Groups Associated to Simple Lie algebras

Zoltán Halasi

Institute of Mathematics, University of Debrecen

First BIOMICS Summer Workshop
17-19 July 2013, University of Debrecen, Hungary
Topics covered on the talk

- smooth manifolds, tangent spaces, tangent bundle
- the Lie algebra of vector fields of a manifold
- (real) Lie groups and their Lie algebras
- the exponential map
- the Lie correspondence
- Real forms of complex Lie algebras
- Chevalley algebras over finite fields
- Construction of Chevalley groups
- An outline of twisted groups
# Smooth manifolds

## Definition

An \( n \) dimensional (smooth) manifold is the following:

- A set \( M \) together with a collection of maps (called charts) into \( \mathbb{R}^n \); each map is a bijection between a subset of \( X \) and an open subset of \( \mathbb{R}^n \).
- Each point of \( M \) is covered by at least one map. The set of all charts is called an atlas on \( M \).
- For any two maps \( \varphi, \psi : X \to \mathbb{R}^n \) we have \( \varphi \circ \psi^{-1} : \mathbb{R}^n \to \mathbb{R}^n \) is a smooth (i.e. infinitely many times differentiable) function.

Maybe the most natural example for an atlas is how the Earth can be covered by a collection of topographical maps.
## Embedded manifolds

**Definition**

A $k$-dimensional embedded manifold in $\mathbb{R}^n$ is a subset $M \subset \mathbb{R}^n$ given as the common roots of smooth functions $f_1, f_2, \ldots, f_{n-k} : \mathbb{R}^n \to \mathbb{R}$ such that $\text{grad } f_1(p), \ldots, \text{grad } f_{n-k}(p)$ are linearly independent vectors for every $p \in M$.

- Embedded manifolds are smooth manifolds in the usual sense.
- By a theorem of Whitney, every $n$-dimensional smooth manifold can be embedded into a vector space of dimension $2n + 1$.

In the following, all of our examples will be embedded manifolds.
Example: \( S^2 \subset \mathbb{R}^3 \)

Let \( S^2 \subset \mathbb{R}^3 \) be the sphere with radius one centered at the origin. By choosing the function \( f(x, y, z) = x^2 + y^2 + z^2 - 1 : \mathbb{R}^3 \rightarrow \mathbb{R} \) we get

\[
S^2 = \{ (x_0, y_0, z_0) \in \mathbb{R}^3 \mid f(x_0, y_0, z_0) = 0 \}.
\]

Moreover,

\[
\text{grad } f(x_0, y_0, z_0) = (f'_x, f'_y, f'_z)_{x_0, y_0, z_0} = (2x_0, 2y_0, 2z_0) = (0, 0, 0) \iff (x_0, y_0, z_0) = (0, 0, 0).
\]

Since the origin is not on the sphere \( S^2 \), \( \text{grad } f \) is nowhere zero on \( S^2 \), so \( S^2 \) is a two dimensional embedded manifold in \( \mathbb{R}^3 \).
Tangent vectors, Tangent space

(smooth) curve

Let \( M \subseteq \mathbb{R}^n \) be a manifold, and \( \gamma : (a, b) \rightarrow M \) be a smooth function. Then \( \gamma \) is called a curve on \( M \). For any \( c \in (a, b) \) we say \( \gamma'(c) \) is the speed of the curve \( \gamma \) at \( \gamma(c) \).

Tangent vectors, tangent spaces and the tangent bundle

Let \( M \subseteq \mathbb{R}^n \) be a manifold and \( p \in M \). Then \( v \in \mathbb{R}^n \) is a tangent vector of \( M \) at \( p \) if there is a smooth curve \( \gamma(-\varepsilon, \varepsilon) \rightarrow M \) with \( \varepsilon > 0 \), \( \gamma(0) = p \) and \( \gamma'(0) = v \). The tangent space of \( M \) at \( p \) (denoted by \( T_p(M) \)) is the set of all tangent vectors of \( M \) at \( p \). The tangent bundle of \( M \) is the disjoint union \( T(M) = \bigcup_p T_p(M) \).

