H_1 and H_2 are abstractly commensurable if there are subgroups K_i of $H_i, i = 1,2$, such that $[H_1 : K_1], [H_2 : K_2] < \infty$ and $K_1 \cong K_2$ [5].

III. DEFINITIONS

Let G be an algebraic group over $\mathbb{Q}$. Let $\rho : G \to GL_V$ be a faithful representation of G on a finite-dimensional vector space V, and let L be a lattice in V. Define

$$.G(\mathbb{Q})_L = \{g \in G(\mathbb{Q}) | \rho(g)L = L\}. \tag{1}$$

An arithmetic subgroup of $\boldsymbol{G}(\mathbb{Q})$ is any subgroup commensurable with $\boldsymbol{G}(\mathbb{Q})_{\boldsymbol{L}}$. For an integer $N > 1$, the principal congruence subgroup of level N is:

$$\Gamma(N)_L = \{g \in G(\mathbb{Q})_L | g \text{ acts as } 1 \text{ on } L/NL\} \tag{2}$$

In other words, $.\Gamma(N)_L$ is the kernel of

$$G(\mathbb{Q})_L \to Aut(L/NL).$$

In particular, it is normal and of finite index in $G(\mathbb{Q})_{\boldsymbol{L}}$ congruence subgroup of $G(\mathbb{Q})$ is any subgroup containing some $\Gamma(N)$ as a subgroup of finite index, so congruence subgroups are arithmetic subgroups [15].

a) *Example*

Let $G = GL_n$ with its standard representation on $\mathbb{Q}^n$ and its standard lattice $L = Z^n$. Then $G(\mathbb{Q})_L$ consists of the $A = GL_n(\mathbb{Q})$ such that
$A\mathbb{Z}^n = \mathbb{Z}^n$. On applying A to $e_1, \dots, e_n$, we see that this implies that A has entries in $\mathbb{Z}$. Since $A^{-1}\mathbb{Z}^n = \mathbb{Z}^n$, the same is true of A^{-1}. Therefore, $G(\mathbb{Q})_L$ is:

$$GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) | det(A) = \pm 1\} \tag{3}$$

The arithmetic subgroups of $GL_n(\mathbb{Q})$ are those commensurable with $GL_n(\mathbb{Z})$[16]. By definition,

$$\Gamma(N) = \{A \in GL_n(\mathbb{Z}) | A \equiv I \bmod N\}$$
$$= \{(a_{ij}) \in GL_n(\mathbb{Z}) | N \text{ divides } (a_{ij} - \delta_{ij})\}, \tag{4}$$

Which is the kernel of

$$GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/N\mathbb{Z}).$$

b) *Example*
The group

$$Sp_{2n}(\mathbb{Z}) = \left\{A \in GL_{2n}(\mathbb{Z}) \Big| A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\right\} \tag{5}$$

15. N. Bourbaki: Lie Groups and Lie Algebras, Chapters 7. Springer, Berlin, 2005. ISBN 3-540-43405-4, MR 2109105.

is an arithmetic subgroup of $Sp_{2n}(\mathbb{Z})$, and all arithmetic subgroups are commensurable with it [3].

IV. R-FORMS OF CLASSICAL SIMPLE GROUPS OVER $\mathbb{C}$

To set the stage, let us recall the classical result that almost all complex simple groups are classical:

a) Theorem

All but finitely many of the simple Lie groups over $\mathbb{C}$ are isogenous to either $SL(n, \mathbb{C})$, $SO(n, \mathbb{C})$, or $Sp(2n, \boldsymbol{C})$, for some n, [15, 17]

b) Remark

Up to isogeny, there are exactly five simple Lie groups over $\mathbb{C}$ that are not classical. They are the "exceptional" simple groups, and are called E_6, E_7, E_8, F_4, and G_2.

