Galois Theory: Past and Present

Tamás Szamuely

Rényi Institute, Budapest

Evariste Galois (1811–1832)

submitted 3 papers on algebraic equations to the French Academy:

Evariste Galois (1811–1832)

submitted 3 papers on algebraic equations to the French Academy:

- one in 1828 – lost by the referee (Cauchy)

The Mémoire

Evariste Galois (1811–1832)

submitted 3 papers on algebraic equations to the French Academy:

- one in 1828 – lost by the referee (Cauchy)
- one in 1829 – lost by the referee (Fourier)

Evariste Galois (1811–1832)

submitted 3 papers on algebraic equations to the French Academy:

- one in 1828 – lost by the referee (Cauchy)
- one in 1829 – lost by the referee (Fourier)
- one in 1830: *Mémoire sur les conditions de résolubilité des équations par radicaux* – refused by the referee (Poisson)

Evariste Galois (1811–1832)

submitted 3 papers on algebraic equations to the French Academy:

- one in 1828 – lost by the referee (Cauchy)
- one in 1829 – lost by the referee (Fourier)
- one in 1830: *Mémoire sur les conditions de résolubilité des équations par radicaux* – refused by the referee (Poisson)
- plus posthumous fragments, and the famous letter to Auguste Chevalier, of which the last words are:

"[...] il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis."

Solvability by radicals

The equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1) \cdots (x - \alpha_n) = 0$$

is *solvable by radicals* if the α_i can be obtained from the a_j in finitely many steps by taking suitable rational functions and m-th roots.

Solvability by radicals

The equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1) \cdots (x - \alpha_n) = 0$$

is *solvable by radicals* if the α_i can be obtained from the a_j in finitely many steps by taking suitable rational functions and m-th roots.

Some highlights of the theory before Galois:

- equations of degree ≤ 4 are solvable by radicals (Cardano, Ferrari)

Solvability by radicals

The equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1)\cdots(x - \alpha_n) = 0$$

is *solvable by radicals* if the α_i can be obtained from the a_j in finitely many steps by taking suitable rational functions and m-th roots.

Some highlights of the theory before Galois:

- equations of degree ≤ 4 are solvable by radicals (Cardano, Ferrari)
- cyclotomic equations

  $$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

  are solvable by radicals (Gauss)

Solvability by radicals

The equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1) \cdots (x - \alpha_n) = 0$$

is *solvable by radicals* if the α_i can be obtained from the a_j in finitely many steps by taking suitable rational functions and m-th roots.

Some highlights of the theory before Galois:

- equations of degree ≤ 4 are solvable by radicals (Cardano, Ferrari)
- cyclotomic equations

  $$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

  are solvable by radicals (Gauss)
- more generally, equations 'with abelian Galois group' are solvable by radicals (Abel)

Solvability by radicals

The equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1) \cdots (x - \alpha_n) = 0$$

is *solvable by radicals* if the α_i can be obtained from the a_j in finitely many steps by taking suitable rational functions and m-th roots.

Some highlights of the theory before Galois:

- equations of degree ≤ 4 are solvable by radicals (Cardano, Ferrari)
- cyclotomic equations

  $$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

  are solvable by radicals (Gauss)
- more generally, equations 'with abelian Galois group' are solvable by radicals (Abel)
- the 'general equations' of degree ≥ 5 are not solvable by radicals (Abel)

Main results of the Mémoire in modern language

Consider the equation

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = $$
$$= (x - \alpha_1) \cdots (x - \alpha_n) = 0$$

where $a_i \in K$, a field of characteristic 0.

Main results of the Mémoire in modern language

Consider the equation

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \\ = (x-\alpha_1)\cdots(x-\alpha_n) = 0$$

where $a_i \in K$, a field of characteristic 0.
Assume the α_i are distinct. Put

$$K(\alpha_1, \ldots, \alpha_n) := \{F(\alpha_1, \ldots, \alpha_n) : F \in K(x_1, \ldots, x_n)\}$$

(This is the smallest subfield of $\overline{K}$ containing the α_i.)
The equation is not assumed to be irreducible.

Main results of the Mémoire in modern language

Consider the equation

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \\ = (x-\alpha_1)\cdots(x-\alpha_n) = 0$$

where $a_i \in K$, a field of characteristic 0.
Assume the α_i are distinct. Put

$$K(\alpha_1, \ldots, \alpha_n) := \{F(\alpha_1, \ldots, \alpha_n) : F \in K(x_1, \ldots, x_n)\}$$

(This is the smallest subfield of $\overline{K}$ containing the α_i.)
The equation is not assumed to be irreducible.