If \( M \) is an \( n \)-dimensional manifold, then there is a natural \( 2n \)-dimensional manifold structure on \( T(M) \).
Tangent spaces for embedded manifolds

If the embedded manifold $M \subseteq \mathbb{R}^n$ is given by the system of equations $f_1 = \ldots = f_{n-k} = 0$, (with $\text{grad } f_i(p), \ldots, \text{grad } f_{n-k}(p)$ linearly independent for each $p \in M$), then the tangent space of $M$ at $p \in M$ is

$$T_p(M) = \{v \in \mathbb{R}^n \mid v \perp \text{grad } f_i(p) \text{ for all } 1 \leq i \leq n-k\},$$

so $T_p(M) \subseteq \mathbb{R}^n$ is a subspace of dimension $k$.

Example: Tangent spaces of $S^2$

Let $S^2 \subset \mathbb{R}^3$ given by $f(x, y, z) = x^2 + y^2 + z^2 - 1 = 0$ and $p = (x_0, y_0, z_0) \in S^2$. Then the tangent space of $S^2$ at $p$ is $(\text{grad } f(p))^\perp$ which is exactly the subspace perpendicular to the radius vector drawn from the centre of the sphere to $p$. 
Derivations

**smooth functions on a manifold**

Let $M$ be an arbitrary manifold. Then $C^\infty(M)$ denotes the set of all smooth functions from $M$ to $\mathbb{R}$. This is a real associative algebra with pointwise operations.

**Derivation at a point $p \in M$**

A linear function $D : C^\infty(M) \to \mathbb{R}$ is called a derivation at the point $p \in M$ if for every $f, g \in C^\infty(M)$ the Leibniz rule holds:

$$D(fg) = D(f)g(p) + f(p)D(g)$$

The set of all derivations at a point $p \in M$ clearly forms a vector space.
Connection between derivations and tangent vectors

- If \( \gamma : (-\varepsilon, \varepsilon) \to M, \ \varepsilon > 0, \ \gamma(0) = p \) is a smooth curve then the map \( D_{\gamma'}(0) : C^\infty(M) \to \mathbb{R}, \ D_{\gamma'}(0)(f) = (f \circ \gamma)'(0) \) is a derivation at \( p \), which depends only on \( \gamma'(0) \).
- The map \( \gamma'(0) \in T_p(M) \to D_{\gamma'}(0) \) is a one-to-one correspondence between the tangent vectors of \( M \) at \( p \) and the derivations at \( p \).

The derivative of a map

If \( M, N \) are manifolds and \( f : M \to N \) is smooth, then its derivative at a point \( p \in M \) is a linear map \( f'_p(M) : T_p(M) \to T_{f(p)}(N) \).
If \( D = \gamma'(0) \in T_p(M) \) with curve \( \gamma \) satisfying \( \gamma(0) = p \), then \( f'_p(D) = (f \circ \gamma)'(0) \).
Vector fields

**Vector field**

A (smooth) vector field on a manifold $M$ is a smooth function $X : M \to T(M)$ such that $X(p) \in T_p(M)$ for every $p \in M$.

- As $X(p) \in T_p(M)$ can be identified with a derivation $C^\infty(M) \to \mathbb{R}$, a vector field defines a differential operator $X : C^\infty(M) \to C^\infty(M)$ as $(X(f))(p) := X(p)(f)$.
- The space of all vector fields (denoted by $\mathfrak{X}(M)$) are identified with the space of functions $X : C^\infty(M) \to C^\infty(M)$ satisfying $X(fg) = X(f)g + fX(g)$ for every $f, g \in C^\infty(M)$.
- In usual multivariable calculus, derivations at a point $p \in M$ correspond to tangential derivatives, and vector fields correspond to differential operators with smoothly varying direction.
The Lie algebra of vector fields

Lie-bracket of vector fields

As we can think to vector fields as functions $\mathcal{C}^\infty(M) \to \mathcal{C}^\infty(M)$ satisfying the Leibniz rule, they can be composed. Thus, for any pairs of vector fields $X, Y \in \mathfrak{X}(M)$ we can define $[X, Y] := X \circ Y - Y \circ X$ called the Lie-bracket of $X$ and $Y$.

The Lie-bracket makes $\mathfrak{X}(M)$ to a Lie algebra i.e. the following holds for every $X, Y, Z \in \mathfrak{X}(M), \lambda \in \mathbb{R}$.