We would like to describe the $\mathbb{R}$-forms of each of the classical groups. For example, finding all the $\mathbb{R}$-forms of $SL(n, \mathbb{C})$ would mean making a list of the (simple) Lie groups G, such that the "complexification" of G is $SL(n, \mathbb{C})$. This is not difficult, but we should perhaps begin by explaining more clearly what it means. It has already been mentioned that, intuitively, the complexification of G is the complex Lie group that is obtained from G by replacing real numbers with complex numbers. For example, the complexification of $SL(n, \mathbb{R})$ is $\boldsymbol{SL}(n, \mathbb{C})$. In general, G is (isogenous to) the set of real solutions of a certain set of equations, and we let $G_\mathbb{C}$ be the set of complex solutions of the same set of equations [18]

c) Notation of complex, semisimple

Assume $G \subseteq SL(\ell, \mathbb{R})$, for some ℓ. Since G is almost Zariski closed, there is a certain subset Q of $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$, such that $G^{\square} = Var(Q)^{\square}$. Let:

$$G_\mathbb{C} = Var_\mathbb{C}(Q) = \{ g \in SL(\ell, \mathbb{C}) | Q(g) = 0, \text{ for all } Q \in Q\}. \tag{6}$$

Then $G_\mathbb{C}$ is a (complex, semisimple) Lie group.

d) Example

- $SL(n, \mathbb{R})_\mathbb{C} = SL(n, \mathbb{C})$.
- $SO(n)_\mathbb{C} = SO(n, \mathbb{C})$.
- $SO(m, n)_\mathbb{C} \cong SO(m + n, \mathbb{C})$.

e) Definition

If $G_\mathbb{C}$ is isomorphic to H, then we say that

• H is the complexification of G, and that

• G is an $\mathbb{R}$-form of H

The following result lists the complexification of each classical group. It is not difficult to memorize the correspondence. For example, it is obvious from the notation that the complexification of $Sp(m, n)$ should be symplectic. Indeed, the only case that really requires memorization is the complexification of $SU(m, n)$ [19,2].

Ref

18. J. E. Humphreys: Introduction to Lie Algebras and Representation Theory. Springer, Berlin Heidelberg New York, 1972. MR 0323842.

1. Z. I. Borevich and I. R. Shafarevich: Number Theory, Academic Press, New York, 1966. MR 0195803390 18. Arithmetic Subgroups of Classical Groups.

f) Proposition

Here is the complexification of each classical Lie group.

Real forms of special linear group:

1 $SL(n, \mathbb{R})_{\mathbb{C}} = SL(n, \mathbb{C})$,
2 $SL(n, \mathbb{C})_{\mathbb{C}} \cong SL(n, \mathbb{C}) \times SL(n, \mathbb{C})$,
3 $SL(n, \mathbb{H})_{\mathbb{C}} \cong SL(2n, \mathbb{C})$,
4 $SU(m, n)_{\mathbb{C}} \cong SL(m + n, \mathbb{C})$.

Real forms of orthogonal groups:

1 $SO(m, n)_{\mathbb{C}} \cong SO(m + n, \mathbb{C})$,
2 $SO(n, \mathbb{C})_{\mathbb{C}} \cong SO(n, \mathbb{C}) \times SO(n, \mathbb{C})$,
3 $SO(n, \mathbb{H})_{\mathbb{C}} \cong SO(2n, \mathbb{C})$.

Real forms of symplectic groups:

1 $Sp(n, \mathbb{R})_{\mathbb{C}} = Sp(n, \mathbb{C})$,
2 $Sp(n, \mathbb{C})_{\mathbb{C}} \cong Sp(n, \mathbb{C}) \times Sp(n, \mathbb{C})$,
3 $Sp(m, n)_{\mathbb{C}} \cong Sp(2(m + n), \mathbb{C})$.

V.   CALCULATING THE COMPLEXIFICATION OF CLASSICAL G

Here is justifies Proposition 4.6, by calculating the complexification of each classical group. Let us start with $SL(n, \mathbb{C})$. This is already a complex Lie group, but wecan think of it as a real Lie group of twice the dimension. As such, it has a complexification [20,6].

a) Lemma

The tensor product $H \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to $Mat_{2 \times 2}(\mathbb{C})$.

