Évariste Galois and Solvable Permutation Groups

David A. Cox

Department of Mathematics
Amherst College
dac@math.amherst.edu

Bilbao
May 2012

Prologue

Most mathematicians know about Galois:

- He introduced the concept of **group**.
- He created **Galois theory**.
- He defined **finite fields**.

This Talk

We will learn some of the **amazing other things** Galois did, especially his work on **solvable permutation groups**.

Prologue

Most mathematicians know about Galois:

- He introduced the concept of **group**.
- He created **Galois theory**.
- He defined **finite fields**.

This Talk

We will learn some of the **amazing other things** Galois did, especially his work on **solvable permutation groups**.

Prologue

Most mathematicians know about Galois:

- He introduced the concept of **group**.
- He created **Galois theory**.
- He defined **finite fields**.

This Talk

We will learn some of the **amazing other things** Galois did, especially his work on **solvable permutation groups**.

Prologue

Most mathematicians know about Galois:

- He introduced the concept of **group**.
- He created **Galois theory**.
- He defined **finite fields**.

This Talk

We will learn some of the **amazing other things** Galois did, especially his work on **solvable permutation groups**.

Outline

Outline

Outline

Three Snapshots from Lagrange

In 1770, Lagrange wrote the wonderful paper:

Réflexions sur la résolution des équations

which introduced many of the key players of group theory and Galois theory.

We will give three excerpts from this paper to show how Lagrange laid the foundation for what Galois did.

Three Snapshots from Lagrange

In 1770, Lagrange wrote the wonderful paper:

Réflexions sur la résolution des équations

which introduced many of the key players of group theory and Galois theory.

We will give three excerpts from this paper to show how Lagrange laid the foundation for what Galois did.

Snapshot #1

A Quote

A function y of the roots of a polynomial gives values $y', y'', \ldots$ when the roots are permuted. Lagrange says:

il s'agit ici uniquement de la forme de valeurs et non de leur quantité absolue.

Since $y = \dfrac{A(\alpha_1, \ldots, \alpha_n)}{B(\alpha_1, \ldots, \alpha_n)}$ has the form $\dfrac{A(x_1, \ldots, x_n)}{B(x_1, \ldots, x_n)}$,

we see that Lagrange regarded the roots as variables!

Snapshot #2

The Universal Extension

Let σ_i be the ith elementary symmetric polynomial. Consider

$$K = k(\sigma_1, \ldots, \sigma_n) \subseteq L = k(x_1, \ldots, x_n).$$

Lagrange's Theorem

If $t, y \in L$ and t is fixed by all permutations that fix y, then t is a rational expression in $y, \sigma_1, \ldots, \sigma_n$.

$K \subseteq K(y) \subseteq L$ gives $\mathrm{Gal}(L/K(y)) = \{$permutations fixing $y\}$. So

$$t \in \text{fixed field of } \mathrm{Gal}(L/K(y)) \Longrightarrow t \in K(y).$$

Hence $K(y)$ is the fixed field of $\mathrm{Gal}(L/K(y))$.

Lagrange knew the Galois correspondence!

Snapshot #2

The Universal Extension

Let σ_i be the ith elementary symmetric polynomial. Consider

$$K = k(\sigma_1, \ldots, \sigma_n) \subseteq L = k(x_1, \ldots, x_n).$$

Lagrange's Theorem

If $t, y \in L$ and t is fixed by all permutations that fix y, then t is a rational expression in $y, \sigma_1, \ldots, \sigma_n$.

$K \subseteq K(y) \subseteq L$ gives $\mathrm{Gal}(L/K(y)) = \{\text{permutations fixing } y\}$. So

$$t \in \text{fixed field of } \mathrm{Gal}(L/K(y)) \Longrightarrow t \in K(y).$$

Hence $K(y)$ is the fixed field of $\mathrm{Gal}(L/K(y))$.

Lagrange knew the Galois correspondence!

Snapshot #2

The Universal Extension

Let σ_i be the ith elementary symmetric polynomial. Consider
$K = k(\sigma_1, \ldots, \sigma_n) \subseteq L = k(x_1, \ldots, x_n)$.

