A Decomposition Theorem of Plesken Lie Algebras over Finite Fields

Mona Merling

Department of Mathematics
Bard College

May 2009
A Decomposition Theorem of Plesken Lie Algebras over Finite Fields

**Definition of Lie Algebra**

Let $k$ be a field. A **Lie algebra** $L$ over $k$ is a $k$-vector space $L$ together with a bilinear map

\[ [ , ] : L \times L \rightarrow L \]

(called the **bracket** or **commutator**) satisfying:

1. $[x, x] = 0$ for all $x$ in $L$;
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z$ in $L$.

(Jacobi identity)

Lie algebras are **neither associative nor commutative**
Definition of Lie Algebra

Let $k$ be a field. A **Lie algebra** $L$ over $k$ is a $k$-vector space $L$ together with a bilinear map

$$[\ ,\ ] : L \times L \to L$$

(called the **bracket** or **commutator**) satisfying:

1. $[x, x] = 0$ for all $x$ in $L$;
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z$ in $L$.
   (Jacobi identity)

Lie algebras are neither associative nor commutative.
Definition of Lie Algebra

Let $k$ be a field. A **Lie algebra** $L$ over $k$ is a $k$-vector space $L$ together with a bilinear map

$$ [ , ] : L \times L \rightarrow L $$

(called the **bracket** or **commutator**) satisfying:

1. $[x, x] = 0$ for all $x$ in $L$;
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z$ in $L$. (Jacobi identity)

Lie algebras are **neither associative nor commutative**.
Let $k$ be a field. A **Lie algebra** $L$ over $k$ is a $k$-vector space $L$ together with a bilinear map

$$[\ , \ ] : L \times L \to L$$

(called the **bracket** or **commutator**) satisfying:

1. $[x, x] = 0$ for all $x$ in $L$;
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z$ in $L$. (Jacobi identity)

Lie algebras are **neither associative nor commutative**
Some Examples

Example

$\mathbb{R}^3$ with the Lie bracket given by the cross product of vectors

$$[x, y] = x \times y,$$
for all $x, y \in \mathbb{R}^3$.

Example

Let $\mathfrak{gl}(n, k)$ be the vector space of all $n \times n$ matrices over $k$ with the Lie bracket defined by

$$[x, y] = xy - yx,$$
where the multiplication on the right is the usual product of matrices.
Some Examples

Example

$\mathbb{R}^3$ with the Lie bracket given by the cross product of vectors

$$[x, y] = x \times y, \text{ for all } x, y \in \mathbb{R}^3.$$  

Example

Let $\mathfrak{gl}(n, k)$ be the vector space of all $n \times n$ matrices over $k$ with the Lie bracket defined by

$$[x, y] = xy - yx,$$

where the multiplication on the right is the usual product of matrices.
Classification of Simple Lie Algebras

- A Lie algebra is **simple** if it has no non-trivial ideals and is not abelian.
- A Lie algebra is **semisimple** if it does not contain any non-zero abelian ideals.
- In particular, a simple Lie algebra is semisimple.
- Conversely, it can be proven that any semisimple Lie algebra is the direct sum of its minimal ideals, which are canonically determined simple Lie algebras.

Classification

With five exceptions, every finite-dimensional simple Lie algebra over \( \mathbb{C} \) is isomorphic to one of the **classical Lie algebras**:

\[ \mathfrak{sl}(n, \mathbb{C}), \mathfrak{o}(n, \mathbb{C}), \mathfrak{sp}(2n, \mathbb{C}). \]
Classification of Simple Lie Algebras

- A Lie algebra is **simple** if it has no non-trivial ideals and is not abelian.
- A Lie algebra is **semisimple** if it does not contain any non-zero abelian ideals.
- In particular, a simple Lie algebra is semisimple.
- Conversely, it can be proven that any semisimple Lie algebra is the direct sum of its minimal ideals, which are canonically determined simple Lie algebras.

Classification

With five exceptions, every finite-dimensional simple Lie algebra over $\mathbb{C}$ is isomorphic to one of the **classical Lie algebras**:

$\mathfrak{sl}(n, \mathbb{C}), \mathfrak{o}(n, \mathbb{C}), \mathfrak{sp}(2n, \mathbb{C})$. 
A Lie algebra is **simple** if it has no non-trivial ideals and is not abelian.