Proof. Define an $\mathbb{R}$-linear map $\phi: \mathbb{H} \to Mat_{2 \times 2}(\mathbb{C})$ by

$$\phi(1) = Id, \;\; \phi(i) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \;\; \phi(j) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \;\; \phi(k) = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \tag{7}$$

It is straight forward to verify that $\phi$is an injective ring homomorphism. Furthermore, $\phi(\{1, i, j, k\})$ is a $\mathbb{C} - $basis of $Mat_{2 \times 2}(\mathbb{C})$. Therefore, the map $\hat{\phi}: \mathbb{H} \otimes \mathbb{C} \to Mat_{2 \times 2}(\mathbb{C})$ defined by $\hat{\phi}(v \otimes \lambda) = \phi(v)$ $\lambda$is a ring isomorphism [1]

b) How to find the real forms of complex groups in $\mathbb{C}$

Now, we will explain how to find all of the possible $\mathbb{R} - $forms of $SL(n, \mathbb{C})$. We take an algebraic approach, based on Galois theory, and we first review the most basic terminology from the theory of (nonabelian) group cohomology [1].

c) Definitions

Suppose a group Xacts (on the left) by automorphismson a group M. (For $x \in X$ and $m \in M$, we write $^x m$ for the image of munder x.) A function $\alpha: X \to M$ is a 1-cocycle (or "crossed homomorphism") if

$$\alpha(xy) = \alpha(x) \cdot \; ^x \alpha(y) \text{for all} x; \; y \in X.$$

Two 1-cocycles α and β are equivalent (or "cohomologous") if there is some $m \in M$, such that

$$\alpha(x) = m^{-1} \cdot \beta(x) \cdot {}^x m \ for \ all \ x \in X.$$

$\mathcal{H}^1(X,M)$ is the set of equivalence classes of all $1 - cocycles$. It is calledthe first cohomology of X with coefficients in M. A $1 - cocycle$ is a coboundary if it is cohomologoy us to the trivial $1 - cocycle$ defined by $\tau(x) = e$ for all $x \in X$ [6].

d) Galoiscohomology

For convenience, let $G_{\mathbb{C}} = SL(n, \mathbb{C})$. Suppose $\rho: G_{\mathbb{C}} \to SL(N, \mathbb{C})$ is an embedding, such that $\rho(G_{\mathbb{C}})$is defined over $\mathbb{R}$. We wish to find all the possibilities for the group $\rho(G_{\mathbb{C}})_{\mathbb{R}} = \rho(G_{\mathbb{C}}) \cap SL(N, \mathbb{R})$ that can be obtained by considering all the possible choices ofρ.Let σdenote complex conjugation, the nontrivial Galois automorphism of C over R. Since $\mathbb{R} = \{Z \in \mathbb{C} | \sigma(Z) = Z\}$, we have

$$SL(N, \mathbb{R}) = \{g \in SL(N, \mathbb{C}) | \sigma(g) = g\}, \tag{8}$$

where we apply σ to a matrix by applying it to each of the matrix entries.Therefore

$$\rho(G_{\mathbb{C}})_{\mathbb{R}} = \rho(G_{\mathbb{C}}) \cap SL(N, \mathbb{R}) = \{g \in \rho(G_{\mathbb{C}}) | \sigma(g) = g\} \tag{9}$$

Since $\rho(G_{\mathbb{C}})$ is defined over $\mathbb{R}$, we know that it is invariant under σ, so wehave

$$G_{\mathbb{C}} \xrightarrow{\rho} \rho(G_{\mathbb{C}}) \xrightarrow{\sigma} \rho(G_{\mathbb{C}}) \xrightarrow{\rho^{-1}} G_{\mathbb{C}}.$$

Let $\tilde{\sigma} = \rho^{-1} \sigma \rho: G_{\mathbb{C}} \to G_{\mathbb{C}}$be the composition. Then the real form corresponding to ρ is

$$G_{\mathbb{R}} = \rho^{-1}\big(\rho(G_{\mathbb{C}}) \cap SL(N, \mathbb{R})\big) = \{g \in G_{\mathbb{C}} | \tilde{\sigma}(g) = g\} \tag{10}$$

To summarize, the obvious $\mathbb{R}$-form of $G_{\mathbb{C}}$is the set of fixed points of the usual complex conjugation, and any other $\mathbb{R}$-form is the set of fixed points of some other auto morphism of $G_{\mathbb{C}}$. Now let

$$\alpha(\sigma) = \tilde{\sigma}\sigma^{-1}: G_{\mathbb{C}} \to G_{\mathbb{C}}. \tag{11}$$