1. For every $\alpha \in K(\alpha_1, \ldots, \alpha_n)$ there is a unique monic irreducible polynomial $p \in K[x]$ with $p(\alpha) = 0$, the *minimal polynomial* of α.

Main results of the Mémoire in modern language

Consider the equation

$$\begin{aligned} f(x) =& x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \\ =& (x-\alpha_1)\cdots(x-\alpha_n) = 0 \end{aligned}$$

where $a_i \in K$, a field of characteristic 0.
Assume the α_i are distinct. Put

$$K(\alpha_1, \ldots, \alpha_n) := \{F(\alpha_1, \ldots, \alpha_n) : F \in K(x_1, \ldots, x_n)\}$$

(This is the smallest subfield of $\overline{K}$ containing the α_i.)
The equation is not assumed to be irreducible.

1. For every $\alpha \in K(\alpha_1, \ldots, \alpha_n)$ there is a unique monic irreducible polynomial $p \in K[x]$ with $p(\alpha) = 0$, the *minimal polynomial* of α.
2. There exists $\beta \in K(\alpha_1, \ldots, \alpha_n)$ with

$$K(\alpha_1, \ldots, \alpha_n) = K(\beta)$$

(*theorem of the primitive element*).

Main results of the Mémoire in modern language

So $\alpha_i = f_i(\beta)$ with some $f_i \in K[x]$, for all i.

So $\alpha_i = f_i(\beta)$ with some $f_i \in K[x]$, for all i.

3. Let $\beta = \beta_1, \ldots, \beta_m$ be the roots of p.
Then for all j the sequence $f_1(\beta_j), \ldots, f_n(\beta_j)$ is a permutation of the α_i.
Denoting this permutation by σ_j, the elements $\sigma_1, \ldots, \sigma_m$ form the *Galois group.*

Main results of the Mémoire in modern language

So $\alpha_i = f_i(\beta)$ with some $f_i \in K[x]$, for all i.

3. Let $\beta = \beta_1, \ldots, \beta_m$ be the roots of p.
Then for all j the sequence $f_1(\beta_j), \ldots, f_n(\beta_j)$ is a permutation of the α_i.
Denoting this permutation by σ_j, the elements $\sigma_1, \ldots, \sigma_m$ form the *Galois group.*

4. Let $L|K$ be a field extension obtained by adjoining roots of some equation $g(x) = 0$ to K.
The Galois group of f over L is a subgroup of its Galois group over K; it is a *normal subgroup* if and only if L is obtained by adjoining *all roots* of g.

Main results of the Mémoire in modern language

So $\alpha_i = f_i(\beta)$ with some $f_i \in K[x]$, for all i.

3. Let $\beta = \beta_1, \ldots, \beta_m$ be the roots of p.
Then for all j the sequence $f_1(\beta_j), \ldots, f_n(\beta_j)$ is a permutation of the α_i.
Denoting this permutation by σ_j, the elements $\sigma_1, \ldots, \sigma_m$ form the *Galois group.*

4. Let $L|K$ be a field extension obtained by adjoining roots of some equation $g(x) = 0$ to K.
The Galois group of f over L is a subgroup of its Galois group over K; it is a *normal subgroup* if and only if L is obtained by adjoining *all roots* of g.

5. The equation $f(x) = 0$ is solvable by radicals if and only if its Galois group is solvable, i.e. there is a chain of normal subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

where G_i is of prime index in G_{i-1}.

Applications

An irreducible equation

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_p) = 0$$

of prime degree is solvable by radicals if and only if the roots α_i can be expressed as rational functions of any two of them.

Applications

An irreducible equation

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_p) = 0$$

of prime degree is solvable by radicals if and only if the roots α_i can be expressed as rational functions of any two of them.

[Uses the classification of solvable transitive subgroups of S_p: they are conjugates of subgroups of

$$\{x \mapsto ax + b : \ a, b \in \mathbf{F}_p\}.]$$

Applications

An irreducible equation

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_p) = 0$$

of prime degree is solvable by radicals if and only if the roots α_i can be expressed as rational functions of any two of them.

[Uses the classification of solvable transitive subgroups of S_p: they are conjugates of subgroups of

$$\{x \mapsto ax + b : \; a, b \in \mathbf{F}_p\}.]$$

Another application from fragments: Let p be an odd prime. Consider the Galois cover

$$\Gamma_0(p) \setminus \mathbf{H} \to \Gamma_0 \setminus \mathbf{H} \cong \mathbf{C}.$$

Adding cusps we get a branched cover of modular curves

$$X_0(p) \to \mathbf{P}^1_{\mathbf{C}}.$$

The Galois group is $\mathrm{PSL}(2, p)$ which is simple for $p \neq 3$. So the *modular equation* is not solvable by radicals.