Lagrange's Theorem

If $t, y \in L$ and t is fixed by all permutations that fix y, then t is a rational expression in $y, \sigma_1, \ldots, \sigma_n$.

$K \subseteq K(y) \subseteq L$ gives $\mathrm{Gal}(L/K(y)) = \{$permutations fixing $y\}$. So

$$t \in \text{fixed field of } \mathrm{Gal}(L/K(y)) \Longrightarrow t \in K(y).$$

Hence $K(y)$ is the fixed field of $\mathrm{Gal}(L/K(y))$.

Lagrange knew the Galois correspondence!

Snapshot #3

Definition

Rational functions $t, y \in L$ are **similar** (“semblable”) when a permutation fixes t if and only if it fixes y.

Corollary of Lagrange’s Theorem

Functions $t, y \in L$ are similar if and only if

$$K(t) = K(y).$$

For us, the Galois correspondence of $K \subseteq L$ is a bijection

$$\text{intermediate fields} \longleftrightarrow \text{subgroups of } S_n.$$

Lagrange worked with individual rational functions. The notion of “similar function” is his attempt at an intrinsic formulation.

Lagrange knew the Galois correspondence!

Snapshot #3

Definition

Rational functions $t, y \in L$ are **similar** (“semblable”) when a permutation fixes t if and only if it fixes y.

Corollary of Lagrange’s Theorem

Functions $t, y \in L$ are similar if and only if

$$K(t) = K(y).$$

For us, the Galois correspondence of $K \subseteq L$ is a bijection

$$\text{intermediate fields} \longleftrightarrow \text{subgroups of } S_n.$$

Lagrange worked with individual rational functions. The notion of “similar function” is his attempt at an intrinsic formulation.

Lagrange knew the Galois correspondence!

Snapshot #3

Definition

Rational functions $t, y \in L$ are **similar** (“semblable”) when a permutation fixes t if and only if it fixes y.

Corollary of Lagrange’s Theorem

Functions $t, y \in L$ are similar if and only if

$$K(t) = K(y).$$

For us, the Galois correspondence of $K \subseteq L$ is a bijection

$$\text{intermediate fields} \longleftrightarrow \text{subgroups of } S_n.$$

Lagrange worked with individual rational functions. The notion of “similar function” is his attempt at an intrinsic formulation.

Lagrange knew the Galois correspondence!

Four Snapshots from Galois

Évariste Galois was born October 25, 1811 and died May 31, 1832. We are celebrating the 200th anniversary of his birth.

In January 1831, he wrote the amazing paper:

Mémoire sur les conditions de résolubilité des équations par radicaux

I will give four excerpts from this memoir to give you a sense of how Galois thought about Galois theory.

Snapshot #1

Proposition I

Théorème. Soit une équation donnée, dont a,b,c,... sont les m racines. Il y aura toujours un groupe de permutations des lettres a,b,c,... qui jouira des propriété suivant:

1º que toute fonction des racines, invariable** par les substitutions de ce groupe, soit rationallement connue;

2º réciproquement, que toute fonction des racines déterminable rationallement, soit invariable par ces substitutions*.

The asterisks ** and * indicate marginal notes in Galois's manuscript.

Snapshot #1

Marginal Note for “invariable”**

Nous appelons ici invariable non seulement une fonction dont la forme est invariable par les substitutions des racines entre elles, mais encore celle dont las valeur numérique ne varieriat pas par ces substitutions.

Galois is aware that his theory applies to the roots of any polynomial, not just the case when the roots are variables.

Galois has gone beyond Lagrange!

Snapshot #2

Galois's Group

Quelle que soit l'équation donnée, on pourra trouver une fonction V des racines telle que toutes les racines soient fonctions rationelles des V. Cela posé, considérons l'equation irréductible done V est racine (lemmes III et IV). Soient $V, V', V'', \dots, V^{(n-1)}$ les racines de cette equation.

Soient $\varphi V, \varphi_1 V, \varphi_2 V, \dots, \varphi_{m-1} V$ les racines de la proposée.