It is not difficult to see that
- $\alpha(\sigma)$ is an automorphism of $G_{\mathbb{C}}$(as an abstract group), and
- $\alpha(\sigma)$ is holomorphic (since $\rho^{-1}$and $\sigma\rho\sigma^{-1}$are holomorphic - in fact, they can be represented by polynomials in local coordinates). So $\alpha(\sigma) \in \text{Aut}(G_{\mathbb{C}})$. Thus, by defining $\alpha(1)$ to be the trivial automorphism,we obtain a function $\alpha: \text{Gal}(\mathbb{C}/\mathbb{R}) \to \text{Aut}(G_{\mathbb{C}})$. Let $\text{Gal}(\mathbb{C}/\mathbb{R})$ act on $\text{Aut}(G_{\mathbb{C}})$, by defining

$$^{\sigma}\varphi = \sigma\varphi\sigma^{-1} \ \text{for}\varphi \in \text{Aut}(G_{\mathbb{C}}). \tag{12}$$

Then $\alpha(\sigma) = \varphi^{-1} \, {}^{\sigma}\varphi$, $so \, \alpha(\sigma) \cdot {}^{\sigma}\alpha(\sigma) = \alpha(1)$ (since $\sigma^2 = 1$). This means that$\alpha$is $1 - cocycle$ of group cohomology, and therefore defines an element of the cohomology set $\mathcal{H}^1 \text{Gal}(\mathbb{C}/\mathbb{R}), \text{Aut}(G_{\mathbb{C}})$. In fact: This construction provides a one-to-one correspondence between $\mathcal{H}^1 \text{Gal}(\mathbb{C}/\mathbb{R}), \text{Aut}(G_{\mathbb{C}})$. and the set of $\mathbb{R}$ -forms of $G_{\mathbb{C}}$ [21,14,19].

6

Ref

6. J. Tits: Classification of algebraic semi simple groups, in A. Borel and G. D. Mostow, eds.: Algebraic Groups and Discontinuous Subgroups(Boulder,Colo., 1965), Amer. Math. Soc, Providence, R.I., 1966,pp. 33–62. MR 0224710.

VI. APPLICATIONS TO MANIFOLDS

$\mathbb{Z}^{n^2}$ is a discrete subset of $\mathbb{R}^{n^2}$, i.e., every point of $\mathbb{Z}^{n^2}$ has an open neighbourhood(for the real topology) containing no other point of $\mathbb{Z}^{n^2}$, Therefore, $GL_n(\mathbb{Z})$ is discrete in $GL_n(\mathbb{R})$ and it follows that every arithmetic subgroup Γ of a group $G$is discrete in $G(\mathbb{R})$ Let G be an algebraic group over $\mathbb{Q}$. Then $G(\mathbb{R})$ is a Lie group, and for every compactsubgroup $K$of $G(\mathbb{R}), M = G(\mathbb{R})/K$is a smooth manifold [22].

a) Torsion-free arithmetic groups

$SL_2(\mathbb{Z})$ is not torsion-free. For example, the following elements have finite order:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^3 \tag{13}$$

b) Theorem

Every arithmetic group contains a torsion-free subgroup of finite index.For this, it suffices to prove the following Lemma [12].

c) Lemma

For any prime $p \in 3,$ the subgroup $\Gamma(p)/$ of $GL_n(\mathbb{Z})$ is torsion-free.

Proof. If not, it will contain an element of order a prime ℓ and so we will have an equation:

$$(1 + p^m A)^\ell = I \tag{14}$$

with $m \geq 1$and Aa matrix in $M_n(\mathbb{Z})$ not divisible by p. Since I and A commute, we can expand this using the binomial theorem, and obtain an equation:

$$\ell p^m A = -\sum_{i=2}^{\ell} \binom{\ell}{i} p^{mi} A^i \tag{15}$$

In the case that $\ell \neq p$, the exact power of $p$dividing the left hand side is p^m, but p^{2m} divides the right hand side, and so we have a contradiction. In the case that $\ell = p,$ the exact power of $p$dividing the left hand side is p^{m+1}, but, for $2 \leq i < p, p^{2m+1}|\binom{p}{i}p^{mi}$ because $p\binom{p}{i}$, and $p^{2m+1}|p^{mi}$ because $p \geq 3$. A gain we have a contradiction [12].