- $[X + Y, Z] = [X, Z] + [Y, Z]$, $[\lambda X, Y] = \lambda [X, Y]$
- $[Y, X] = -[X, Y]$ (anti-commutation)
- $[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$ (Jacobi-identity)
Lie groups and their Lie algebras

**Group**

$(G, \cdot)$ is a group if $G$ is a set and $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h$ is an operation (usually called multiplication or product) satisfying the following.

- is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every $a, b, c \in G$.
- (identity element) $\exists e \in G$ such that $e \cdot g = g \cdot e = g$ for every $g \in G$.
- (inverse) For every $g \in G$, there is an $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.

**Lie group**

A *(real) Lie group* $G$ is a manifold together with a group structure such that $\cdot : G \times G \to G$ is a smooth function.
Let $G$ be a Lie group. Then the following functions are smooth:

- $G \times G \to G$, $(g, h) \mapsto gh^{-1}$;
- $(\, \cdot \,)^{-1} : G \to G$, $g \mapsto g^{-1}$;
- For any $g \in G$ the **left translation** by $g$ defined as $L_g : G \to G$, $h \mapsto gh$;
- Similarly, $R_g : G \to G$, $h \mapsto hg$ the **right translation** by $g$;
- The **conjugation** by $g \in G$, that is, $L_g \circ R_{g^{-1}} = R_{g^{-1}} \circ L_g$.

**left invariant vector fields**

A vector field $X \in \mathfrak{X}(G)$ on a Lie group $G$ is **left invariant** if $L'_g(X) = X$ for all $g \in G$.

If $X, Y \in \mathfrak{X}(G)$ are both left invariant vector fields, then $[X, Y]$ is also a left invariant vector field.
The Lie algebra of a Lie group

The Lie algebra $\mathfrak{g}$ of a Lie group $G$ consists of all left invariant vector fields over $G$. (It is really a Lie algebra with respect to the Lie bracket.)

- If $X \in \mathcal{X}(G)$ is left invariant then $X(g) = L'_g(X(e))$ for every $g \in G$, so a left invariant vector field $X$ is uniquely determined by $X(e)$.

- Conversely, every $v \in T_e(G)$ can be extended to a left invariant vector field in this way.

- As a result, $X \mapsto X(e)$ is a linear isomorphism from $\mathfrak{g}$ into $T_e(G)$.

- $\mathfrak{g}$ is a finite dimensional Lie algebra and its dimension is the same as the dimension of $G$ (as a manifold).
The classical groups

The general linear group

- Let $M^{n \times n}(\mathbb{R})$ be the set of all $n \times n$ real matrices. (associative algebra over $\mathbb{R}$)
- $GL_n(\mathbb{R}) = \{A \in M^{n \times n}(\mathbb{R}) \mid \exists A^{-1}\}$ is the general linear group.
- $GL_n(\mathbb{R})$ is an open subset of $M^{n \times n}(\mathbb{R})$ given as $A \in GL_n(\mathbb{R}) \iff \det A \neq 0$. ($\det : M^{n \times n}(\mathbb{R}) \to \mathbb{R}$ is a polynomial function with $n^2$ variables)
- The matrix multiplication is given by multivariable polynomials, ($GL_n(\mathbb{R})$ is an algebraic group) so it is smooth.
- Its Lie algebra $\mathfrak{gl}_n(\mathbb{R})$ is isomorphic with the space $M^{n \times n}(\mathbb{R})$ with Lie bracket defined as $[A, B] = AB - BA$.
- Hence, $\mathfrak{gl}_n(\mathbb{R})$ is an $n^2$ dimensional Lie algebra and $GL_n(\mathbb{R})$ is an $n^2$ dimensional Lie group.
The special linear group

- The special linear group is \( SL_n(\mathbb{R}) = \{ A \in M^{n \times n}(\mathbb{R}) \mid \det A = 1 \} \subseteq GL_n(\mathbb{R}) \).

- It is a subset of the space \( M^{n \times n}(\mathbb{R}) \cong \mathbb{R}^{n^2} \) given by the polynomial equation \( f(A) = \det(A) - 1 = 0 \). It is easy to check that \( \text{grad } f(A) = 0 \Rightarrow \det A = 0 \), so the gradient is nowhere zero on \( SL_n(\mathbb{R}) \).

- \( SL_n(\mathbb{R}) \) is an embedded manifold in \( \mathbb{R}^{n^2} \) of dimension \( n^2 - 1 \).