Later developments

- The work of Galois was clarified by Liouville, Jordan...

Later developments

- The work of Galois was clarified by Liouville, Jordan...
- Weber (1888) recast the theory in the language of field extensions

Later developments

- The work of Galois was clarified by Liouville, Jordan...
- Weber (1888) recast the theory in the language of field extensions
- Dedekind (1894) defined the Galois group as the automorphism group of a field extension

Later developments

- The work of Galois was clarified by Liouville, Jordan...
- Weber (1888) recast the theory in the language of field extensions
- Dedekind (1894) defined the Galois group as the automorphism group of a field extension
- Steinitz (1909) constructed the algebraic closure and clarified questions of separability

Later developments

- The work of Galois was clarified by Liouville, Jordan...
- Weber (1888) recast the theory in the language of field extensions
- Dedekind (1894) defined the Galois group as the automorphism group of a field extension
- Steinitz (1909) constructed the algebraic closure and clarified questions of separability
- Artin (1920's) formulated the *Galois correspondence*, i.e. the bijection

$$\{\text{subextensions of } L|K\} \leftrightarrow \{\text{subgroups of } G\}$$

for a finite Galois extension $L|K$ with group G

Later developments

- The work of Galois was clarified by Liouville, Jordan...
- Weber (1888) recast the theory in the language of field extensions
- Dedekind (1894) defined the Galois group as the automorphism group of a field extension
- Steinitz (1909) constructed the algebraic closure and clarified questions of separability
- Artin (1920's) formulated the *Galois correspondence*, i.e. the bijection

  $$\{\text{subextensions of } L|K\} \leftrightarrow \{\text{subgroups of } G\}$$

  for a finite Galois extension $L|K$ with group G
- Artin (1942) defined a finite Galois extension as a field extension $L|K$ where K is the fixed field of a finite group G acting on L.

Infinite Galois extensions

Dedekind's insight: for infinite Galois extensions *"die Galoissche Gruppe gewissermaßen eine stetige Mannigfaltigkeit bilde"*.

Infinite Galois extensions

Dedekind's insight: for infinite Galois extensions *"die Galoissche Gruppe gewissermaßen eine stetige Mannigfaltigkeit bilde"*.

Justified by Krull (1928). In modern language:

Like Artin, define an algebraic extension $K|k$ to be *Galois* if the subfield of K fixed by the action of $\mathrm{Aut}(K|k)$ is k.
In this case $\mathrm{Gal}(K|k) := \mathrm{Aut}(K|k)$ is the Galois group.

Infinite Galois extensions

Dedekind's insight: for infinite Galois extensions *"die Galoissche Gruppe gewissermaßen eine stetige Mannigfaltigkeit bilde"*.

Justified by Krull (1928). In modern language:

Like Artin, define an algebraic extension $K|k$ to be *Galois* if the subfield of K fixed by the action of $\mathrm{Aut}(K|k)$ is k.
In this case $\mathrm{Gal}(K|k) := \mathrm{Aut}(K|k)$ is the Galois group.
Given a tower of finite Galois subextensions $M|L|k$ contained in $K|k$, there is a canonical surjection $\phi_{ML} : \mathrm{Gal}(M|k) \twoheadrightarrow \mathrm{Gal}(L|k)$.
If $K \supset N \supset M$ is yet another finite Galois extension of k, we have

$$\phi_{NL} = \phi_{ML} \circ \phi_{NM}.$$

Infinite Galois extensions

Dedekind's insight: for infinite Galois extensions *"die Galoissche Gruppe gewissermaßen eine stetige Mannigfaltigkeit bilde"*.

Justified by Krull (1928). In modern language:

Like Artin, define an algebraic extension $K|k$ to be *Galois* if the subfield of K fixed by the action of $\mathrm{Aut}(K|k)$ is k.
In this case $\mathrm{Gal}(K|k) := \mathrm{Aut}(K|k)$ is the Galois group.
Given a tower of finite Galois subextensions $M|L|k$ contained in $K|k$, there is a canonical surjection $\phi_{ML} : \mathrm{Gal}(M|k) \twoheadrightarrow \mathrm{Gal}(L|k)$.
If $K \supset N \supset M$ is yet another finite Galois extension of k, we have

$$\phi_{NL} = \phi_{ML} \circ \phi_{NM}.$$

So if we "pass to the limit in M", then $\mathrm{Gal}(L|k)$ will become a quotient of $\mathrm{Gal}(K|k)$.