d) Application to quadratic forms

Consider a binary quadratic form:

$$q(x,y) = ax^2 + bxy + cy^2, \quad a,b,c \in \mathbb{R} \tag{16}$$

Assume q is positive definite, so that its discriminant $\Delta = b^2 - 4ac < 0$. There are many questions one can ask about such forms. For example, for which integers N is there a solution to $q(x,y) = N$ with $x,y \in \mathbb{Z}$ For this, and other questions,the answer depends only on the equivalence class of q, where two forms are said to be equivalent if each can be obtained from the other by an integer change of variables. More precisely, $q$and $q'$are equivalent if there is a matrix $A \in SL_2(\mathbb{Z})$ taking q into $q'$by thechange of variables,

12. LEE, D. H. 2002. The structure of complex Lie groups, volume 429 of Chapman & Hall/CRC Research Notes in Mathematics. Chapman & Hall/CRC, Boca Raton, FL.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}. \tag{17}$$

In other words, the forms:

$$q(x, y) = (x, y). Q. \begin{pmatrix} x \\ y \end{pmatrix}, \quad q'(x, y) = (x, y). Q'. \begin{pmatrix} x \\ y \end{pmatrix} \tag{18}$$

are equivalent if $Q = A^t. Q'. A$ for $A \in SL_2(\mathbb{Z})$. Every positive-definite binary quadratic form can be written uniquely:

$$q(x, y) = a(x - \omega y)(x - \bar{\omega} y), a \in \mathbb{R}, \quad \omega \in \mathcal{H}. \tag{19}$$

If we let Q denote the set of such forms, there are commuting actions of $\mathbb{R}$ and $SL_2(\mathbb{Z})$ on it, and

$$Q/\mathbb{R} \cong \mathcal{H}$$

as $SL_2(\mathbb{Z})$ sets. We say that q is reduced if

$$|\omega| > 1 \text{ and } -\frac{1}{2} \le \Re(\omega) < \frac{1}{2}, \text{or} |\omega| = 1 \text{ and } -\frac{1}{2} \le \Re(\omega) < 0 \tag{20}$$

More explicitly, $q(x, y) = ax^2 + bxy + cy^2$ is reduced if and only if either [9].

$$-a < b \le a < c \text{ or } 0 \le b \le a = c.$$

e) Applications of the classification of arithmetic groups

Consequences of the classification of F-forms. Suppose Γ is an arithmetic subgroup of $SO(m, n)$, and $m + n \ge 5$ is odd. Then there is a finite extension F of Q, with ring of integers $\mathcal{O}$, such that $\Gamma$is commensurable to $SO(A, \mathcal{O})$, for some invertible, symmetric matrix A in $\text{Mat}_{n \times n}(F)$. So $G = SO(m, n)$. Restriction of scalars implies there isa group $\hat{G}$that is defined over an algebraic number field $F$and has a simple factor that is is ogenous to G, such that Γ is commensurable to $\hat{G}_\mathcal{O}$. By inspection, we see that a group of the form $SO(m, n)$ never appears at two places. However, we know that $m + n$ is odd, so the only possibility for $\hat{G}_F$ is $SO(A, F)$. Therefore, Γ is commensurable to $SO(A, \mathcal{O})$ [5, 1, 12].

VII. CONCLUSION

To state the conclusion in our applications, we can expand binomial and obtain an equation. The coefficient group M is sometimesnon-abelian. In case, $H^1(X, M)$ is a set with no obvious algebraic structure. However, if M is an abelian group (as is often assumed ingroup cohomology), $H^1(X, M)$ is an abelian group.The general principle: if $X$is an algebraic object that is defined over $\mathbb{R}$, then $\mathcal{H}^1\text{Gal}(\mathbb{C}/\mathbb{R}), \text{Aut}(X_\mathbb{C})$ is in one-to-one correspondence with the set of $\mathbb{R}$-isomorphism classes of $\mathbb{R}$-defined objects whose $\mathbb{C}$-points are isomorphic to $X_\mathbb{C}$. We will explain how to find all of the possible $\mathbb{R}$-forms of $SL(n, \mathbb{C})$. The techniques can be used algebraic structure, but additional calculations are needed.