- Its Lie algebra is \( sl_n(\mathbb{R}) = \{ A \in M^{n \times n} \mid \text{Tr } A = 0 \} \).

One can similarly define the groups \( GL_n(\mathbb{C}) \) and \( SL_n(\mathbb{C}) \) and their Lie algebras \( gl_n(\mathbb{C}) \) and \( sl_n(\mathbb{C}) \). Their dimensions are \( 2n^2 \) and \( 2n^2 - 1 \), respectively.
A general construction for classical groups

In the following way we can define

- Let the field $K$ be either $\mathbb{R}$ or $\mathbb{C}$.
- Let $(\cdot)': M^{n\times n}(K) \to M^{n\times n}(K)$ be an $\mathbb{R}$-linear map reversing the order of multiplication (i.e. $(xy)' = y'x'$ and satisfying $(I)' = I$).
- Let $J \in M^{n\times n}(K)$ be a fixed matrix.
- Then $G_J = \{ A \in GL_n(K) \mid AJA' = J \} \leq GL_n(K)$ is a Lie group.
- The Lie algebra $\mathfrak{g}_J$ of $G_J$ is $\mathfrak{g}_J = \{ A \in M^{n\times n}(K) \mid AJ + JA' = 0 \}$.
- Choosing special $(\cdot)'$ and $J$ we get the classical groups.
- In each case, one can take the intersection $G_J \cap SL_n(K)$ to define further groups.
The orthogonal group

- We choose $K = \mathbb{R}$, $(\ )' = (\ )^T$ (transpose) and $J = I \in M^{n \times n}(\mathbb{R})$ (the identity matrix).

- Now, $G_J$ is the orthogonal group
  
  $O_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid AA^T = I \}$

- Every element of $O_n(\mathbb{R})$ has determinant $\pm 1$.

- $SO_n(\mathbb{R}) = \{ A \in O_n(\mathbb{R}) \mid \det A = 1 \}$ is the special orthogonal group, which is a subgroup of index 2 in $O_n(\mathbb{R})$.

- The Lie algebra of both $O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$ is
  
  $\mathfrak{o}_n(\mathbb{R}) = \{ A \in M^{n \times n}(\mathbb{R}) \mid A^T = -A \}$ the Lie algebra of all antisymmetric matrices.

- The dimensions of $O_n(\mathbb{R})$, $SO_n(\mathbb{R})$ and $\mathfrak{o}_n(\mathbb{R})$ are $\frac{n^2 - n}{2}$.

The pseudoorthogonal group

Using $J$ as a diagonal matrix with $k$ ones and $n - k$ minus ones we get the pseudoorthogonal group $G_J = O_{k,n-k}(\mathbb{R})$ of dimension $\frac{n^2 - n}{2}$. As a special case, $O_{n-1,1}(\mathbb{R})$ is the Lorentz group.
The symplectic group

- Let $K = \mathbb{R}$, $(\cdot)' = (\cdot)^T$, $n = 2k$ even and $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$.

- We get the symplectic group $G_J = Sp_n(\mathbb{R})$. Every element of the symplectic group has determinant 1.

- Its Lie algebra is

$$\mathfrak{sp}_n(\mathbb{R}) = \left\{ \begin{pmatrix} A & B \\ C & -A^T \end{pmatrix} \middle| A, B, C \in M^{k \times k}(\mathbb{R}), \right.$$ 

$$B = B^T, \quad C = C^T \right\}$$

- The dimension of the Lie algebra $\mathfrak{sp}_n(\mathbb{R})$ (and of the Lie group $Sp_n(\mathbb{R})$) is $2k^2 + k$. 
The unitary group

- Let $K = \mathbb{C}$, $( )' = ( )^*$ (transpose conjugate $A^* = \overline{A}^T$) and $J = I$.
- We get the unitary group $G_J = U_n = \{ A \in GL_n(\mathbb{C}) \mid AA^* = I \}$ and the special unitary group $SU_n = U_n \cap SL_n(\mathbb{C})$.
- The Lie algebra of $U_n$ is the Lie algebra $u_n = \{ A \in M^{n \times n}(\mathbb{C}) \mid A^* = \}$. 
- As a real Lie group $\dim U_n = n^2$. 
The exponential map

**one-parameter subgroup**

For a Lie group $G$ a **one-parameter subgroup** of $G$ is a smooth homomorphism $\gamma : (\mathbb{R}, +) \to G$.