Écrivons les n permutations suivants des racines:

$$\begin{array}{cccccc}
(V), & \varphi V, & \varphi_1 V, & \varphi_2 V, & \dots, & \varphi_{n-1} V, \\
(V'), & \varphi V', & \varphi_1 V', & \varphi_2 V', & \dots, & \dots, \\
\dots, & \dots, & \dots, & \dots, & \dots, & \dots, \\
(V^{(m-1)}), & \varphi V^{(m-1)}, & \varphi_1 V^{(m-1)}, & \varphi_2 V^{(m-1)}, & \dots, & \varphi_{n-1} V^{(m-1)}
\end{array}$$

Je dis que ce groupe de permutations jouit de la propriété énoncée.

Snapshot #2

For Galois, ***permutations*** are bijections

$$\{1,\ldots,m\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these arrangements}$$

while ***substitutions*** are bijections

$$\{\text{roots}\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these substitutions.}$$

- Arrangements give a strong visual picture.
- Substitutions give a group.
- Arrangements give a principal homogeneous space for the substitutions.

Marginal note for "substitutions*"

Mettre partout á la place du mot permutation le mot substitution

But then he crosses this out!

Snapshot #2

For Galois, ***permutations*** are bijections

$$\{1, \ldots, m\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these arrangements}$$

while ***substitutions*** are bijections

$$\{\text{roots}\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these substitutions.}$$

- Arrangements give a strong visual picture.
- Substitutions give a group.
- Arrangements give a principal homogeneous space for the substitutions.

Marginal note for "substitutions*"

Mettre partout á la place du mot permutation le mot substitution

But then he crosses this out!

Snapshot #2

For Galois, ***permutations*** are bijections

$$\{1,\ldots,m\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these arrangements}$$

while ***substitutions*** are bijections

$$\{\text{roots}\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these substitutions.}$$

- Arrangements give a strong visual picture.
- Substitutions give a group.
- Arrangements give a principal homogeneous space for the substitutions.

Marginal note for "substitutions*"

Mettre partout á la place du mot permutation le mot substitution

But then he crosses this out!

Snapshot #2

For Galois, ***permutations*** are bijections

$$\{1,\ldots,m\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these arrangements}$$

while ***substitutions*** are bijections

$$\{\text{roots}\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these substitutions.}$$

- Arrangements give a strong visual picture.
- Substitutions give a group.
- Arrangements give a principal homogeneous space for the substitutions.

Marginal note for "substitutions*"

Mettre partout á la place du mot permutation le mot substitution

But then he crosses this out!

Snapshot #2

For Galois, ***permutations*** are bijections

$$\{1, \ldots, m\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these arrangements}$$

while ***substitutions*** are bijections

$$\{\text{roots}\} \longrightarrow \{\text{roots}\} \quad \Leftarrow \text{call these substitutions.}$$

- Arrangements give a strong visual picture.
- Substitutions give a group.
- Arrangements give a principal homogeneous space for the substitutions.

Marginal note for "substitutions*"

Mettre partout á la place du mot permutation le mot substitution

But then he crosses this out!

Snapshot #3

Galois introduced normal subgroups as follows.

Proposition III

Théorème. Si ll'on adjoint á une équation toutes les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété que les substitutions sont les mêmes dans chaque groupe.

If G is the Galois group and a is one arrangement, then $G \cdot a$ is Galois's "groupe." The cosets of $H \subseteq G$ give

$$G \cdot a = g_1 H \cdot a \cup g_2 H \cdot a \cup \cdots .$$

These are the "groupes" of Proposition III. Key observation:

$$g(g_i H \cdot a) = g_i H \cdot a \iff g \in g_i H g_i^{-1}.$$

So "sont les mêmes" means H is normal!

Snapshot #3

Galois introduced normal subgroups as follows.

PROPOSITION III

THÉORÈME. Si ll'on adjoint á une équation TOUTES les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété que les substitutions sont les mêmes dans chaque groupe.

If G is the Galois group and a is one arrangement, then $G \cdot a$ is Galois's "groupe." The cosets of $H \subseteq G$ give

$$G \cdot a = g_1 H \cdot a \cup g_2 H \cdot a \cup \cdots .$$

These are the "groupes" of PROPOSITION III. Key observation:

$$g(g_i H \cdot a) = g_i H \cdot a \iff g \in g_i H g_i^{-1}.$$

So "sont les mêmes" means H is normal!