This is achieved by proving

$$\mathrm{Gal}(K|k) \cong \varprojlim_{L} \mathrm{Gal}(L|k)$$

The RHS is a subgroup of the direct product, so inherits a topology if the $\mathrm{Gal}(L|k)$ are taken to be discrete. It is called the *Krull topology.*

This is achieved by proving

$$\mathrm{Gal}(K|k) \cong \varprojlim_{L} \mathrm{Gal}(L|k)$$

The RHS is a subgroup of the direct product, so inherits a topology if the $\mathrm{Gal}(L|k)$ are taken to be discrete. It is called the *Krull topology.*

$\mathrm{Gal}(K|k)$ is compact and totally disconnected. It is either finite or uncountable. Its finite quotients are the $\mathrm{Gal}(L|k)$.

Theorem (Krull's Galois correspondence)

$$\{\text{subextensions of } K|k\} \leftrightarrow \{\text{closed subgroups of } \mathrm{Gal}(K|k)\}$$

This is achieved by proving

$$\mathrm{Gal}(K|k) \cong \varprojlim_{L} \mathrm{Gal}(L|k)$$

The RHS is a subgroup of the direct product, so inherits a topology if the $\mathrm{Gal}(L|k)$ are taken to be discrete. It is called the *Krull topology.*

$\mathrm{Gal}(K|k)$ is compact and totally disconnected. It is either finite or uncountable. Its finite quotients are the $\mathrm{Gal}(L|k)$.

Theorem (Krull's Galois correspondence)

$$\{\text{subextensions of } K|k\} \leftrightarrow \{\text{closed subgroups of } \mathrm{Gal}(K|k)\}$$

This applies in particular to $K = k_s =$ separable closure of k. $\mathrm{Gal}(k_s|k)$ is the *absolute Galois group* of k.

Inverse questions

Fact: If G is a finite group, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k) \cong G$.

Inverse questions

Fact: If G is a finite group, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k) \cong G$.
[Embed G in S_n for some n and make it act on $k(x_1, \ldots, x_n)$ by permuting the x_i; then take G-invariants.]

Inverse questions

Fact: If G is a finite group, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k) \cong G$.
[Embed G in S_n for some n and make it act on $k(x_1, \ldots, x_n)$ by permuting the x_i; then take G-invariants.]

Leptin (1955): The above is true for any profinite group G.

Inverse questions

Fact: If G is a finite group, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k) \cong G$.
[Embed G in S_n for some n and make it act on $k(x_1, \ldots, x_n)$ by permuting the x_i; then take G-invariants.]

Leptin (1955): The above is true for any profinite group G.

Question: Which profinite groups are absolute Galois groups?

Inverse questions

Fact: If G is a finite group, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k) \cong G$.
[Embed G in S_n for some n and make it act on $k(x_1, \ldots, x_n)$ by permuting the x_i; then take G-invariants.]

Leptin (1955): The above is true for any profinite group G.

Question: Which profinite groups are absolute Galois groups?

Artin, Schreier (1927): A finite group G is an absolute Galois group if and only if $|G| \leq 2$.

Inverse questions

Fact: If G is a finite group, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k) \cong G$.
[Embed G in S_n for some n and make it act on $k(x_1, \ldots, x_n)$ by permuting the x_i; then take G-invariants.]

Leptin (1955): The above is true for any profinite group G.

Question: Which profinite groups are absolute Galois groups?

Artin, Schreier (1927): A finite group G is an absolute Galois group if and only if $|G| \leq 2$.

For arbitrary G the question is open. A famous necessary condition is given by:

Voevodsky (2003): If G is the absolute Galois group of a field, then the cohomology ring

$$\bigoplus_{i=1}^{\infty} H^i(G, \mathbf{Z}/2\mathbf{Z})$$

is generated by $H^1(G, \mathbf{Z}/2\mathbf{Z})$.

Galois characterization of fields

Take two primes $p \neq q$, and consider

$$K_1 = \mathbf{Q}(\sqrt{p}) \quad \text{and} \quad K_2 = \mathbf{Q}(\sqrt{q}).$$

Question: can $\mathrm{Gal}(\bar{\mathbf{Q}}|K_1)$ and $\mathrm{Gal}(\bar{\mathbf{Q}}|K_2)$ be isomorphic?