- For every left invariant vector field $X \in \mathfrak{g}$ there is a unique one-parameter subgroup $\gamma_X : (\mathbb{R}, +) \to G$ with $\gamma_X'(0) = X(e)$.
- With this notation, $\gamma_X'(t) = X(\gamma(t))$ for each $t \in \mathbb{R}$, that is, $\gamma_X$ is the **maximal integral curve** of $X$ satisfying $\gamma(0) = e$.

**The exponential map**

Let $G$ be a Lie group with Lie algebra $\mathfrak{g}$. The **exponential map** of $G$ is a function $\exp : \mathfrak{g} \to G$ given as

$$\exp(X) = \gamma_X(1)$$

for each $X \in \mathfrak{g}$ and the corresponding one-parameter subgroup $\gamma_X$. 
Connection between Lie groups and their Lie algebras

There is a one-to-one correspondence between connected (immersed) subgroups of $G$ and the subalgebras of the Lie algebra $\mathfrak{g}$; normal subgroups correspond to ideals.

For every finite dimensional Lie algebra $\mathfrak{g}$ there is a connected and simply connected Lie group whose Lie algebra is $\mathfrak{g}$.

If $G$ and $H$ are connected and simply connected Lie groups with Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ respectively, then $G$ and $H$ are isomorphic Lie groups if and only if $\mathfrak{g}$ and $\mathfrak{h}$ are isomorphic Lie algebras.
Groups with isomorphic Lie algebras

Let $G$ be an arbitrary Lie group and $G_0$ the identity component of $G$. Thus, $G_0$ is a connected Lie group. One can show that there exists a connected, simply connected universal covering group (denoted by $\hat{G}$) of $G_0$ and it is unique up to isomorphism. The Lie groups, $G$, $G_0$ and $\hat{G}$ have isomorphic Lie algebras.

Example: The rotation group $O_3(\mathbb{R})$

- The Lie group $O_3(\mathbb{R})$ is not connected: It has two components, the elements of determinant 1 and $-1$, respectively.
- Its identity component is $SO_3(\mathbb{C})$, which is not a simply connected Lie group.
- $SU_2$ is the universal covering group of $SO_3(\mathbb{R})$.
- The Lie groups $O_3(\mathbb{R})$, $SO_3(\mathbb{R})$ and $SU_2$ have isomorphic Lie algebras.
The exponential map for linear Lie groups

linear Lie groups and Lie algebras

A Lie group $G$ (resp. Lie algebra $\mathfrak{g}$) is said to be linear if $G \leq GL_n(\mathbb{R})$ (resp. $\mathfrak{g} \leq gl_n(\mathbb{R})$) for some $n$.

The exponential function for matrices

Let $A \in \mathfrak{gl}_n(\mathbb{R})$. Then one can define $e^A$ by substituting $A$ into the usual power series of the exponential function: $e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k$. (Note that this series is convergent for every real matrix $A$.) Now, starting from a linear Lie algebra $\mathfrak{g}$ the group $G = \langle e^A \mid A \in \mathfrak{g} \rangle$ is a Lie group with Lie algebra $\mathfrak{g}$. Moreover, $A \to e^A : \mathfrak{g} \to G$ is exactly the exponential map of $G$.

The above statement can be used to check that the Lie algebras of the classical Lie groups were correctly given before.
Steps toward a description of Lie groups

- Classifying Lie groups is almost the same as classifying Lie algebras.
- **Levi-Mal’cev Theorem**: Every finite dimensional Lie algebra \( \mathfrak{g} \) is of the form \( \mathfrak{g} = \mathfrak{r} \times \mathfrak{s} \), where \( \mathfrak{r} \) is the solvable radical of \( \mathfrak{g} \) and \( \mathfrak{s} \) is a semisimple Lie subalgebra called a **Levi subalgebra**.
- The description of all solvable Lie algebras is hopeless, so we do not care about it.
- A semisimple Lie algebra is a direct sum of simple Lie algebras.
- To classify real simple Lie algebras, one uses the classification of simple Lie algebras over the complex numbers.
Connection between real and complex Lie algebras

**Complexification**

Given a real Lie algebra \( \mathfrak{g} \) its **complexification** is \( \mathfrak{g}(\mathbb{C}) = \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C} \).

