Introduction to Profinite Groups

Martyn Quick

23rd March 2005

Motivation

Frequent theme in infinite group theory

How do the finite images of a group affect its structure?

Motivation

Frequent theme in infinite group theory

How do the finite images of a group affect its structure?

Theorem (Hirsch, 1946)

Let G be polycyclic-by-finite. If every finite quotient of G is nilpotent, then G is nilpotent.

Motivation

Frequent theme in infinite group theory

How do the finite images of a group affect its structure?

Theorem (Hirsch, 1946)

Let G be polycyclic-by-finite. If every finite quotient of G is nilpotent, then G is nilpotent.

Theorem (Grunewald–Pickel–Segal, 1980)

Let G be polycyclic-by-finite. Then there are finitely many isomorphism classes of polycyclic-by-finite groups having the same finite quotients as G.

Motivation

Frequent theme in infinite group theory

How do the finite images of a group affect its structure?

Theorem (Hirsch, 1946)

Let G be polycyclic-by-finite. If every finite quotient of G is nilpotent, then G is nilpotent.

Theorem (Grunewald–Pickel–Segal, 1980)

Let G be polycyclic-by-finite. Then there are finitely many isomorphism classes of polycyclic-by-finite groups having the same finite quotients as G.

Motivation II

Theorem (Zelmanov, RBP)

For every pair of integers d and n, there is a largest finite d-generator group of exponent n.

Motivation II

Theorem (Zelmanov, RBP)

For every pair of integers d and n, there is a largest finite d-generator group of exponent n.

Positive Solution of the Restricted Burnside Problem:

A f.g. profinite group of finite exponent is finite.

Motivation II

Theorem (Zelmanov, RBP)

For every pair of integers d and n, there is a largest finite d-generator group of exponent n.

Positive Solution of the Restricted Burnside Problem:
A f.g. profinite group of finite exponent is finite.

Theorem (Lubotzky–Mann–Segal, PSG-Theorem, 1993)

Let G be a f.g. residually finite group and define

$$s_n(G) = \#\{\, H \leqslant G \mid |G : H| \leqslant n \,\}.$$

Motivation II

Theorem (Zelmanov, RBP)

For every pair of integers d and n, there is a largest finite d-generator group of exponent n.

Positive Solution of the Restricted Burnside Problem:
A f.g. profinite group of finite exponent is finite.

Theorem (Lubotzky–Mann–Segal, PSG-Theorem, 1993)

Let G be a f.g. residually finite group and define

$$s_n(G) = \#\{\, H \leqslant G \mid |G : H| \leqslant n \,\}.$$

Then G has PSG
if and only if G is virtually soluble of finite rank.

Motivation II

Theorem (Zelmanov, RBP)

For every pair of integers d and n, there is a largest finite d-generator group of exponent n.

Positive Solution of the Restricted Burnside Problem:

A f.g. profinite group of finite exponent is finite.

Theorem (Lubotzky–Mann–Segal, PSG-Theorem, 1993)

Let G be a f.g. residually finite group and define

$$s_n(G) = \#\{\, H \leqslant G \mid |G : H| \leqslant n \,\}.$$

Then G has PSG ($s_n(G) \leqslant n^c$ for some c)
if and only if G is virtually soluble of finite rank.

Inverse Systems

Definition

A *directed set* is a partially ordered set I such that if $i_1, i_2 \in I$ there is some $j \in I$ such that $i_1 \leqslant j$ and $i_2 \leqslant j$.

Inverse Systems

Definition

A *directed set* is a partially ordered set I such that if $i_1, i_2 \in I$ there is some $j \in I$ such that $i_1 \leqslant j$ and $i_2 \leqslant j$.

Definition

An *inverse system*

$$\{ G_i, \phi_{ij} \mid i, j \in I,\ i \geqslant j \}$$

of groups indexed by a directed set I consists of

Inverse Systems

Definition

A *directed set* is a partially ordered set I such that if $i_1, i_2 \in I$ there is some $j \in I$ such that $i_1 \leqslant j$ and $i_2 \leqslant j$.

Definition

An *inverse system*

$$\{ G_i, \phi_{ij} \mid i, j \in I,\ i \geqslant j \}$$

of groups indexed by a directed set I consists of

- a group G_i for each $i \in I$

Inverse Systems

Definition

A *directed set* is a partially ordered set I such that if $i_1, i_2 \in I$ there is some $j \in I$ such that $i_1 \leqslant j$ and $i_2 \leqslant j$.