Galois characterization of fields

Take two primes $p \neq q$, and consider

$$K_1 = \mathbf{Q}(\sqrt{p}) \quad \text{and} \quad K_2 = \mathbf{Q}(\sqrt{q}).$$

Question: can $\mathrm{Gal}(\bar{\mathbf{Q}}|K_1)$ and $\mathrm{Gal}(\bar{\mathbf{Q}}|K_2)$ be isomorphic?
Answer: NO, for arithmetic reasons.
[The prime p ramifies in K_1 but not in K_2; this is 'seen' by the local Euler characteristic.]

Galois characterization of fields

Take two primes $p \neq q$, and consider

$$K_1 = \mathbf{Q}(\sqrt{p}) \quad \text{and} \quad K_2 = \mathbf{Q}(\sqrt{q}).$$

Question: can $\mathrm{Gal}(\bar{\mathbf{Q}}|K_1)$ and $\mathrm{Gal}(\bar{\mathbf{Q}}|K_2)$ be isomorphic?
Answer: NO, for arithmetic reasons.
[The prime p ramifies in K_1 but not in K_2; this is 'seen' by the local Euler characteristic.]
In fact, we have:

Neukirch (1969): Let K_1 and K_2 be Galois extensions of $\mathbf{Q}$. Then every isomorphism

$$\mathrm{Gal}(\overline{K}_1|K_1) \xrightarrow{\sim} \mathrm{Gal}(\overline{K}_2|K_2)$$

is induced by a unique isomorphism of fields

$$K_2 \xrightarrow{\sim} K_1.$$

Galois characterization of fields

Take two primes $p \neq q$, and consider

$$K_1 = \mathbf{Q}(\sqrt{p}) \quad \text{and} \quad K_2 = \mathbf{Q}(\sqrt{q}).$$

Question: can $\mathrm{Gal}(\bar{\mathbf{Q}}|K_1)$ and $\mathrm{Gal}(\bar{\mathbf{Q}}|K_2)$ be isomorphic?
Answer: NO, for arithmetic reasons.
[The prime p ramifies in K_1 but not in K_2; this is 'seen' by the local Euler characteristic.]
In fact, we have:

Neukirch (1969): Let K_1 and K_2 be Galois extensions of $\mathbf{Q}$. Then every isomorphism

$$\mathrm{Gal}(\overline{K}_1|K_1) \xrightarrow{\sim} \mathrm{Gal}(\overline{K}_2|K_2)$$

is induced by a unique isomorphism of fields

$$K_2 \xrightarrow{\sim} K_1.$$

Vast generalization (Pop, 1996): The above is true more generally for fields finitely generated over the prime field (up to a purely inseparable extension in characteristic > 0)).

The absolute Galois group of $\mathbf{Q}$

Conjecture (folklore)

Every finite group is a quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$.

The absolute Galois group of $\mathbf{Q}$

Conjecture (folklore)

Every finite group is a quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$.

Open in general, known in many cases, among which:

- solvable groups (Shafarevich; Neukirch for groups of odd order)

The absolute Galois group of $\mathbf{Q}$

Conjecture (folklore)

Every finite group is a quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$.

Open in general, known in many cases, among which:

- solvable groups (Shafarevich; Neukirch for groups of odd order)
- most finite simple groups, including all sporadic groups but one (Belyi, Fried, Malle, Matzat, Thompson...)

The absolute Galois group of $\mathbf{Q}$

Conjecture (folklore)

Every finite group is a quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$.

Open in general, known in many cases, among which:

- solvable groups (Shafarevich; Neukirch for groups of odd order)
- most finite simple groups, including all sporadic groups but one (Belyi, Fried, Malle, Matzat, Thompson...)

The absolute Galois group of $\mathbf{Q}$

Conjecture (folklore)

Every finite group is a quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$.

Open in general, known in many cases, among which:

- solvable groups (Shafarevich; Neukirch for groups of odd order)
- most finite simple groups, including all sporadic groups but one (Belyi, Fried, Malle, Matzat, Thompson...)

But even if we knew a positive answer to the conjecture, this would not describe the structure of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$. The following would yield more:

The absolute Galois group of $\mathbf{Q}$

Conjecture (folklore)

Every finite group is a quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$.

Open in general, known in many cases, among which:

- solvable groups (Shafarevich; Neukirch for groups of odd order)
- most finite simple groups, including all sporadic groups but one (Belyi, Fried, Malle, Matzat, Thompson...)

But even if we knew a positive answer to the conjecture, this would not describe the structure of $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$. The following would yield more:

Conjecture (Shafarevich)

The group $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q}(\mu))$ *is a free profinite group, where* $\mathbf{Q}(\mu)$ *is obtained by adjoining all roots of unity.*

Grothendieck's reformulation

Let k be a field, k_s a separable closure,
$G := \mathrm{Gal}(k_s|k)$.