Snapshot #3

Galois introduced normal subgroups as follows.

Proposition III

Théorème. Si ll'on adjoint á une équation toutes les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété que les substitutions sont les mêmes dans chaque groupe.

If G is the Galois group and a is one arrangement, then $G \cdot a$ is Galois's "groupe." The cosets of $H \subseteq G$ give

$$G \cdot a = g_1 H \cdot a \cup g_2 H \cdot a \cup \cdots .$$

These are the "groupes" of Proposition III. Key observation:

$$g(g_i H \cdot a) = g_i H \cdot a \iff g \in g_i H g_i^{-1}.$$

So "sont les mêmes" means H is normal!

Snapshot #4

Galois had a wonderful result about the Galois group of a solvable polynomial of prime degree.

Proposition VII

Problème. Quel est le groupe d'une équation irréductible d'un degré premier *n*, soluble par radicaux?

Faisons en general $x_n = x_0,\ x_{n+1} = x_1,\ \ldots$

Donc, "si d'une équation irréductible de degré premier est soluble par radicaux, le groupe de cette léquation ne saurait contenir que les substitutions de la forme

$$x_k \quad x_{ak+b}$$

a et *b* étant des constants."

Snapshot #4

In modern terms, Galois's Proposition VII says that the Galois group of an irreducible polynomial of prime p is solvable by radicals if and only if the Galois group is isomorphic to a subgroup of the **affine linear group**

$$\mathrm{AGL}(1, \mathbb{F}_p) = \{x \mapsto ax + b \mid a, b \in \mathbb{F}_p,\ a \neq 0\}.$$

There are two aspects of this result worth mentioning:

- Up to conjugacy, $\mathrm{AGL}(1, \mathbb{F}_p)$ is the maximal solvable subgroup of the symmetric group S_p.
- This proposition implies that such a polynomial is solvable by radicals iff any two roots generate the splitting field.

Snapshot #4

In modern terms, Galois's Proposition VII says that the Galois group of an irreducible polynomial of prime p is solvable by radicals if and only if the Galois group is isomorphic to a subgroup of the **affine linear group**

$$\mathrm{AGL}(1, \mathbb{F}_p) = \{x \mapsto ax + b \mid a, b \in \mathbb{F}_p,\ a \neq 0\}.$$

There are two aspects of this result worth mentioning:

- Up to conjugacy, $\mathrm{AGL}(1, \mathbb{F}_p)$ is the maximal solvable subgroup of the symmetric group S_p.
- This proposition implies that such a polynomial is solvable by radicals iff any two roots generate the splitting field.

There is More!

The four snapshots from Galois:

- are well-known to most mathematicians, and
- illustrate nicely the power of the theory he developed.
- However, **Galois did a lot more!**
- In particular, we will explore:
  - what Galois knew about solvable permutation groups, and
  - why he invented finite fields.

There is More!

The four snapshots from Galois:

- are well-known to most mathematicians, and
- illustrate nicely the power of the theory he developed.
- However, **Galois did a lot more!**
- In particular, we will explore:
  - what Galois knew about solvable permutation groups, and
  - why he invented finite fields.

There is More!

The four snapshots from Galois:

- are well-known to most mathematicians, and
- illustrate nicely the power of the theory he developed.
- However, **Galois did a lot more!**
- In particular, we will explore:
  - what Galois knew about solvable permutation groups, and
  - why he invented finite fields.

There is More!

The four snapshots from Galois:

- are well-known to most mathematicians, and
- illustrate nicely the power of the theory he developed.
- However, **Galois did a lot more!**
- In particular, we will explore:
  - what Galois knew about solvable permutation groups, and
  - why he invented finite fields.

There is More!

The four snapshots from Galois:

- are well-known to most mathematicians, and
- illustrate nicely the power of the theory he developed.
- However, **Galois did a lot more!**
- In particular, we will explore:
  - what Galois knew about solvable permutation groups, and
  - why he invented finite fields.