Notes

ACKNOWLEDGEMENTS

REFERENCES RÉFÉRENCES REFERENCIAS

1. Z. I. Borevich and I. R. Shafarevich: Number Theory, Academic Press,New York, 1966. MR 0195803390 18. ARITHMETIC SUBGROUPS OF CLASSICAL GROUPS
2. S. Helgason: Differential Geometry, Lie Groups, and Symmetric Spaces. Academic Press, New York, 1978. ISBN 0-12-338460-5, MR 0514561
3. F. E. A. Johnson: On the existence of irreducible discrete subgroups in isotypic Lie groups of classical type, Proc. London Math. Soc.(3) 56 (1988) 51–77. MR 0915530, http://dx.doi.org/10.1112/plms/s3-56.1.51
4. LEE, D. H. 2002. The structure of complex Lie groups, volume 429 of Chapman &Hall/CRC Research Notes in Mathematics. Chapman & Hall/CRC, Boca Raton, FL.
5. BOURBAKI, N. LIE. Groupes et Algebresde Lie. ' El ן ements de math ן ematique. Hermann; ןMasson, Paris. Chap. I, Hermann 1960; Chap. II,III, Hermann 1972; Chap. IV,V,VI, Masson 1981;Chap. VII,VIII, Masson 1975; Chap. IX, Masson 1982 (English translation available from Springer).
6. J. Tits: Classification of algebraic semi simple groups, in A. Borel and G. D. Mostow, eds.: Algebraic Groups and Discontinuous Subgroups(Boulder,Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966,pp. 33–62. MR 0224710.
7. A. Borel , Introduction aux groups arithmjetiques, Paris, Hermann & Cie. 125p. (1969).
8. A.Borel and G. Harder: Existence of discrete cocompact subgroups of reductive groups over local fields, J. Reine Angew. Math.298 (1978)53–64. MR 0483367, http://eudml.org/doc/151965.
9. HELGASON, S. 1978. Differential geometry, Lie groups, and symmetric spaces, volume 80 of Pure and Applied Mathematics. Academic Press Inc., New York.
10. ERDMANN, K. AND WILDON, M. J. 2006. Introduction to Lie algebras. Springer Undergraduate Mathematics Series. Springer-Verlag London Ltd., London.
11. LEE, D. H. 1999. Algebraic subgroups of Lie groups. J. Lie Theory 9:271–284.
12. LEE, D. H. 2002. The structure of complex Lie groups, volume 429 of Chapman & Hall/CRC Research Notes in Mathematics. Chapman & Hall/CRC, Boca Raton, FL.
13. JACOBSON, N. 1962. Lie algebras. Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers, New York-London. Reprinted by Dover 1979.
14. A. Weil: Algebras with involution and the classical groups, J. Indian Math. Soc. 24 (1960) 589–623. MR 0136682.
15. N. Bourbaki: Lie Groups and Lie Algebras, Chapters 7. Springer, Berlin, 2005. ISBN 3-540-43405-4, MR 2109105.
16. V. Platonov and A. Rapinchuk: Algebraic Groups and Number Theory. Academic Press, Boston, 1994. ISBN 0-12-558180-7, MR 1278263.
17. N. Jacobson: Basic Algebra I, 2nd ed. Freeman, New York, 1985. ISBN0-7167-1480-9, MR 0780184.

Notes

18. J. E. Humphreys: Introduction to Lie Algebras and Representation Theory. Springer, Berlin Heidelberg New York, 1972. MR 0323842.

19. E. Cartan: Les groupesŕeels simples finis et continus, ´Ann. Sci. Ecole ´Norm. Sup. 31 (1914) 263 {355. Zbl45.1408.03, *http://* www.numdam.org/item*? id=ASENS 1914 3 31 263 0.*

20. R. S. Pierce: Associative Algebras. Springer, New York, 1982. ISBN0-387-90693-2, MR 0674652.

21. J.–P. Serre: A Course in Arithmetic, Springer, New York 1973.MR 0344216.

22. LEE, J. M. 2003. Introduction to smooth manifolds, volume 218 of Graduate Textsin Mathematics. Springer-Verlag, New York.

Notes