**Realification**

Given a complex Lie algebra \( \mathfrak{g} \) its **realification** \( \mathfrak{g}_\mathbb{R} \) can be obtained by simply “forgetting” the multiplication with non-real scalars.

- Both complexification and realification preserve Levi-Mal’cev decompositions. In particular, \( \mathfrak{g} \) is semisimple \( \iff \mathfrak{g}(\mathbb{C}) \) is semisimple.
- If \( \mathfrak{g} \) is a complex simple Lie algebra, then its realification \( \mathfrak{g}_\mathbb{R} \) is a real simple Lie algebra. Using the classification theory we get a series of simple Lie algebras \( (A_l)_\mathbb{R}, \ldots, (G_2)_\mathbb{R} \).
- All the other simple real Lie algebras can be found by finding the so-called **real forms** of the complex simple Lie algebras.
real form

A real form of a simple complex Lie algebra $\mathfrak{g}$ is a real subalgebra $\mathfrak{h}$ of $\mathfrak{g}_\mathbb{R}$ such that $\mathfrak{h} \otimes \mathbb{C} \cong \mathfrak{g}$.

- Every real form of a simple complex Lie algebra is a simple real Lie algebra.
- A simple complex Lie algebra has at least two real forms (there can be more); the two “extreme cases” are the compact and the split real forms.

the signature of a simple real algebra

If $\mathfrak{g}$ is a real simple Lie algebra, its Killing form is a non-degenerate symmetric bilinear function. So, with respect to a suitable basis, it is represented by a diagonal matrix containing only $+1$ and $-1$ in the main diagonal. If the number of $+1$-s and $-1$-s in this matrix are $p$ and $q$, then we say that the signature of $\mathfrak{g}$ is $(p, q)$. 
Compact and split Lie forms

The **compact real form** of a simple complex Lie algebra is a real form such that its Killing form is negative definite, that is, it signature is of the form \((0, n)\).

The **split real form** of a simple complex Lie algebra is the real form with signature \((p, q)\) having the property that \(p\) is as large as possible among the signatures of the real forms of the simple complex Lie algebra. (That is, a split real form is the farthest from being compact).

- The split real form can be given by choosing a **Chevalley basis** in a simple complex Lie algebra and taking the real subspace generated by it.
- As an example, or \(A_{l-1} = \mathfrak{sl}_l(\mathbb{C})\), its split real form is \(\mathfrak{sl}_l(\mathbb{R})\), while its compact real form is \(\mathfrak{su}_n\). For \(l = 2\), these are all the real forms of \(A_{l-1}\), but for larger \(l\) there are also other real forms.
Conjugation with respect to a real form

Let \( \mathfrak{g} \) be a complex Lie algebra with real form \( \mathfrak{h} \). Then \( \mathfrak{g} = \mathfrak{h} \oplus (i\mathfrak{h}) \), i.e. every element of \( \mathfrak{g} \) has a unique form \( x + iy \) with \( x, y \in \mathfrak{h} \). Then \( \sigma : \mathfrak{g} \to \mathfrak{g}, \sigma(x + iy) = x - iy \) \((x, y \in \mathfrak{h})\) is a well-defined function called the conjugation on \( \mathfrak{g} \) with respect to \( \mathfrak{h} \).

- \( \sigma \) is an involutory (i.e. \( \sigma \circ \sigma = \text{id}_\mathfrak{g} \)) antilinear (i.e. \( \sigma(z) = \overline{\lambda \sigma(z)} \) for each \( \lambda \in \mathbb{C}, z \in \mathfrak{g} \)) Lie algebra automorphism of \( \mathfrak{g} \).
- \( \mathfrak{h} = \mathfrak{g}^\sigma = \{ x \in \mathfrak{g} \mid \sigma(x) = x \} \).
- If \( \varphi : \mathfrak{g} \to \mathfrak{g} \) is any involutory antilinear Lie algebra automorphism (conjugation) of \( \mathfrak{g} \), then \( \mathfrak{g}^\varphi = \{ x \in \mathfrak{g} \mid \varphi(x) = x \} \) is a real form of \( \mathfrak{g} \).
- For two conjugation \( \sigma, \varphi : \mathfrak{g} \to \mathfrak{g} \) we have \( \mathfrak{g}^\sigma \simeq \mathfrak{g}^\varphi \) if and only if there exists a \( \tau \in \text{Aut} \mathfrak{g} \) with \( \tau \circ \sigma \circ \tau^{-1} = \varphi \).
Consequence: In order to classify all simple real Lie algebras (and through it, simple Lie groups), one needs to classify the equivalence classes of involutory antilinear Lie algebra automorphisms (conjugations) of the simple complex Lie algebras;

It turns out, that for each simple complex Lie algebra $A_l, \ldots, G_2$ there are only finitely many equivalence classes of conjugations, which can be described by Satake-diagrams.