A Lie algebra is **semisimple** if it does not contain any non-zero abelian ideals.

In particular, a simple Lie algebra is semisimple.

Conversely, it can be proven that any semisimple Lie algebra is the direct sum of its minimal ideals, which are canonically determined simple Lie algebras.

**Classification**

With five exceptions, every finite-dimensional simple Lie algebra over \( \mathbb{C} \) is isomorphic to one of the **classical Lie algebras**:

\[ \mathfrak{sl}(n, \mathbb{C}), \mathfrak{o}(n, \mathbb{C}), \mathfrak{sp}(2n, \mathbb{C}). \]
Classification of Simple Lie Algebras

- A Lie algebra is **simple** if it has no non-trivial ideals and is not abelian.
- A Lie algebra is **semisimple** if it does not contain any non-zero abelian ideals.
- In particular, a simple Lie algebra is semisimple.
- Conversely, it can be proven that any semisimple Lie algebra is the direct sum of its minimal ideals, which are canonically determined simple Lie algebras.

Classification

With five exceptions, every finite-dimensional simple Lie algebra over $\mathbb{C}$ is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbb{C}), \mathfrak{o}(n, \mathbb{C}), \mathfrak{sp}(2n, \mathbb{C}).$$
A Lie algebra is **simple** if it has no non-trivial ideals and is not abelian.

A Lie algebra is **semisimple** if it does not contain any non-zero abelian ideals.

In particular, a simple Lie algebra is semisimple.

Conversely, it can be proven that any semisimple Lie algebra is the direct sum of its minimal ideals, which are canonically determined simple Lie algebras.

**Classification**

With five exceptions, every finite-dimensional simple Lie algebra over $\mathbb{C}$ is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbb{C}), \mathfrak{o}(n, \mathbb{C}), \mathfrak{sp}(2n, \mathbb{C}).$$
The Group Algebra

Definition

Let $G$ be a group and $k$ a field. The group algebra $k[G]$ is the set of all linear combinations of finitely many elements of $G$ with coefficients in $k$.

The group algebra is a Lie algebra.
The Group Algebra

Definition

Let $G$ be a group and $k$ a field. The **group algebra** $k[G]$ is the set of all linear combinations of finitely many elements of $G$ with coefficients in $k$.

The group algebra is a Lie algebra.
A Decomposition Theorem of Plesken Lie Algebras over Finite Fields

Structure Theorem

Let \( \mathcal{L}(G) \) be the subspace of \( \mathbb{C}[G] \) that is the linear span of the elements \( \hat{g} = g - g^{-1} \). Then \( \mathcal{L}(G) \) is a Lie-subalgebra of \( \mathbb{C}[G] \), defined by Plesken.

What Lie algebra is it?

Theorem

The Lie algebra \( \mathcal{L}(G) \) admits the decomposition

\[
\mathcal{L}(G) = \bigoplus_{\chi \in \mathcal{R}} \mathfrak{o}(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{Sp}} \mathfrak{sp}(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{C}} \mathfrak{gl}(\chi(1))
\]

where \( \mathcal{R}, \mathcal{Sp}, \) and \( \mathcal{C} \) are the sets of irreducible characters of real, symplectic, and complex types, respectively, and where the prime signifies that there is just one summand \( \mathfrak{gl}(\chi(1)) \) for each pair \( \{\chi, \bar{\chi}\} \) from \( \mathcal{C} \).
Structure Theorem

Let \( L(G) \) be the subspace of \( \mathbb{C}[G] \) that is the linear span of the elements \( \hat{g} = g - g^{-1} \). Then \( L(G) \) is a Lie-subalgebra of \( \mathbb{C}[G] \), defined by Plesken.

What Lie algebra is it?

