A Decomposition Theorem of Plesken Lie Algebras over Finite Fields

Mona Merling

Department of Mathematics
Bard College

May 2009

Definition of Lie Algebra

Definition

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

Definition

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

Definition

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

Definition

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

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

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

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

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

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

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 **C** is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbf{C}), \mathfrak{o}(n, \mathbf{C}), \mathfrak{sp}(2n, \mathbf{C}).$$

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 $\mathbf{C}$ is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbf{C}), \mathfrak{o}(n, \mathbf{C}), \mathfrak{sp}(2n, \mathbf{C}).$$

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 $\mathbf{C}$ is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbf{C}), \mathfrak{o}(n, \mathbf{C}), \mathfrak{sp}(2n, \mathbf{C}).$$

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 **C** is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbf{C}), \mathfrak{o}(n, \mathbf{C}), \mathfrak{sp}(2n, \mathbf{C}).$$

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 **C** is isomorphic to one of the **classical Lie algebras**:

$$\mathfrak{sl}(n, \mathbf{C}), \mathfrak{o}(n, \mathbf{C}), \mathfrak{sp}(2n, \mathbf{C}).$$

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.

Structure Theorem

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

What Lie algebra is it?

Theorem

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

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

where $\mathfrak{R}$, $\mathfrak{Sp}$ and $\mathfrak{C}$ 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 $\mathfrak{C}$.

Structure Theorem

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

What Lie algebra is it?

Theorem

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

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

where $\mathfrak{R}$, $\mathfrak{Sp}$ and $\mathfrak{C}$ 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 $\mathfrak{C}$.

Structure Theorem

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

What Lie algebra is it?

Theorem

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

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

where $\mathfrak{R}, \mathfrak{Sp}$ and $\mathfrak{C}$ 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 $\mathfrak{C}$.

Structure Theorem

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

What Lie algebra is it?

Theorem

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

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

where $\mathfrak{R}, \mathfrak{Sp}$ and $\mathfrak{C}$ 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 $\mathfrak{C}$.

Example

Example

The character table for A_5 is:

Conjugacy Class	1	2	3	4	5
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{\sqrt{5}-1}{2}$	$\frac{\sqrt{5}+1}{2}$
χ_3	3	-1	0	$\frac{\sqrt{5}+1}{2}$	$\frac{\sqrt{5}-1}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

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

$$\mathfrak{L}(A_5) = \mathfrak{o}(1, \mathbf{C}) \oplus \mathfrak{o}(3, \mathbf{C}) \oplus \mathfrak{o}(3, \mathbf{C}) \oplus \mathfrak{o}(4, \mathbf{C}) \oplus \mathfrak{o}(5, \mathbf{C}).$$

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 $\mathbf{C}$?

- 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 $\mathbf{C}$?

- 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 $\mathbf{C}$?

- 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 $\mathbf{C}$?

- 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.

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

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.

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

Important Result

Theorem

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

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

Example

$$\mathfrak{L}(A_5)^{\otimes \mathbf{F}_p} = \mathfrak{o}(1, \mathbf{F}_p) \oplus \mathfrak{o}(3, \mathbf{F}_p) \oplus \mathfrak{o}(3, \mathbf{F}_p) \oplus \mathfrak{o}(4, \mathbf{F}_p) \oplus \mathfrak{o}(5, \mathbf{F}_p).$$

Important Result

Theorem

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

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

Example

$$\mathfrak{L}(A_5)^{\otimes \mathbf{F}_p} = \mathfrak{o}(1, \mathbf{F}_p) \oplus \mathfrak{o}(3, \mathbf{F}_p) \oplus \mathfrak{o}(3, \mathbf{F}_p) \oplus \mathfrak{o}(4, \mathbf{F}_p) \oplus \mathfrak{o}(5, \mathbf{F}_p).$$

Main Result

Theorem

If $p \neq 2$ and $p \nmid \#G$ the Lie algebras $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(G)_{\mathbf{F}_p}$ are the same if

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

The spliting field of $\mathbf{C}[G]$ 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 algegraic integers in the field.

Main Result

Theorem

If $p \neq 2$ and $p \nmid \#G$ the Lie algebras $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(G)_{\mathbf{F}_p}$ are the same if

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

The spliting field of $\mathbf{C}[G]$ 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 algegraic integers in the field.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Example

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

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.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ 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 $\mathbf{Z}[\sqrt{5}]$.
- $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

Why Most People Do Not Associate With Lie Algebras