Grothendieck's reformulation

Let k be a field, k_s a separable closure,
$G := \mathrm{Gal}(k_s|k)$.
It acts on k_s, hence on $\mathrm{Hom}_k(L, k_s)$ for all $L|k$ (k-algebra homomorphisms).

Grothendieck's reformulation

Let k be a field, k_s a separable closure,
$G := \mathrm{Gal}(k_s|k)$.
It acts on k_s, hence on $\mathrm{Hom}_k(L, k_s)$ for all $L|k$ (k-algebra homomorphisms).
If $L = k(\alpha)$ is finite separable, $\mathrm{Hom}_k(L, k_s)$ is finite. Give it the discrete topology. The G-action is continuous and transitive.

Grothendieck's reformulation

Let k be a field, k_s a separable closure,
$G := \mathrm{Gal}(k_s|k)$.
It acts on k_s, hence on $\mathrm{Hom}_k(L, k_s)$ for all $L|k$ (k-algebra homomorphisms).
If $L = k(\alpha)$ is finite separable, $\mathrm{Hom}_k(L, k_s)$ is finite. Give it the discrete topology. The G-action is continuous and transitive.

Theorem

The contravariant functor

$$L \to \mathrm{Hom}_k(L, k_s)$$

gives an anti-equivalence of categories:

$$\{\text{finite separable extensions } L|k\} \leftrightarrow \{\text{finite sets} + \text{continuous transitive } G\text{-action}\}$$

Grothendieck's reformulation

Let k be a field, k_s a separable closure,
$G := \mathrm{Gal}(k_s|k)$.
It acts on k_s, hence on $\mathrm{Hom}_k(L, k_s)$ for all $L|k$ (k-algebra homomorphisms).
If $L = k(\alpha)$ is finite separable, $\mathrm{Hom}_k(L, k_s)$ is finite. Give it the discrete topology. The G-action is continuous and transitive.

Theorem

The contravariant functor

$$L \to \mathrm{Hom}_k(L, k_s)$$

gives an anti-equivalence of categories:

$$\{\text{finite separable extensions } L|k\} \leftrightarrow \{\text{finite sets} + \text{continuous transitive } G\text{-action}\}$$

Grothendieck's reformulation

[Inverse functor:
finite continuous G-set $\mapsto$ subfield of k_s fixed by the stabilizer of a point]

[Inverse functor:
finite continuous G-set $\mapsto$ subfield of k_s fixed by the stabilizer of a point]

Definition. A finite étale k-algebra is a finite direct product of separable extensions of k.

Grothendieck's reformulation

[Inverse functor:
finite continuous G-set $\mapsto$ subfield of k_s fixed by the stabilizer of a point]

Definition. A finite étale k-algebra is a finite direct product of separable extensions of k.

Theorem

The contravariant functor

$$A \to \mathrm{Hom}_k(A, k_s)$$

gives an anti-equivalence of categories

$$\{\text{finite étale } k\text{-algebras}\} \leftrightarrow \{\text{finite sets} + \text{continuous } G\text{-action}\}$$

Topological analogue

X= 'nice' topological space, e.g. a topological manifold

Topological analogue

X= ‘nice’ topological space, e.g. a topological manifold
$Y \to X$: cover of X

Topological analogue

$X=$ 'nice' topological space, e.g. a topological manifold
$Y \to X$: cover of X
$\mathrm{Fib}_x(Y) :=$ fibre of Y over $x \in X$.

Topological analogue

X= 'nice' topological space, e.g. a topological manifold
$Y \to X$: cover of X
$\mathrm{Fib}_x(Y) :=$ fibre of Y over $x \in X$.
It carries an action by the fundamental group $\pi_1(X, x)$ ('lifting paths and homotopies').

Topological analogue

$X=$ 'nice' topological space, e.g. a topological manifold
$Y \to X$: cover of X
$\mathrm{Fib}_x(Y) :=$ fibre of Y over $x \in X$.
It carries an action by the fundamental group $\pi_1(X, x)$ ('lifting paths and homotopies').

Theorem

The functor

$$Y \to \mathrm{Fib}_x(Y)$$

gives an equivalence of categories

$$\{\text{covers of } X\} \leftrightarrow \{\pi_1(X, x)\text{-sets}\}$$

Topological analogue

X= 'nice' topological space, e.g. a topological manifold
$Y \to X$: cover of X
$\mathrm{Fib}_x(Y) :=$ fibre of Y over $x \in X$.
It carries an action by the fundamental group $\pi_1(X, x)$ ('lifting paths and homotopies').