Theorem

The Lie algebra \( L(G) \) admits the decomposition

\[
L(G) = \bigoplus_{\chi \in \mathcal{R}} o(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{Sp}} sp(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{C}} 'g\mathfrak{l}(\chi(1))
\]

where \( \mathcal{R} \), \( \mathcal{Sp} \) and \( \mathcal{C} \) are the sets of irreducible characters of real, symplectic, and complex types, respectively, and where the prime signifies that there is just one summand \( g\mathfrak{l}(\chi(1)) \) for each pair \( \{\chi, \bar{\chi}\} \) from \( \mathcal{C} \).
Structure Theorem

Let $\mathcal{L}(G)$ be the subspace of $\mathbb{C}[G]$ that is the linear span of the elements $\hat{g} = g - g^{-1}$. Then $\mathcal{L}(G)$ is a Lie-subalgebra of $\mathbb{C}[G]$, defined by Plesken.

What Lie algebra is it?

Theorem

The Lie algebra $\mathcal{L}(G)$ admits the decomposition

$$\mathcal{L}(G) = \bigoplus_{\chi \in \mathcal{R}} \mathfrak{o}(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{Sp}} \mathfrak{sp}(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{C}} \mathfrak{gl}(\chi(1))$$

where $\mathcal{R}$, $\mathcal{Sp}$ and $\mathcal{C}$ are the sets of irreducible characters of real, symplectic, and complex types, respectively, and where the prime signifies that there is just one summand $\mathfrak{gl}(\chi(1))$ for each pair $\{\chi, \bar{\chi}\}$ from $\mathcal{C}$. 
Structure Theorem

Let $\mathcal{L}(G)$ be the subspace of $\mathbb{C}[G]$ that is the linear span of the elements $\hat{g} = g - g^{-1}$. Then $\mathcal{L}(G)$ is a Lie-subalgebra of $\mathbb{C}[G]$, defined by Plesken.

What Lie algebra is it?

Theorem

The Lie algebra $\mathcal{L}(G)$ admits the decomposition

$$\mathcal{L}(G) = \bigoplus_{\chi \in \mathcal{R}} o(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{Sp}} sp(\chi(1)) \oplus \bigoplus_{\chi \in \mathcal{C}} 'gl(\chi(1))$$

where $\mathcal{R}$, $\mathcal{Sp}$, and $\mathcal{C}$ are the sets of irreducible characters of real, symplectic, and complex types, respectively, and where the prime signifies that there is just one summand $'gl(\chi(1))$ for each pair $\{\chi, \bar{\chi}\}$ from $\mathcal{C}$. 
Example

The character table for $A_5$ is:

<table>
<thead>
<tr>
<th>Conjugacy Class</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>$\frac{\sqrt{5}+1}{2}$</td>
<td>$\frac{\sqrt{5}+1}{2}$</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>$\frac{\sqrt{5}+1}{2}$</td>
<td>$\frac{\sqrt{5}-1}{2}$</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>5</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The group $A_5$ has 5 characters, all of real type, of degrees 1,3,3,4,5. So, $\mathcal{L}(A_5)$ decomposes in the following way:

$$\mathcal{L}(A_5) = \mathfrak{o}(1, \mathbb{C}) \oplus \mathfrak{o}(3, \mathbb{C}) \oplus \mathfrak{o}(3, \mathbb{C}) \oplus \mathfrak{o}(4, \mathbb{C}) \oplus \mathfrak{o}(5, \mathbb{C}).$$
My project

\[ \mathcal{L}(G) \text{ is a Lie-subalgebra of } k[G] \text{ for any field } k. \]

Question

Can we find a similar structure theorem if we take \( k \) to be a finite field instead of \( \mathbb{C} \)?

- Classification of Lie algebras over finite fields is MUCH more complicated.
- Representations of groups over finite fields is also much more complex than over an algebraically closed field.
My project

\[ \mathfrak{L}(G) \] is a Lie-subalgebra of \( k[G] \) for any field \( k \).

**Question**

Can we find a similar structure theorem if we take \( k \) to be a finite field instead of \( \mathbb{C} \)?

- Classification of Lie algebras over finite fields is MUCH more complicated.
- Representations of groups over finite fields is also much more complex than over an algebraically closed field.
My project

\[ \mathfrak{L}(G) \] is a Lie-subalgebra of \( k[G] \) for any field \( k \).