Definition

An *inverse system*

$$\{ G_i, \phi_{ij} \mid i, j \in I,\ i \geqslant j \}$$

of groups indexed by a directed set I consists of

- a group G_i for each $i \in I$
- a homomorphism $\phi_{ij} : G_i \to G_j$ whenever $i \geqslant j$ in I

Inverse Systems

Definition

A *directed set* is a partially ordered set I such that if $i_1, i_2 \in I$ there is some $j \in I$ such that $i_1 \leqslant j$ and $i_2 \leqslant j$.

Definition

An *inverse system*

$$\{ G_i, \phi_{ij} \mid i, j \in I,\ i \geqslant j \}$$

of groups indexed by a directed set I consists of

- a group G_i for each $i \in I$
- a homomorphism $\phi_{ij} : G_i \to G_j$ whenever $i \geqslant j$ in I such that

$$\phi_{ij}\phi_{jk} = \phi_{ik} \qquad \text{when } i \geqslant j \geqslant k.$$

Inverse Limits

Definition

The *inverse limit* of the inverse system $\{G_i, \phi_{ij}\}_I$ is

$$\varprojlim G_i = \{ (g_i)_{i \in I} \mid g_i \in G_i \text{ for all } i$$

Inverse Limits

Definition

The *inverse limit* of the inverse system $\{G_i, \phi_{ij}\}_I$ is

$$\varprojlim G_i = \{\, (g_i)_{i\in I} \mid g_i \in G_i \text{ for all } i \text{ and } g_i\phi_{ij} = g_j \text{ whenever } i \geqslant j \,\}.$$

Inverse Limits

Definition

The *inverse limit* of the inverse system $\{G_i, \phi_{ij}\}_I$ is

$$\varprojlim G_i = \{\, (g_i)_{i\in I} \mid g_i \in G_i \text{ for all } i \text{ and } g_i\phi_{ij} = g_j \text{ whenever } i \geqslant j \,\}.$$

Note $\varprojlim G_i \subseteq \prod_{i\in I} G_i$.

Inverse Limits

Definition

The *inverse limit* of the inverse system $\{G_i, \phi_{ij}\}_I$ is

$$\varprojlim G_i = \{\, (g_i)_{i\in I} \mid g_i \in G_i \text{ for all } i \text{ and } g_i\phi_{ij} = g_j \text{ whenever } i \geqslant j \,\}.$$

Note $\varprojlim G_i \subseteq \prod_{i\in I} G_i$.

Lemma

$\varprojlim G_i$ is a subgroup of $\prod_{i\in I} G_i$.

Universal Property of Inverse Limits

Theorem

Let $\{G_i, \phi_{ij}\}_I$ *be an inverse system of groups,* $G = \varprojlim G_i$ *and* $\rho_i \colon G \to G_i$ *the projection to the* i*th component.*

Universal Property of Inverse Limits

Theorem

Let $\{G_i, \phi_{ij}\}_I$ be an inverse system of groups, $G = \varprojlim G_i$ and $\rho_i \colon G \to G_i$ the projection to the ith component.
Then (G, ρ_i) is the unique solution of the following universal problem:

Universal Property of Inverse Limits

Theorem

Let $\{G_i, \phi_{ij}\}_I$ be an inverse system of groups, $G = \varprojlim G_i$ and $\rho_i \colon G \to G_i$ the projection to the ith component.
Then (G, ρ_i) is the unique solution of the following universal problem:

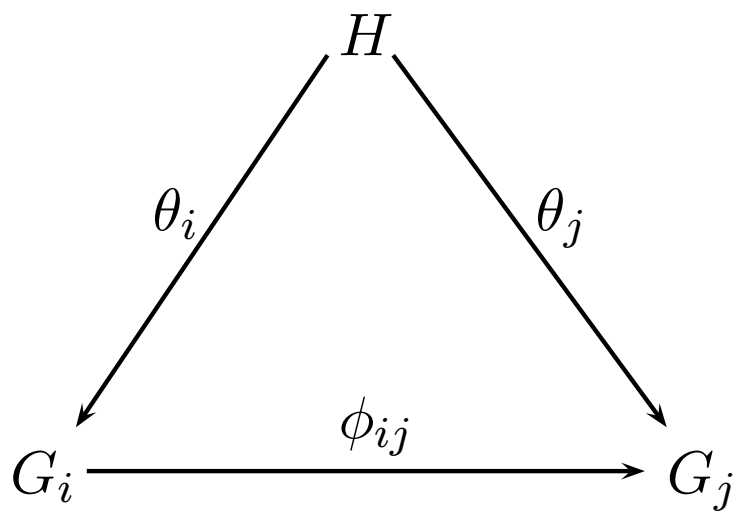
> *Given a group H and homomorphisms $\theta_i \colon H \to G_i$ such that $\theta_i \phi_{ij} = \theta_j$ whenever $i \geqslant j$, there is a unique homomorphism $\theta \colon H \to G$ such that $\theta_i = \theta \rho_i$ for all i.*