Theorem

The functor

$$Y \to \mathrm{Fib}_x(Y)$$

gives an equivalence of categories

$$\{\text{covers of } X\} \leftrightarrow \{\pi_1(X, x)\text{-sets}\}$$

Let $\Pi :=$ profinite completion of $\pi_1(X, x)$.

Topological analogue

$X=$ 'nice' topological space, e.g. a topological manifold
$Y \to X$: cover of X
$\mathrm{Fib}_x(Y) :=$ fibre of Y over $x \in X$.
It carries an action by the fundamental group $\pi_1(X, x)$ ('lifting paths and homotopies').

Theorem

The functor

$$Y \to \mathrm{Fib}_x(Y)$$

gives an equivalence of categories

$$\{\text{covers of } X\} \leftrightarrow \{\pi_1(X, x)\text{-sets}\}$$

Let $\Pi :=$ profinite completion of $\pi_1(X, x)$.
We get an equivalence

$$\{\text{finite covers of } X\} \leftrightarrow \{\text{finite continuous } \Pi\text{-sets}\}$$

Grothendieck's π_1

Analogue of finite cover in algebraic geometry: surjective finite étale maps $Y \to X$.

Grothendieck's π_1

Analogue of finite cover in algebraic geometry: surjective finite étale maps $Y \to X$.

For X equipped with a geometric point Grothendieck defined a profinite group $\pi_1(X, \bar{x})$ together with an equivalence of categories

$$\{\text{finite étale } Y \to X\} \leftrightarrow$$
$$\leftrightarrow \{\text{finite continuous } \pi_1(X, \bar{x})\text{-sets}\}$$

Grothendieck's π_1

Analogue of finite cover in algebraic geometry: surjective finite étale maps $Y \to X$.
For X equipped with a geometric point Grothendieck defined a profinite group $\pi_1(X, \bar{x})$ together with an equivalence of categories

$$\{\text{finite étale } Y \to X\} \leftrightarrow$$
$$\leftrightarrow \{\text{finite continuous } \pi_1(X, \bar{x})\text{-sets}\}$$

It is induced by a fibre functor $Y \to \mathrm{Fib}_{\bar{x}}(Y)$.

Grothendieck's π_1

Analogue of finite cover in algebraic geometry: surjective finite étale maps $Y \to X$.
For X equipped with a geometric point Grothendieck defined a profinite group $\pi_1(X, \bar{x})$ together with an equivalence of categories

$$\{\text{finite étale } Y \to X\} \leftrightarrow$$
$$\leftrightarrow \{\text{finite continuous } \pi_1(X, \bar{x})\text{-sets}\}$$

It is induced by a fibre functor $Y \to \mathrm{Fib}_{\bar{x}}(Y)$.

- For X= point over k, $\pi_1(X, \bar{x}) = \mathrm{Gal}(k_s|k)$.

Grothendieck's π_1

Analogue of finite cover in algebraic geometry: surjective finite étale maps $Y \to X$.

For X equipped with a geometric point Grothendieck defined a profinite group $\pi_1(X, \bar{x})$ together with an equivalence of categories

$$\{\text{finite étale } Y \to X\} \leftrightarrow$$
$$\leftrightarrow \{\text{finite continuous } \pi_1(X, \bar{x})\text{-sets}\}$$

It is induced by a fibre functor $Y \to \mathrm{Fib}_{\bar{x}}(Y)$.

- For X= point over k, $\pi_1(X, \bar{x}) = \mathrm{Gal}(k_s|k)$.
- For X= variety over **C**,

$$\pi_1(X, \bar{x}) = \text{profinite completion of } \pi_1^{\mathrm{top}}(X, \bar{x})$$

(actually its *opposite group*).

Grothendieck's π_1

Analogue of finite cover in algebraic geometry: surjective finite étale maps $Y \to X$.
For X equipped with a geometric point Grothendieck defined a profinite group $\pi_1(X, \bar{x})$ together with an equivalence of categories

$$\{\text{finite étale } Y \to X\} \leftrightarrow$$
$$\leftrightarrow \{\text{finite continuous } \pi_1(X, \bar{x})\text{-sets}\}$$

It is induced by a fibre functor $Y \to \mathrm{Fib}_{\bar{x}}(Y)$.

- For $X=$ point over k, $\pi_1(X, \bar{x}) = \mathrm{Gal}(k_s|k)$.
- For $X=$ variety over **C**,

$$\pi_1(X, \bar{x}) = \text{profinite completion of } \pi_1^{\mathrm{top}}(X, \bar{x})$$

(actually its *opposite group*).