There is More!

The four snapshots from Galois:

- are well-known to most mathematicians, and
- illustrate nicely the power of the theory he developed.
- However, **Galois did a lot more!**
- In particular, we will explore:
  - what Galois knew about solvable permutation groups, and
  - why he invented finite fields.

The Main Problem

Definition

On appelle équations non primitives les équations qui étant, par exemple, du degré mn, se décomposent en m facteurs du degré n, au moyen d'une seule équation du degré m.

Example

$x^4 - 2$ has degree $4 = 2 \cdot 2$. Adjoining roots of $x^2 - 2$ gives

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}).$$

Thus $x^4 - 2$ is ***imprimitive*** ("non primitive").

Revenons maintenant á notre object, et cherchons en général dans quel cas une équation primitive est soluble par radicaux.

The Main Problem

Definition

On appelle équations non primitives les équations qui étant, par exemple, du degré mn, se décomposent en m facteurs du degré n, au moyen d'une seule équation du degré m.

Example

$x^4 - 2$ has degree $4 = 2 \cdot 2$. Adjoining roots of $x^2 - 2$ gives

$$x^4 - 2 = \left(x^2 - \sqrt{2}\right)\left(x^2 + \sqrt{2}\right).$$

Thus $x^4 - 2$ is ***imprimitive*** ("non primitive").

Revenons maintenant á notre object, et cherchons en général dans quel cas une équation primitive est soluble par radicaux.

The Main Problem

Definition

On appelle équations non primitives les équations qui étant, par exemple, du degré mn, se décomposent en m facteurs du degré n, au moyen d'une seule équation du degré m.

Example

$x^4 - 2$ has degree $4 = 2 \cdot 2$. Adjoining roots of $x^2 - 2$ gives

$$x^4 - 2 = \left(x^2 - \sqrt{2}\right)\left(x^2 + \sqrt{2}\right).$$

Thus $x^4 - 2$ is ***imprimitive*** ("non primitive").

Revenons maintenant á notre object, et cherchons en général dans quel cas une équation primitive est soluble par radicaux.

The First Result

Galois's Version

. . . pour qu'une équation primitive soit soluble par radicaux, it faut que son degré soit de la forme p^ν, p étant premier.

Definition

A subgroup $G \subseteq S_n$ is ***imprimitive*** if

$$\{1, \ldots, n\} = R_1 \cup \cdots \cup R_k,\ k > 1,\ |R_i| > 1 \text{ for some } i$$

and elements of G preserve the R_i. Then G is ***primitive*** if it is not imprimitive.

Theorem

If $G \subseteq S_n$ is primitive and solvable, then $n = p^\nu$, p prime.

The First Result

Galois's Version

. . . pour qu'une équation primitive soit soluble par radicaux, it faut que son degré soit de la forme p^ν, p étant premier.

Definition

A subgroup $G \subseteq S_n$ is ***imprimitive*** if

$$\{1,\ldots,n\} = R_1 \cup \cdots \cup R_k,\ k > 1,\ |R_i| > 1 \text{ for some } i$$

and elements of G preserve the R_i. Then G is ***primitive*** if it is not imprimitive.

Theorem

If $G \subseteq S_n$ is primitive and solvable, then $n = p^\nu$, p prime.

The First Result

Galois's Version

… pour qu'une équation primitive soit soluble par radicaux, it faut que son degré soit de la forme p^ν, p étant premier.

Definition

A subgroup $G \subseteq S_n$ is ***imprimitive*** if

$$\{1, \ldots, n\} = R_1 \cup \cdots \cup R_k,\ k > 1,\ |R_i| > 1 \text{ for some } i$$

and elements of G preserve the R_i. Then G is ***primitive*** if it is not imprimitive.

Theorem

If $G \subseteq S_n$ is primitive and solvable, then $n = p^\nu$, p prime.

Proof

Assume $G \subseteq S_n$ is primitive and solvable. To show: $n = p^\nu$.