**Question**

Can we find a similar structure theorem if we take \( k \) to be a finite field instead of \( \mathbb{C} \)?

- Classification of Lie algebras over finite fields is MUCH more complicated.
- Representations of groups over finite fields is also much more complex than over an algebraically closed field.
My project

\( \mathcal{L}(G) \) is a Lie-subalgebra of \( k[G] \) for any field \( k \).

**Question**

Can we find a similar structure theorem if we take \( k \) to be a finite field instead of \( \mathbb{C} \)?

- Classification of Lie algebras over finite fields is MUCH more complicated.
- Representations of groups over finite fields is also much more complex than over an algebraically closed field.
Method

We define the reduction mod $p$ of the Plesken Lie algebra in two ways and clash the results against each other, the result being a fascinating theorem.

- $\mathfrak{L}(G)_{\mathbb{F}_p}$ is the Plesken Lie algebra as a subalgebra of $\mathbb{F}_p[G]$.
- $\mathfrak{L}(G) \otimes_{\mathbb{Z}} \mathbb{F}_p = (\mathfrak{L}(G))_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$, the tensor product of the $\mathbb{Z}$-span of the Chevalley basis of the complex Lie algebra $\mathfrak{L}(G)$ with $\mathbb{F}_p$. 
Method

We define the reduction mod $p$ of the Plesken Lie algebra in two ways and clash the results against each other, the result being a fascinating theorem.

- $\mathcal{L}(G)_{\mathbb{F}_p}$ is the Plesken Lie algebra as a subalgebra of $\mathbb{F}_p[G]$

- $\mathcal{L}(G) \otimes_{\mathbb{F}_p} = (\mathcal{L}(G))(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{F}_p$, the tensor product of the $\mathbb{Z}$-span of the Chevalley basis of the complex Lie algebra $\mathcal{L}(G)$ with $\mathbb{F}_p$. 
A Decomposition Theorem of Plesken Lie Algebras over Finite Fields

**Important Result**

**Theorem**

*If the Lie algebra* $L$ *is a direct sum of simple ideals* $L = L_1 \oplus \cdots \oplus L_n$, *then*

$$L \otimes F_p = L_1 \otimes F_p \oplus \cdots \oplus L_n \otimes F_p.$$  

**Example**

$$\mathcal{L}(A_5) \otimes F_p = \mathfrak{o}(1, F_p) \oplus \mathfrak{o}(3, F_p) \oplus \mathfrak{o}(3, F_p) \oplus \mathfrak{o}(4, F_p) \oplus \mathfrak{o}(5, F_p).$$
Important Result

Theorem

If the Lie algebra $L$ is a direct sum of simple ideals $L = L_1 \oplus \cdots \oplus L_n$, then

$$L \otimes \mathbb{F}_p = L_1 \otimes \mathbb{F}_p \oplus \cdots \oplus L_n \otimes \mathbb{F}_p.$$ 

Example

$\mathcal{L}(A_5) \otimes \mathbb{F}_p = \mathfrak{o}(1, \mathbb{F}_p) \oplus \mathfrak{o}(3, \mathbb{F}_p) \oplus \mathfrak{o}(3, \mathbb{F}_p) \oplus \mathfrak{o}(4, \mathbb{F}_p) \oplus \mathfrak{o}(5, \mathbb{F}_p).$
Main Result

Theorem

If \( p \neq 2 \) and \( p \nmid \#G \) the Lie algebras \( \mathcal{L}(G) \otimes_{\mathbb{F}_p} \) and \( \mathcal{L}(G)_{\mathbb{F}_p} \) are the same if

- the splitting field of \( \mathbb{C}[G] \) is \( \mathbb{Q} \), or
- the splitting field of \( \mathbb{C}[G] \) is \( K \), an extension of \( \mathbb{Q} \) and \( p \) splits completely in the ring of integers of \( K \).