The Satake diagram of a real form is obtained from the Dynkin diagram of the associated complex simple Lie algebra with some vertices colored to black and some other vertices in pairs connected by arrows.
The Classification Theorem Of Finite Simple Groups

- CFSG is the Theorem having the longest proof in the history of mathematics;
- The first “proof” has been reported in 1981, cumulating the works of hundreds of mathematicians, and it was roughly 15000 pages long.
- It was several holes in the proof. By my knowledge, the last significant correction was published in 2004.
- Now, it is commonly believed to be true.
- There is a “third generation proof” in progress, with approximated length of 5000 pages.
The list of finite simple groups

CFSG

Any finite simple group is one of the following

- A cyclic group of prime order;
- The alternating group $A_n$ of degree $n \geq 5$;
- A simple group of Lie type containing 16 infinite sequences:
  
  **The Chevalley groups:** $A_l(q), B_l(q), C_l(q), D_l(q), E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$;
  
  **The Steinberg groups:** $^2A_l(q^2), ^2D_l(q^2), ^2E_6(q^2), ^3D_4(q^3)$;
  
  **The Suzuki-Ree groups:** $^2B(2^{2k+1}), ^2F_4(2^{2k+1}), ^2G_2(3^{2k+1})$;

- One of the 26 sporadic groups;
An outline of finite fields

Finite fields

Let $K$ be a finite field.

- There is a prime number $p$ such that $a + \ldots + a = 0$ for each $a \in K$. This $p$ is called the characteristic of $K$ and is denoted by $\text{char } K$.
- If $\text{char } K = p$ then $|K| = q = p^n$ for some $n$.
- For each prime power $q$, there exists a field of $q$ elements and it is unique (up to isomorphism). The $q$-element field is denoted by $\mathbb{F}_q$.
- The automorphism group of $\mathbb{F}_{p^n}$ is

$$\text{Aut } \mathbb{F}_q = \{\varphi_k : a \rightarrow a^{p^k} \mid k = 0, 1, \ldots, n - 1\} \cong C_n.$$
Chevalley algebras over finite fields

- Let $\mathfrak{s}$ be a simple Lie algebra over $\mathbb{C}$, i.e. $\mathfrak{s} \in \{A_l, B_l, \ldots, G_2\}$.
- Starting from a Cartan decomposition of $\mathfrak{s}$, we choose a Chevalley basis $B_{Ch} = \{h_r, r \in \Pi; e_s, s \in \Phi\}$. That is, the Lie bracket of every two elements of $B_{Ch}$ is an integer multiple of some other element of $B_{Ch}$.
- The set of all linear combinations of $B_{Ch}$ with integer coefficients is a Lie algebra over $\mathbb{Z}$ denoted by $\mathfrak{s}(\mathbb{Z})$.
- By taking $\mathfrak{s}(\mathbb{Z})$ “modulo $p$” we get a finite Lie algebra $\mathfrak{s}(\mathbb{F}_p)$.
- By extending scalars, i.e. taking the tensor product $\mathfrak{s}(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ we get the finite Lie algebra $\mathfrak{s}(\mathbb{F}_q)$.
- Even if $\mathfrak{s}$ is simple, $\mathfrak{s}(\mathbb{F}_q)$ will be not allways simple.
- Although one can choose a Chevalley basis in many different ways, the resulting Lie algebra $\mathfrak{s}(\mathbb{Z})$ is unique up to isomorphism. So, $\mathfrak{s}(\mathbb{F}_q)$ is also uniquely defined.
Constructing Chevalley groups

- For a Chevalley algebra $\mathfrak{s}(K)$ over the field $K$, the associated Chevalley group $S(K)$ is a subgroup in the automorphism group of $\mathfrak{s}(K)$.