Universal Property of Inverse Limits

Theorem

Let $\{G_i, \phi_{ij}\}_I$ be an inverse system of groups, $G = \varprojlim G_i$ and $\rho_i \colon G \to G_i$ the projection to the ith component.
Then (G, ρ_i) is the unique solution of the following universal problem:

> *Given a group H and homomorphisms $\theta_i \colon H \to G_i$ such that $\theta_i \phi_{ij} = \theta_j$ whenever $i \geqslant j$, there is a unique homomorphism $\theta \colon H \to G$ such that $\theta_i = \theta \rho_i$ for all i.*

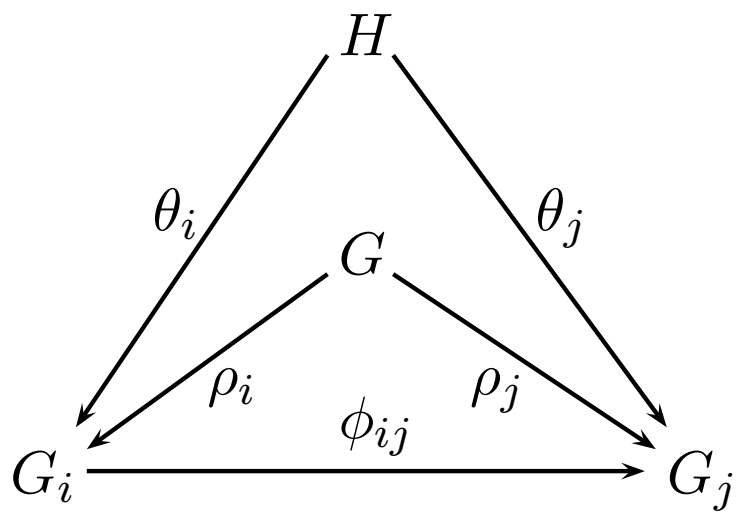


Universal Property of Inverse Limits

Theorem

Let $\{G_i, \phi_{ij}\}_I$ be an inverse system of groups, $G = \varprojlim G_i$ and $\rho_i \colon G \to G_i$ the projection to the ith component.
Then (G, ρ_i) is the unique solution of the following universal problem:

> *Given a group H and homomorphisms $\theta_i \colon H \to G_i$ such that $\theta_i \phi_{ij} = \theta_j$ whenever $i \geqslant j$, there is a unique homomorphism $\theta \colon H \to G$ such that $\theta_i = \theta \rho_i$ for all i.*

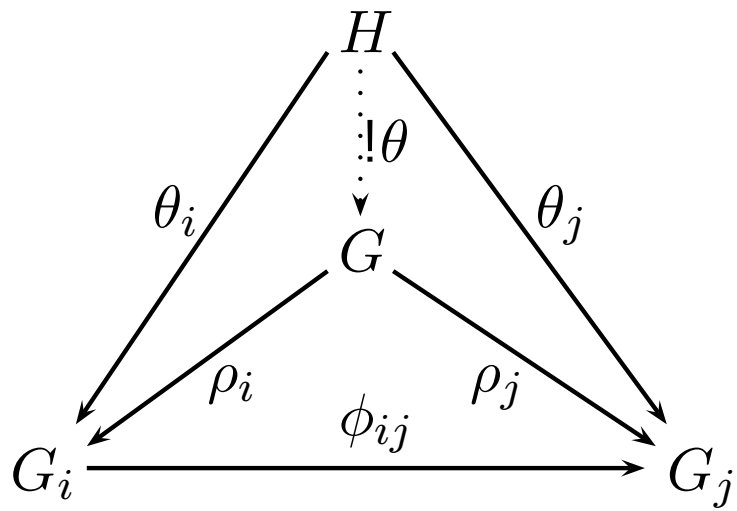


Universal Property of Inverse Limits

Theorem

Let $\{G_i, \phi_{ij}\}_I$ be an inverse system of groups, $G = \varprojlim G_i$ and $\rho_i \colon G \to G_i$ the projection to the ith component.
Then (G, ρ_i) is the unique solution of the following universal problem:

> *Given a group H and homomorphisms $\theta_i \colon H \to G_i$ such that $\theta_i \phi_{ij} = \theta_j$ whenever $i \geqslant j$, there is a unique homomorphism $\theta \colon H \to G$ such that $\theta_i = \theta \rho_i$ for all i.*



Some topology

Definition

A *topological space* X is a set together with a family $\mathscr{T}$ of *open sets* such that

(T1) $\varnothing, X \in \mathscr{T}$;

(T2) if $U_\lambda \in \mathscr{T}$ for $\lambda \in \Lambda$, then $\bigcup_{\lambda\in\Lambda} U_\lambda \in \mathscr{T}$;

(T3) if $U_1, U_2, \ldots, U_n \in \mathscr{T}$, then $U_1 \cap U_2 \cap \cdots \cap U_n \in \mathscr{T}$.

Some topology

Definition

A *topological space* X is a set together with a family $\mathscr{T}$ of *open sets* such that

(T1) $\varnothing, X \in \mathscr{T}$;

(T2) if $U_\lambda \in \mathscr{T}$ for $\lambda \in \Lambda$, then $\bigcup_{\lambda\in\Lambda} U_\lambda \in \mathscr{T}$;

(T3) if $U_1, U_2, \ldots, U_n \in \mathscr{T}$, then $U_1 \cap U_2 \cap \cdots \cap U_n \in \mathscr{T}$.

Definition

A topological space X is *compact* if whenever

$$X = \bigcup_{\lambda\in\Lambda} U_\lambda \qquad (U_\lambda \text{ open}),$$

Some topology

Definition

A *topological space* X is a set together with a family $\mathscr{T}$ of *open sets* such that

(T1) $\varnothing, X \in \mathscr{T}$;

(T2) if $U_\lambda \in \mathscr{T}$ for $\lambda \in \Lambda$, then $\bigcup_{\lambda\in\Lambda} U_\lambda \in \mathscr{T}$;

(T3) if $U_1, U_2, \ldots, U_n \in \mathscr{T}$, then $U_1 \cap U_2 \cap \cdots \cap U_n \in \mathscr{T}$.

Definition

A topological space X is *compact* if whenever

$$X = \bigcup_{\lambda\in\Lambda} U_\lambda \qquad (U_\lambda \text{ open}),$$

there exist $\lambda_1, \lambda_2, \ldots, \lambda_k$ such that

$$X = U_{\lambda_1} \cup U_{\lambda_2} \cup \cdots \cup U_{\lambda_k}.$$

Definition

A topological space X is *Hausdorff* if whenever $x, y \in X$ $(x \neq y)$ there are *disjoint* open sets U, V such that $x \in U$ and $y \in V$.

Definition

A topological space X is *Hausdorff* if whenever $x, y \in X$ $(x \neq y)$ there are *disjoint* open sets U, V such that $x \in U$ and $y \in V$.

Example

If X is a finite set, the *discrete topology* is that where *all* subsets of X are decreed to be open.
With this topology, X is compact and Hausdorff.

Back to inverse limits

Suppose $\{G_i, \phi_{ij}\}_I$ is an inverse system of *finite* groups.
View each G_i as a topological space via the discrete topology.

Back to inverse limits

Suppose $\{G_i, \phi_{ij}\}_I$ is an inverse system of *finite* groups.
View each G_i as a topological space via the discrete topology.

Let $C = \prod_{i \in I} G_i$ have the *product topology*.

Back to inverse limits

Suppose $\{G_i, \phi_{ij}\}_I$ is an inverse system of *finite* groups.
View each G_i as a topological space via the discrete topology.

Let $C = \prod_{i \in I} G_i$ have the *product topology*.
Tychonoff's Theorem $\Rightarrow C$ is compact.

Back to inverse limits

Suppose $\{G_i, \phi_{ij}\}_I$ is an inverse system of *finite* groups.
View each G_i as a topological space via the discrete topology.

Let $C = \prod_{i \in I} G_i$ have the *product topology*.
Tychonoff's Theorem $\Rightarrow C$ is compact.
Easy to see C is Hausdorff.

Back to inverse limits

Suppose $\{G_i, \phi_{ij}\}_I$ is an inverse system of *finite* groups.
View each G_i as a topological space via the discrete topology.