Let N be a minimal normal subgroup of G. One can prove that there is a simple group A such that

$$N \simeq A^\nu$$

This is a standard fact about minimal normal subgroups. Then:

- G primitive $\Longrightarrow$ N transitive.
- G solvable $\Longrightarrow$ $N \simeq \mathbb{F}_p^\nu$.
- N transitive and abelian $\Longrightarrow$ its isotropy subgroups are all equal and hence trivial. Thus:

$$p^\nu = |N| = |\text{orbit}| \cdot |\text{isotropy subgroup}| = n \cdot 1 = n. \quad \text{QED}$$

Proof

Assume $G \subseteq S_n$ is primitive and solvable. To show: $n = p^\nu$.

Let N be a minimal normal subgroup of G. One can prove that there is a simple group A such that

$$N \simeq A^\nu$$

This is a standard fact about minimal normal subgroups. Then:

- G primitive $\Longrightarrow$ N transitive.
- G solvable $\Longrightarrow$ $N \simeq \mathbb{F}_p^\nu$.
- N transitive and abelian $\Longrightarrow$ its isotropy subgroups are all equal and hence trivial. Thus:

$$p^\nu = |N| = |\text{orbit}| \cdot |\text{isotropy subgroup}| = n \cdot 1 = n. \quad \text{QED}$$

Proof

Assume $G \subseteq S_n$ is primitive and solvable. To show: $n = p^\nu$.

Let N be a minimal normal subgroup of G. One can prove that there is a simple group A such that

$$N \simeq A^\nu$$

This is a standard fact about minimal normal subgroups. Then:

- G primitive $\Longrightarrow$ N transitive.
- G solvable $\Longrightarrow$ $N \simeq \mathbb{F}_p^\nu$.
- N transitive and abelian $\Longrightarrow$ its isotropy subgroups are all equal and hence trivial. Thus:

$$p^\nu = |N| = |\text{orbit}| \cdot |\text{isotropy subgroup}| = n \cdot 1 = n. \quad \text{QED}$$

The Affine Linear Group

When G is primitive and solvable, the proof just given shows that $N \simeq \mathbb{F}_p^\nu$ is normal in G. One can show without difficulty that

$$G \subseteq \mathrm{AGL}(\nu, \mathbb{F}_p) = \{x \mapsto Ax + b \mid A \in \mathrm{GL}(\nu, \mathbb{F}_p),\ b \in \mathbb{F}_p^\nu\}.$$

Galois knew this!

Letter to Chevalier, 29 May 1832

Toutes les permuations d'une équation primitive soluble par radicaux sont de la forme

$$x_{k.l.m...}/x_{ak+bl+cm+...+f.a_1k+b_1l+c_1m+...+g.\ ...}$$

$k, l, m, \ldots$ étant ν indices qui prenant chacun p valeurs indiquent toutes les racines. Les indices sont pris suivant le module p, c'est-á-dire que la racines sera la même quand on adjoutera á l'un des indices un multiple de p.

Finite Fields and the Affine Semilinear Group

When a primitive of degree p^ν is solvable by radicals, its Galois group lies in

$$\mathrm{AGL}(\nu, \mathbb{F}_p) \subseteq S_{p^\nu}.$$

However, $\mathrm{AGL}(\nu, \mathbb{F}_p)$ is not solvable when $\nu \geq 2$. What is its maximal primitive solvable subgroup? This is the question Galois wanted to answer.

Galois used the ***Galois theory of finite fields*** to create some primitive solvable permutation subgroups of $\mathrm{AGL}(\nu, \mathbb{F}_p)$:

- $\mathrm{AGL}(1, \mathbb{F}_{p^\nu})$: The ***affine linear group*** over $\mathbb{F}_{p^\nu}$ is

$$\{x \mapsto ax + b \mid a, b \in \mathbb{F}_{p^\nu}, a \neq 0\}.$$

- $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^\nu})$: The ***affine semilinear group*** over $\mathbb{F}_{p^\nu}$ is

$$\{x \mapsto a\sigma(x) + b \mid a, b \in \mathbb{F}_{p^\nu}, \sigma \in \mathrm{Gal}(\mathbb{F}_{p^\nu}/\mathbb{F}_p), a \neq 0\}.$$

Finite Fields and the Affine Semilinear Group

When a primitive of degree p^ν is solvable by radicals, its Galois group lies in

$$\mathrm{AGL}(\nu, \mathbb{F}_p) \subseteq S_{p^\nu}.$$

However, $\mathrm{AGL}(\nu, \mathbb{F}_p)$ is not solvable when $\nu \geq 2$. What is its maximal primitive solvable subgroup? This is the question Galois wanted to answer.