The splitting field of \( \mathbb{C}[G] \) is the smallest field over which the complex irreducible representations of \( G \) can be realized, and its ring of integers is the collection of all the algebraic integers in the field.
Main Result

Theorem

If $p \neq 2$ and $p \nmid \# G$ the Lie algebras $\mathcal{L}(G) \otimes_{\mathbb{F}_p} \mathbb{F}_p$ and $\mathcal{L}(G)_{\mathbb{F}_p}$ are the same if

- the splitting field of $\mathbb{C}[G]$ is $\mathbb{Q}$, or
- the splitting field of $\mathbb{C}[G]$ is $K$, an extension of $\mathbb{Q}$ and $p$ splits completely in the ring of integers of $K$.

The splitting field of $\mathbb{C}[G]$ is the smallest field over which the complex irreducible representations of $G$ can be realized, and its ring of integers is the collection of all the algebraic integers in the field.
Example

The splitting field of $C[A_5]$ is $Q(\sqrt{5})$ whose ring of integers is $Z[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $O_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{F_{13}}$, and $\mathcal{L}(A_5) \otimes F_{13}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $Z[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5) \otimes F_{11}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{F_{13}}$, and $\mathcal{L}(A_5) \otimes_{F_{13}}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5) \otimes_{F_{11}}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal (13) does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{\mathbb{F}_{13}}$, and $\mathcal{L}(A_5) \otimes_{\mathbb{F}_{13}}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{\mathbb{F}_{11}}$ is the same as $\mathcal{L}(A_5) \otimes_{\mathbb{F}_{11}}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $\rho = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{F_{13}}$ and $\mathcal{L}(A_5) \otimes_{F_{13}}$ are not the same.

Example

Let $\rho = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5) \otimes_{F_{11}}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $L(A_5)_{F_{13}}$, and $L(A_5) \otimes_{F_{13}}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $L(A_5)_{F_{11}}$ is the same as $L(A_5) \otimes_{F_{11}}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{F_{13}}$ and $\mathcal{L}(A_5) \otimes F_{13}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5) \otimes F_{11}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{F_{13}}$, and $\mathcal{L}(A_5) \otimes_{F_{13}}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5) \otimes_{F_{11}}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_{F_{13}}$, and $\mathcal{L}(A_5)^{\otimes F_{13}}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5)^{\otimes F_{11}}$. 
Example

The splitting field of $\mathbb{C}[A_5]$ is $\mathbb{Q}(\sqrt{5})$ whose ring of integers is $\mathbb{Z}[\sqrt{5}]$.

Example (Let $p = 13$.)

- $x^2 - 5$ is irreducible modulo 13,
- the ideal $(13)$ does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal.
- $\mathcal{L}(A_5)_F_{13}$, and $\mathcal{L}(A_5) \otimes F_{13}$ are not the same.

Example

Let $p = 11$.

- $x^2 - 5 \equiv (x + 4)(x + 7) \pmod{11}$,
- we get the ideal factorization $(11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7)$.
- the prime 11 splits completely in $\mathbb{Z}[\sqrt{5}]$.
- $\mathcal{L}(A_5)_{F_{11}}$ is the same as $\mathcal{L}(A_5) \otimes F_{11}$. 
Example

The splitting field of \( \mathbb{C}[A_5] \) is \( \mathbb{Q}(\sqrt{5}) \) whose ring of integers is \( \mathbb{Z}[\sqrt{5}] \).

Example (Let \( p = 13 \).)

- \( x^2 - 5 \) is irreducible modulo 13,
- the ideal \( (13) \) does not factor in \( \mathcal{O}_K \), i.e., it is a prime ideal.
- \( L(A_5)_{F_{13}} \) and \( L(A_5) \otimes F_{13} \) are not the same.

Example

Let \( p = 11 \).

- \( x^2 - 5 \equiv (x + 4)(x + 7) \) (mod 11),
- we get the ideal factorization \( (11) = (5, \sqrt{5} + 4)(5, \sqrt{5} + 7) \).
- the prime 11 splits completely in \( \mathbb{Z}[\sqrt{5}] \).
- \( L(A_5)_{F_{11}} \) is the same as \( L(A_5) \otimes F_{11} \).
Why Most People Do Not Associate With Lie Algebras

If algebras were people...
I'm sorry, I just can't associate with you.
LIE!

2007
© COURTNEY GIBBONS