Let $C = \prod_{i \in I} G_i$ have the *product topology*.
Tychonoff's Theorem $\Rightarrow C$ is compact.
Easy to see C is Hausdorff.

$\varprojlim G_i = \{ (g_i) \mid g_i \phi_{ij} = g_j \ \forall i \geqslant j \}$ is closed in C.

Back to inverse limits

Suppose $\{G_i, \phi_{ij}\}_I$ is an inverse system of *finite* groups.
View each G_i as a topological space via the discrete topology.

Let $C = \prod_{i \in I} G_i$ have the *product topology*.
Tychonoff's Theorem $\Rightarrow C$ is compact.
Easy to see C is Hausdorff.

$\varprojlim G_i = \{ (g_i) \mid g_i \phi_{ij} = g_j \ \forall i \geqslant j \}$ is closed in C.

Proposition

The inverse limit $\varprojlim G_i$ of an inverse system of finite groups is a compact Hausdorff topological group.

Profinite Groups

Definition

A *profinite group* is

- an inverse limit of finite groups,

Profinite Groups

Definition

A *profinite group* is

- an inverse limit of finite groups,
  or equivalently
- a compact Hausdorff topological group such that every open set containing 1 (*neighbourhood*) necessarily contains an open subgroup.

Profinite Groups

Definition

A *profinite group* is

- an inverse limit of finite groups,
  or equivalently
- a compact Hausdorff topological group such that every open set containing 1 (*neighbourhood*) necessarily contains an open subgroup.

Lemma

If G is a compact topological group, then every open subgroup has finite index.

Profinite Groups

Definition

A *profinite group* is

- an inverse limit of finite groups,
  or equivalently
- a compact Hausdorff topological group such that every open set containing 1 (*neighbourhood*) necessarily contains an open subgroup.

Lemma

If G is a compact topological group, then every open subgroup has finite index.

Theorem

Let G satisfy the second part of the Definition. Then

$$G \cong \varprojlim (G/N)_{N \trianglelefteqslant_O G}.$$

Finite images of abstract groups

Let Γ be an (infinite abstract) group.
Then $\{\, \Gamma/N \mid N \trianglelefteqslant_f \Gamma \,\}$ forms an inverse system.

Finite images of abstract groups

Let Γ be an (infinite abstract) group.
Then $\{\, \Gamma/N \mid N \trianglelefteqslant_f \Gamma \,\}$ forms an inverse system.
Form $G = \varprojlim(\Gamma/N)_{N \trianglelefteqslant_f \Gamma}$.

Finite images of abstract groups

Let Γ be an (infinite abstract) group.
Then $\{\,\Gamma/N \mid N \trianglelefteqslant_f \Gamma\,\}$ forms an inverse system.
Form $G = \varprojlim(\Gamma/N)_{N\trianglelefteqslant_f\Gamma}$.
Define

$$\begin{aligned}\theta\colon \Gamma &\to G\\ x &\mapsto (Nx)_{N\trianglelefteqslant_f\Gamma}\end{aligned}$$

Finite images of abstract groups

Let Γ be an (infinite abstract) group.
Then $\{\, \Gamma/N \mid N \trianglelefteqslant_f \Gamma \,\}$ forms an inverse system.
Form $G = \varprojlim(\Gamma/N)_{N \trianglelefteqslant_f \Gamma}$.
Define

$$\begin{aligned} \theta \colon \Gamma &\to G \\ x &\mapsto (Nx)_{N \trianglelefteqslant_f \Gamma} \end{aligned}$$

$$\ker\theta = \bigcap_{N \trianglelefteqslant_f \Gamma} N \qquad (\textit{finite residual} \text{ of } \Gamma).$$

Finite images of abstract groups

Let Γ be an (infinite abstract) group.
Then $\{\, \Gamma/N \mid N \trianglelefteqslant_f \Gamma \,\}$ forms an inverse system.
Form $G = \varprojlim(\Gamma/N)_{N \trianglelefteqslant_f \Gamma}$.
Define

$$\begin{aligned} \theta \colon \Gamma &\to G \\ x &\mapsto (Nx)_{N \trianglelefteqslant_f \Gamma} \end{aligned}$$

$$\ker\theta = \bigcap_{N \trianglelefteqslant_f \Gamma} N \qquad (\textit{finite residual} \text{ of } \Gamma).$$

Typically $\operatorname{im}\theta < G$, but it *is* dense.