When X is defined over a subfield $k \subset \mathbf{C}$, $\pi_1(X, \bar{x})$ carries an *outer action* by $\mathrm{Gal}(k_s|k)$.
This gives interesting representations of $\mathrm{Gal}(k_s|k)$.

Linearization

Up to now we have only considered *permutation representations.* But *linear* representations are much more common ‘in nature’.

Linearization

Up to now we have only considered *permutation representations*. But *linear* representations are much more common 'in nature'.

Example

If $X \subset \mathbf{C}$ *is a complex domain,* $x \in X$*, n-th order linear holomorphic differential equations*

$$y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0$$

give rise to representations $\rho : \pi_1(X, x) \to \mathrm{GL}_n(\mathbf{C})$*:*

Linearization

Up to now we have only considered *permutation representations.* But *linear* representations are much more common 'in nature'.

Example

If $X \subset \mathbf{C}$ *is a complex domain,* $x \in X$*, n-th order linear holomorphic differential equations*

$$y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0$$

give rise to representations $\rho : \pi_1(X, x) \to \mathrm{GL}_n(\mathbf{C})$*:*
By Cauchy's existence theorem, local solutions around x *form an n-dimensional* $\mathbf{C}$*-vector space on which* $\pi_1(X, x)$ *acts by the monodromy action.*

Tannakian duality

Algebraically, finite-dimensional complex representations form a category stable by subrepresentations, quotients, tensor products, duals.

Tannakian duality

Algebraically, finite-dimensional complex representations form a category stable by subrepresentations, quotients, tensor products, duals.

Consider the subcategory generated by ρ after doing all these constructions. How much of $\pi_1(X, x)$ does it determine?

Tannakian duality

Algebraically, finite-dimensional complex representations form a category stable by subrepresentations, quotients, tensor products, duals.

Consider the subcategory generated by ρ after doing all these constructions. How much of $\pi_1(X, x)$ does it determine?

Answer: The Zariski closure of $\mathrm{Im}\,(\rho)$ in $\mathrm{GL}_n(\mathbf{C})$.
This is a *linear algebraic group.*

Tannakian duality

Algebraically, finite-dimensional complex representations form a category stable by subrepresentations, quotients, tensor products, duals.

Consider the subcategory generated by ρ after doing all these constructions. How much of $\pi_1(X, x)$ does it determine?

Answer: The Zariski closure of $\mathrm{Im}\,(\rho)$ in $\mathrm{GL}_n(\mathbf{C})$.
This is a *linear algebraic group.*

If we consider *all* monodromy representations, we get an *affine group scheme.*

Tannakian duality

Algebraically, finite-dimensional complex representations form a category stable by subrepresentations, quotients, tensor products, duals.

Consider the subcategory generated by ρ after doing all these constructions. How much of $\pi_1(X, x)$ does it determine?

Answer: The Zariski closure of $\mathrm{Im}\,(\rho)$ in $\mathrm{GL}_n(\mathbf{C})$.
This is a *linear algebraic group.*

If we consider *all* monodromy representations, we get an *affine group scheme.*

Tannakian duality

A rigid k-linear abelian tensor category C equipped with a faithful exact tensor functor ('fibre functor')
$C \to$ finite-dimensional k-vector spaces
is equivalent to the finite-dimensional representations of an affine k-group scheme.

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

- holomorphic differential equations $\rightarrow$ algebraic monodromy groups

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

- holomorphic differential equations $\to$ algebraic monodromy groups
- differential modules $\to$ differential Galois groups

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

- holomorphic differential equations $\to$ algebraic monodromy groups
- differential modules $\to$ differential Galois groups
- Hodge structures $\to$ Mumford–Tate groups

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

- holomorphic differential equations $\to$ algebraic monodromy groups
- differential modules $\to$ differential Galois groups
- Hodge structures $\to$ Mumford–Tate groups
- motives $\to$ motivic Galois groups

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

- holomorphic differential equations $\to$ algebraic monodromy groups
- differential modules $\to$ differential Galois groups
- Hodge structures $\to$ Mumford–Tate groups
- motives $\to$ motivic Galois groups

Thus all these objects are classified by algebraic group actions.

Examples

In examples, the tensor subcategories generated by a single object often correspond to representations of a linear algebraic group.

- holomorphic differential equations $\to$ algebraic monodromy groups
- differential modules $\to$ differential Galois groups
- Hodge structures $\to$ Mumford–Tate groups
- motives $\to$ motivic Galois groups

Thus all these objects are classified by algebraic group actions. This was Galois' main idea!