Galois used the ***Galois theory of finite fields*** to create some primitive solvable permutation subgroups of $\mathrm{AGL}(\nu, \mathbb{F}_p)$:

- $\mathrm{AGL}(1, \mathbb{F}_{p^\nu})$: The ***affine linear group*** over $\mathbb{F}_{p^\nu}$ is

$$\{x \mapsto ax + b \mid a, b \in \mathbb{F}_{p^\nu}, a \neq 0\}.$$

- $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^\nu})$: The ***affine semilinear group*** over $\mathbb{F}_{p^\nu}$ is

$$\{x \mapsto a\sigma(x) + b \mid a, b \in \mathbb{F}_{p^\nu}, \sigma \in \mathrm{Gal}(\mathbb{F}_{p^\nu}/\mathbb{F}_p), a \neq 0\}.$$

What Galois Knew

Why Do We Need Finite Fields?

C'est surtout dans la théorie des permutations . . . que la considération des racines imaginaires des congruences paraît indispensable. Elle donne une moyen simple et facile de reconnaître dans quel cas une équation primitive soit soluble par radicaux . . .

Galois notes that if the Galois group of a primitive equation lies in $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^\nu})$, then the equation is solvable by radicals.

Galois Goes On To Say:

Cette remarque aurait peu d'importance, si je n'etais parvenu á demontrer que réciproquement une équation primitive ne saurait soluble par radicaux, á moins de satisfaire aux conditions que je viens d'enoncer.

What Galois Knew

Why Do We Need Finite Fields?

C'est surtout dans la théorie des permutations . . . que la considération des racines imaginaires des congruences paraît indispensable. Elle donne une moyen simple et facile de reconnaître dans quel cas une équation primitive soit soluble par radicaux . . .

Galois notes that if the Galois group of a primitive equation lies in $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^\nu})$, then the equation is solvable by radicals.

Galois Goes On To Say:

Cette remarque aurait peu d'importance, si je n'etais parvenu á demontrer que réciproquement une équation primitive ne saurait soluble par radicaux, á moins de satisfaire aux conditions que je viens d'enoncer.

Subsequent Developments

Galois Knew That There Were Exceptions:

J'excepte les équations du 9^{e} et 25^{e} degré.

- In 1868, Jordan classifed primitive solvable subgroups of S_{p^2}. He used $A\Gamma L(1, \mathbb{F}_{p^2})$ together with two other groups.
- Of Jordan's groups, only $A\Gamma L(1, \mathbb{F}_{p^2})$ is doubly-transitive.
- Doubly-transitive subgroups are automatically primitive, though the converse (as shown by Jordan) is false.

Jordan's result shows that Galois characterization of primitive solvable equations has some gaps. But maybe Galois was implicitly assuming double-transitivity. If this is the case, then his characterization (with the above exceptions) is remarkably close to being complete.

Subsequent Developments

Galois Knew That There Were Exceptions:

J'excepte les équations du 9^e et 25^e degré.

- In 1868, Jordan classifed primitive solvable subgroups of S_{p^2}. He used $A\Gamma L(1, \mathbb{F}_{p^2})$ together with two other groups.
- Of Jordan's groups, only $A\Gamma L(1, \mathbb{F}_{p^2})$ is doubly-transitive.
- Doubly-transitive subgroups are automatically primitive, though the converse (as shown by Jordan) is false.

Jordan's result shows that Galois characterization of primitive solvable equations has some gaps. But maybe Galois was implicitly assuming double-transitivity. If this is the case, then his characterization (with the above exceptions) is remarkably close to being complete.

Subsequent Developments

Galois Knew That There Were Exceptions:

J'excepte les équations du 9^e et 25^e degré.