- A derivation of a Lie algebra $\mathfrak{l}$ is a linear function $\delta : \mathfrak{l} \rightarrow \mathfrak{l}$ satisfying $\delta([f, g]) = [\delta(f), g] + [f, \delta g]$ for each $f, g \in \mathfrak{l}$.

- If $\delta$ is a nilpotent (i.e. $\delta^k = 0$ for some $k \in \mathbb{N}$) derivation of $\mathfrak{l}$, and $\text{char } K = 0$, then $\exp(\delta) := \sum_{k=0}^{\infty} \frac{\delta^k}{k!}$ is meaningful, and $\exp(\delta) : \mathfrak{l} \rightarrow \mathfrak{l}$ is Lie algebra automorphism.

- For any $e_r$ (with $r \in \Phi$) and $\zeta \in K$, the map $\zeta \text{ ad } e_r : x \mapsto \zeta[e_r, x]$ is a nilpotent derivation of $\mathfrak{l}$, so $x_r(\zeta) := \exp(\zeta \text{ ad } e_s)$ is an automorphism of $\mathfrak{l}$.

- The Chevalley group related to $\mathfrak{s}(K)$ is $S(K) = \langle x_r(\zeta) \mid r \in \Phi, \zeta \in K \rangle$. 
The above construction does not work in general if \( \text{char } K > 0 \). Still, there is a way to define \( S(K) \) for any \( K \).

One can show that in the char \( K = 0 \) case the following hold for every \( \zeta \in K \) and \( r, s \in \Phi \) with \( r, s \) linearly independent.

1. \( x_r(\zeta)(e_r) = e_r \);
2. \( x_r(\zeta)(e_{-r}) = e_{-r} + \zeta h_r - \zeta^2 e_r \);
3. \( x_r(\zeta)h_r = h_r - 2\zeta e_r \);
4. \( x_r(\zeta)h_s = h_s - A_{sr}\zeta e_r \);
5. \( x_r(\zeta)e_s = \sum_{i=0}^{q} \pm \binom{p^i}{i} \zeta^i e_{ir+s} \).

In these equalities, each coefficient is an integer multiple of a power of \( \zeta \), so for any field \( K \) and \( t \in K \) one can define \( x_r(t) \) by substituting \( t \) in place of \( \zeta \) in the above equalities.

As in the char \( K = 0 \) case, the Chevalley group \( S(q) \) related to \( s(q) \) is defined as \( S(K) = \langle x_r(t) \mid r \in \Phi, t \in \mathbb{F}_q \rangle \).

In that way we get the finite Chevalley groups \( A_1(q), \ldots, G_2(q) \).
The twisted groups

- Let $s(q)$ be a finite Chevalley algebra such that its Dynkin graph has a non-trivial symmetry $\pi$ of order 2 or 3.
- Let us assume that there is an automorphism $g \in \text{Aut } s(q)$ such that the restriction of $g$ to a system of fundamental roots defines $\pi$.
- If the Dynkin graph of $s(q)$ does not contain multiple edges, there is always such a $g \in \text{Aut } s(q)$; If the Dynkin graph contains double (resp. triple) edges, then such a $g$ only exists if $\text{char } \mathbb{F}_q = 2$ or (resp. $\text{char } \mathbb{F}_q = 3$).
- Let $f_0 \in \text{Aut } \mathbb{F}_q$ such that its extension $f$ to $s(q)$ has the property that $p(g) = o(gf)$. (The existence of such an $f$ gives us further restriction on $q$).
If both $g$ and $f$ exists with the above properties, then associated actions can also be defined on the Chevalley group $S(q)$, denoted by $\bar{g}$ and $\bar{f}$. Let $\sigma = \bar{g}\bar{f} \in \text{Aut } S(q)$. Then the twisted group of Lie type is defined as $S(q)^\sigma = \{x \in S(q) \mid \sigma(x) = x\}$.

In that way, if the Dynkin graph of $s(q)$ does not contain multiple edges we get the Steinberg groups: $^2A_l(q^2)$, $^2D_l(q^2)$, $^2E_6(q^2)$, $^3D_4(q^3)$, while if it contains multiple edges we get the Suzuki-Ree groups $^2B_2(2^{2k+1})$, $^2F_4(2^{2k+1})$, $^2G_2(3^{2k+1})$. 