Profinite Completions

Definition

If Γ is an arbitrary group, the inverse limit

$$\hat{\Gamma} = \varprojlim (\Gamma/N)_{N \trianglelefteqslant_f \Gamma}$$

is called the *profinite completion* of Γ.

Theorem

If Γ is residually finite, then it embeds as a dense subgroup of its profinite completion $\hat{\Gamma}$.

A final number theoretic example

Let $\bar{\mathbb{Q}}$ be the *algebraic closure* of $\mathbb{Q}$:

$$\bar{\mathbb{Q}} = \{\, \alpha \in \mathbb{C} \mid p(\alpha) = 0 \text{ for some } p \in \mathbb{Q}[X] \,\}$$

A final number theoretic example

Let $\bar{\mathbb{Q}}$ be the *algebraic closure* of $\mathbb{Q}$:

$$\begin{aligned}\bar{\mathbb{Q}} &= \{\, \alpha \in \mathbb{C} \mid p(\alpha) = 0 \text{ for some } p \in \mathbb{Q}[X] \,\} \\ &= \bigcup_{p \in \mathbb{Q}[X]} K_p\end{aligned}$$

where K_p is the splitting field of the polynomial p.

A final number theoretic example

Let $\bar{\mathbb{Q}}$ be the *algebraic closure* of $\mathbb{Q}$:

$$\begin{aligned}\bar{\mathbb{Q}} &= \{\, \alpha \in \mathbb{C} \mid p(\alpha) = 0 \text{ for some } p \in \mathbb{Q}[X] \,\} \\ &= \bigcup_{p \in \mathbb{Q}[X]} K_p\end{aligned}$$

where K_p is the splitting field of the polynomial p.
These splitting fields K form a directed set.

A final number theoretic example

Let $\bar{\mathbb{Q}}$ be the *algebraic closure* of $\mathbb{Q}$:

$$\begin{aligned}\bar{\mathbb{Q}} &= \{\, \alpha \in \mathbb{C} \mid p(\alpha) = 0 \text{ for some } p \in \mathbb{Q}[X] \,\} \\ &= \bigcup_{p \in \mathbb{Q}[X]} K_p\end{aligned}$$

where K_p is the splitting field of the polynomial p.
These splitting fields K form a directed set.
An automorphism ϕ of $\bar{\mathbb{Q}}$ is determined by its effect on all the splitting fields.

A final number theoretic example

Let $\bar{\mathbb{Q}}$ be the *algebraic closure* of $\mathbb{Q}$:

$$\begin{aligned}\bar{\mathbb{Q}} &= \{\, \alpha \in \mathbb{C} \mid p(\alpha) = 0 \text{ for some } p \in \mathbb{Q}[X] \,\} \\ &= \bigcup_{p \in \mathbb{Q}[X]} K_p\end{aligned}$$

where K_p is the splitting field of the polynomial p.
These splitting fields K form a directed set.
An automorphism ϕ of $\bar{\mathbb{Q}}$ is determined by its effect on all the splitting fields.
Thus

$$\phi \mapsto (\phi|_K)$$

is an isomorphism

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(K/\mathbb{Q}),$$

so the absolute Galois group is a profinite group.

A final number theoretic example

Let $\bar{\mathbb{Q}}$ be the *algebraic closure* of $\mathbb{Q}$:

$$\begin{aligned}\bar{\mathbb{Q}} &= \{\, \alpha \in \mathbb{C} \mid p(\alpha) = 0 \text{ for some } p \in \mathbb{Q}[X] \,\} \\ &= \bigcup_{p \in \mathbb{Q}[X]} K_p\end{aligned}$$

where K_p is the splitting field of the polynomial p.
These splitting fields K form a directed set.
An automorphism ϕ of $\bar{\mathbb{Q}}$ is determined by its effect on all the splitting fields.
Thus

$$\phi \mapsto (\phi|_K)$$

is an isomorphism

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(K/\mathbb{Q}),$$

so the absolute Galois group is a profinite group.

Further reading

- J. D. Dixon, M. P. F. du Sautoy, A. Mann & D. Segal, *Analytic pro-p groups, 2nd edition*, Cambridge studies in advanced math. **61** (CUP, 1999)
- Luis Ribes & Pavel Zalesskii, *Profinite groups*, Ergebnisse der Math. **40** (Springer, 2000)
- John S. Wilson, *Profinite groups*, LMS Monographs **19** (OUP, 1998)