Galois theory and matrix groups

Math 3560 Groups and Symmetry, Fall 2014

Raul Gomez

Cornell University

Galois theory

Figure : Évariste Galois

Évariste Galois

Biography highlights

1828 Failed admission to École Polytechnique.

1829 Father commits suicide.

1829 Failed admission to École Polytechnique again.

1830 Joins the artillery of the national guard.

1831 Gets arrested for threatening King Louis-Philipe.

1831 Gets arrested again for wearing the national guard uniform during the Bastille day.

Évariste Galois

Biography highlights

1832 Poisson rejects his paper "On the condition that an equation be soluble by radicals" for being poorly elaborated, asks for an expanded version.

1832 Gets involved in a duel. Legend says he spent his last night polishing his paper on Galois theory. This note was found in his paper: "There is something to complete in this demonstration. I do not have the time..."

1832 Gets shot during his duel, and dies because of his wounds. His funeral becomes the focus of a republican rally and the subsequent riots last for several days.

1846 Liouville publishes his paper in 1846.

Irreducible polynomials

Definition

Let F be a subfield of $\mathbb{C}$, and let $F[x]$ be the space of polynomials with coefficients in F. We say that a polynomial $p(x) \in F[x]$ is irreducible if for any decomposition

$$p(x) = q(x)r(x), \qquad q(x),\ r(x) \in F[x],$$

we have that either $q(x)$ or $r(x)$ is a constant.

Example

The polynomials $p(x) = x^2 + 1$ and $r(x) = x^3 + 2$ are irreducible over $\mathbb{Q}$. (But not over $\mathbb{C}$.) However the polynomial

$$r(x) = x^3 + 1 = (x+1)(x^2 - x + 1)$$

is not irreducible.

Proposition

Let F be a subfield of $\mathbb{C}$, and let $p(x) \in F[x]$ be an irreducible polynomial. Then all the roots of $p(x)$ (in $\mathbb{C}$) are different.

Splitting fields

Lemma

Let $\{F_i\}_{i \in I}$ be a collection of subfields of $\mathbb{C}$. Then $F = \cap_{i \in I} F_i$ is a field.

Definition

Let F be a subfield of $\mathbb{C}$, and let $p(x) \in F[x]$ be an irreducible polynomial. Let $R_{p(x)} = \{\alpha_1, \ldots, \alpha_n\}$ be the set of roots of $p(x)$ in $\mathbb{C}$. We define the splitting field of $p(x)$ to be the field

$$E = \bigcap_{\substack{K \subset \mathbb{C} \text{ field} \\ R_{p(x)} \subset K}} K$$

Derived groups

Definition

Let G be a group. We define its first derived group to be

$$G' = G^{(1)} = [G,G] = \langle xyx^{-1}y^{-1} \,|\, x,y \in G \rangle.$$

We define its higher derived groups in a recursive fashion:

$$G^{(k)} = \left(G^{(k-1)}\right)'.$$

Example

If G is an abelian group, then $G' = 0$.

Raul Gomez (gomez@cornell.edu)

Solvable groups

Observation

Given a group G, we have a descending chain

$$\cdots \subset G^{(2)} \subset G^{(1)} \subset G^{(0)} = G.$$

Definition

A group G is said to be solvable if there exists $k \in \mathbb{N}$ such that

$$G^{(k)} = \langle e \rangle.$$

Example

Let $G = S_3$. Then it can be checked that

$$G' = \langle e, (123), (132) \rangle \cong \mathbb{Z}/3\mathbb{Z},$$

and hence,

$$G^{(2)} = \langle e \rangle.$$

That is, S_3 is solvable.

Theorem

Let $G = S_n$. Then

1. For $n = 1, \ldots, 4$, G is solvable.
2. For $n \geq 5$, $G' = A_n$ and $G^{(2)} = A_n$. In particular, G is not solvable.

Theorem

Let F be a subfield of $\mathbb{C}$, and let $p(x) \in F[x]$ be an irreducible polynomial. Let E be the splitting field of $p(x)$, and let $G = \mathrm{Gal}(E/F)$ be the corresponding Galois group. Then $p(x)$ is solvable by radicals if and only if the group G is solvable.

Lemma

The Galois group of the splitting field of the polynomial $x^5 - x - 1$ is isomorphic to S_5.

Corollary

The polynomail $x^5 - x - 1$ is not solvable by radicals.

The Classical Groups

Figure : Sophus Lie

Following the ideas of Galois, Sophus Lie defined the symmetry group of a system of differential equations.

He then proved the following result:

Theorem

Let G be the symmetry group of a system of differential equations. Then the system is solvable by quadrature if and only if G is a solvable group.

His ideas lead to the definition of what it is now called a Lie group.