- In 1868, Jordan classifed primitive solvable subgroups of S_{p^2}. He used $A\Gamma L(1, \mathbb{F}_{p^2})$ together with two other groups.
- Of Jordan's groups, only $A\Gamma L(1, \mathbb{F}_{p^2})$ is doubly-transitive.
- Doubly-transitive subgroups are automatically primitive, though the converse (as shown by Jordan) is false.

Jordan's result shows that Galois characterization of primitive solvable equations has some gaps. But maybe Galois was implicitly assuming double-transitivity. If this is the case, then his characterization (with the above exceptions) is remarkably close to being complete.

Subsequent Developments

Galois Knew That There Were Exceptions:

J'excepte les équations du 9^e et 25^e degré.

- In 1868, Jordan classifed primitive solvable subgroups of S_{p^2}. He used $A\Gamma L(1, \mathbb{F}_{p^2})$ together with two other groups.
- Of Jordan's groups, only $A\Gamma L(1, \mathbb{F}_{p^2})$ is doubly-transitive.
- Doubly-transitive subgroups are automatically primitive, though the converse (as shown by Jordan) is false.

Jordan's result shows that Galois characterization of primitive solvable equations has some gaps. But maybe Galois was implicitly assuming double-transitivity. If this is the case, then his characterization (with the above exceptions) is remarkably close to being complete.

Subsequent Developments

Galois Knew That There Were Exceptions:

J'excepte les équations du 9^e et 25^e degré.

- In 1868, Jordan classifed primitive solvable subgroups of S_{p^2}. He used $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^2})$ together with two other groups.
- Of Jordan's groups, only $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^2})$ is doubly-transitive.
- Doubly-transitive subgroups are automatically primitive, though the converse (as shown by Jordan) is false.

Jordan's result shows that Galois characterization of primitive solvable equations has some gaps. But maybe Galois was implicitly assuming double-transitivity. If this is the case, then his characterization (with the above exceptions) is remarkably close to being complete.

Huppert's Theorem

Here is the great theorem proved by Huppert in 1957.

Theorem

Assume $G \subseteq S_n$ is solvable and doubly-transitive. Then:

- $n = p^\nu$, p prime.
- Furthermore, if

$$p^\nu \notin \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\},$$

then $G \subseteq \mathrm{A\Gamma L}(1, \mathbb{F}_{p^\nu})$ up to conjugacy.

Given that Galois invented groups in 1829, his level of insight is astonishing! So, in this 200th anniversary of Galois's birth, we have more to celebrate than we thought!

Huppert's Theorem

Here is the great theorem proved by Huppert in 1957.

Theorem

Assume $G \subseteq S_n$ is solvable and doubly-transitive. Then:

- $n = p^\nu$, p prime.
- Furthermore, if

$$p^\nu \notin \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\},$$

then $G \subseteq A\Gamma L(1, \mathbb{F}_{p^\nu})$ up to conjugacy.

Given that Galois invented groups in 1829, his level of insight is astonishing! So, in this 200th anniversary of Galois's birth, we have more to celebrate than we thought!

Huppert's Theorem

Here is the great theorem proved by Huppert in 1957.

Theorem

Assume $G \subseteq S_n$ is solvable and doubly-transitive. Then:

- $n = p^\nu$, p prime.
- Furthermore, if

$$p^\nu \notin \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\},$$

then $G \subseteq A\Gamma L(1, \mathbb{F}_{p^\nu})$ up to conjugacy.

Given that Galois invented groups in 1829, his level of insight is astonishing! So, in this 200th anniversary of Galois's birth, we have more to celebrate than we thought!

Huppert's Theorem

Here is the great theorem proved by Huppert in 1957.

Theorem

Assume $G \subseteq S_n$ is solvable and doubly-transitive. Then:

- $n = p^\nu$, p prime.
- Furthermore, if
$$p^\nu \notin \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\},$$
then $G \subseteq \mathrm{A\Gamma L}(1, \mathbb{F}_{p^\nu})$ up to conjugacy.

Given that Galois invented groups in 1829, his level of insight is astonishing! So, in this 200th anniversary of Galois's birth, we have more to celebrate than we thought!