The general and the special linear group

Definition

Let $F = \mathbb{R}$ or $\mathbb{C}$. We define

$$\mathrm{GL}(n,F) = \{g : F^n \longrightarrow F^n \,|\, g \text{ is an invertible linear map}\}$$

and

$$\mathrm{SL}(n,F) = \{g \in \mathrm{GL}(n,F) \,|\, \det g = 1\}.$$

Bilinear forms

Definition

Let V be an F-vector space. A bilinear form is a map

$$B : V \times V \to F$$

such that

$$B(av_1 + bv_2, v_3) = aB(v_1, v_3) + bB(v_2, v_3)$$

and

$$B(v_1, abv_2 + bv_3) = aB(v_1, v_2) + bB(v_1, v_3),$$

for all v_1, v_2 and $v_3 \in V$.

Definition

We say that B si non-degenerate if for all $v \in V$, there exists $w \in V$ such that

$$B(v,w) \neq 0.$$

We say that B is symmetric if

$$B(v,w) = B(w,v)$$

for all v, $w \in V$.
We say that it's antisymmetric if

$$B(v,w) = -B(w,v)$$

for all v, $w \in V$.

Example

Let $V = \mathbb{R}^3$. Given vectors $v_1 = (x_1, y_1, z_1)$ and $v_2 = (x_2, y_2, z_2)$, we define

$$B(v_1, v_2) = v_1 \cdot v_2 = x_1 x_2 + y_1 y_2 + z_1 z_2,$$

to be the usual dot product. Then B is a non-degenerate symmetric bilinear form.

Definition

Given a vector space V, with a basis

$$\mathscr{B} = \{v_1, \ldots, v_n\}$$

and a bilinear form B on V, we define its associated matrix to be

$$[B] = [B]_{\mathscr{B}} = (B(v_i, v_j))_{i,j}.$$

Example

Let $V = \mathbb{R}^3$, and let

$$B(v_1, v_2) = v_1 \cdot v_2$$

as before. If $\mathscr{B} = \{e_1, e_2, e_3\}$ is the canonical basis, then

$$[B]_{\mathscr{B}} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}.$$

Example

Let $V = \mathbb{R}^2$, and let

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Define

$$B_A : V \times V \longrightarrow \mathbb{R}$$

by

$$B_A(v_1, v_2) = v_1^t A v_2.$$

Example

More concretely, if

$$v_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} 2 \\ 0 \end{bmatrix},$$

then

$$B_A(v_1, v_2) = \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} 4 \\ 2 \end{bmatrix} = 2.$$

The orthogonal groups

Definition

Let $A \in M_n(F)$ be a symmetric matrix, that is $A^T = A$. We define the orthogonal group associated to A to be

$$\mathrm{O}(A) = \{g \in \mathrm{GL}(n,F) \,|\, g^T A g = A\}$$

and the special orthogonal group to be

$$\mathrm{SO}(A) = \mathrm{O}(A) \cap \mathrm{SL}(n,F).$$

Definition

We set

$$\mathrm{O}(p,q) = \mathrm{O}(I_{p,q}),$$

where

$$I_{p,q} = \begin{bmatrix} I_p & \\ & -I_q \end{bmatrix}.$$

We also set

$$\mathrm{O}(n,F) = \mathrm{O}(n,0) \qquad \text{and} \qquad \mathrm{SO}(n,F) = \mathrm{SO}(n,0).$$

Theorem

Let $A \in M_n(F)$ be a non-singular symmetric matrix. Then

1. If $F = \mathbb{R}$, then there exists $p \geq q \geq 0$ such that

$$\mathrm{O}(A) \cong \mathrm{O}(p,q), \qquad \text{and} \qquad \mathrm{O}(A) \cong \mathrm{SO}(p,q).$$

2. If $F = \mathbb{C}$, then

$$\mathrm{O}(A) \cong \mathrm{O}(n,\mathbb{C}) \qquad \text{and} \qquad \mathrm{SO}(A) \cong \mathrm{SO}(n,\mathbb{C}).$$

Example

In two dimensions we have two different types of special orthogonal groups:

$$\mathsf{SO}(2,\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \middle| \theta \in \mathbb{R} \right\},$$

and

$$\mathsf{SO}(1,1) = \left\{ \pm \begin{bmatrix} \cosh\alpha & \sinh\alpha \\ \sinh\alpha & \cosh\alpha \end{bmatrix} \middle| \alpha \in \mathbb{R} \right\}.$$

The symplectic group

Definition

Let $A \in M_n(F)$ be an antisymmetric matrix, that is $A^T = -A$. We define the symplectic group associated to A to be

$$\mathrm{Sp}(A) = \{g \in \mathrm{GL}(n,F) \,|\, g^t A g = A\}.$$

Let

$$J = \begin{bmatrix} & -I_n \\ I_n & \end{bmatrix}.$$

We set

$$\mathrm{Sp}(2n,F) = \mathrm{Sp}(J).$$

Theorem

If $A \in M_{2n}(F)$, is an antisymmetric matrix, then

$$\mathrm{Sp}(A) \cong \mathrm{Sp}(2n, F).$$