Construction of number fields with solvable Galois group

Carlo Sircana

09/07/2020,
IRTG Seminar

The problem

Inverse Galois problem

Given a finite group G, decide whether there exists a number field K such that $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Shafarevich's theorem

Let G be a solvable group. There exists a number field K such that $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Aim

Construct number fields with a given solvable Galois group G.

Galois fields

A number field K is a finite field extension of $\mathbf{Q}$.

We represent a number field via a primitive element $\alpha \in K$ such that $K = \mathbf{Q}(\alpha)$. If f is the minimal polynomial of α, K can be represented as $\mathbf{Q}[x]/(f(x))$.

Galois fields

A number field K is a finite field extension of $\mathbf{Q}$.

We represent a number field via a primitive element $\alpha \in K$ such that $K = \mathbf{Q}(\alpha)$. If f is the minimal polynomial of α, K can be represented as $\mathbf{Q}[x]/(f(x))$.

Galois field

A number field $K = \mathbf{Q}[x]/(f(x))$ is a Galois field if $f(t) \in K[t]$ is a product of linear polynomials $f(t) = \prod_{i=1}^{n}(x - \alpha_i)$.

Every root corresponds to an automorphism of K

$$\begin{array}{rccc} \varphi_i\colon & K & \to & K \\ & \alpha & \to & \alpha_i \end{array}$$

If K is a Galois field, $\mathrm{Aut}(K)$ is called the Galois group $\mathrm{Gal}(K/\mathbf{Q})$.

A pure cubic field

$K = \mathbf{Q}[x]/(x^3 - 2) = \mathbf{Q}(\alpha)$ is not Galois, because

$$t^3 - 2 = (t - \alpha)(t^2 + \alpha t + \alpha^2) \in K[t]$$

has only one root in K.

Cyclotomic field of order 5

$K = \mathbf{Q}(\alpha) = \mathbf{Q}[x]/(x^4 + x^3 + x^2 + x + 1)$ is a Galois field, since

$$t^4 + t^3 + t^2 + t + 1 = \prod_{i=1}^{4} (t - \alpha^i) \in K[t].$$

The Galois group is given by $\varphi_i(\alpha) = \alpha^i$ for $i \in \{1, \ldots, 4\}$ and it is cyclic, generated by φ_2.

Galois correspondence

Let K be a number field and let $f \in K[x]$ be an irreducible polynomial. Then $L = K[x]/(f)$ is a number field.

Galois extension

$L = K(\alpha)$ is a Galois extension of K if the minimal polynomial of α splits into linear factors over L.

We denote by $\mathrm{Gal}(L/K)$ the automorphism group of L/K.

Galois correspondence

Let K be a number field and let $f \in K[x]$ be an irreducible polynomial. Then $L = K[x]/(f)$ is a number field.

Galois extension

$L = K(\alpha)$ is a Galois extension of K if the minimal polynomial of α splits into linear factors over L.

We denote by $\mathrm{Gal}(L/K)$ the automorphism group of L/K.

Galois correspondence

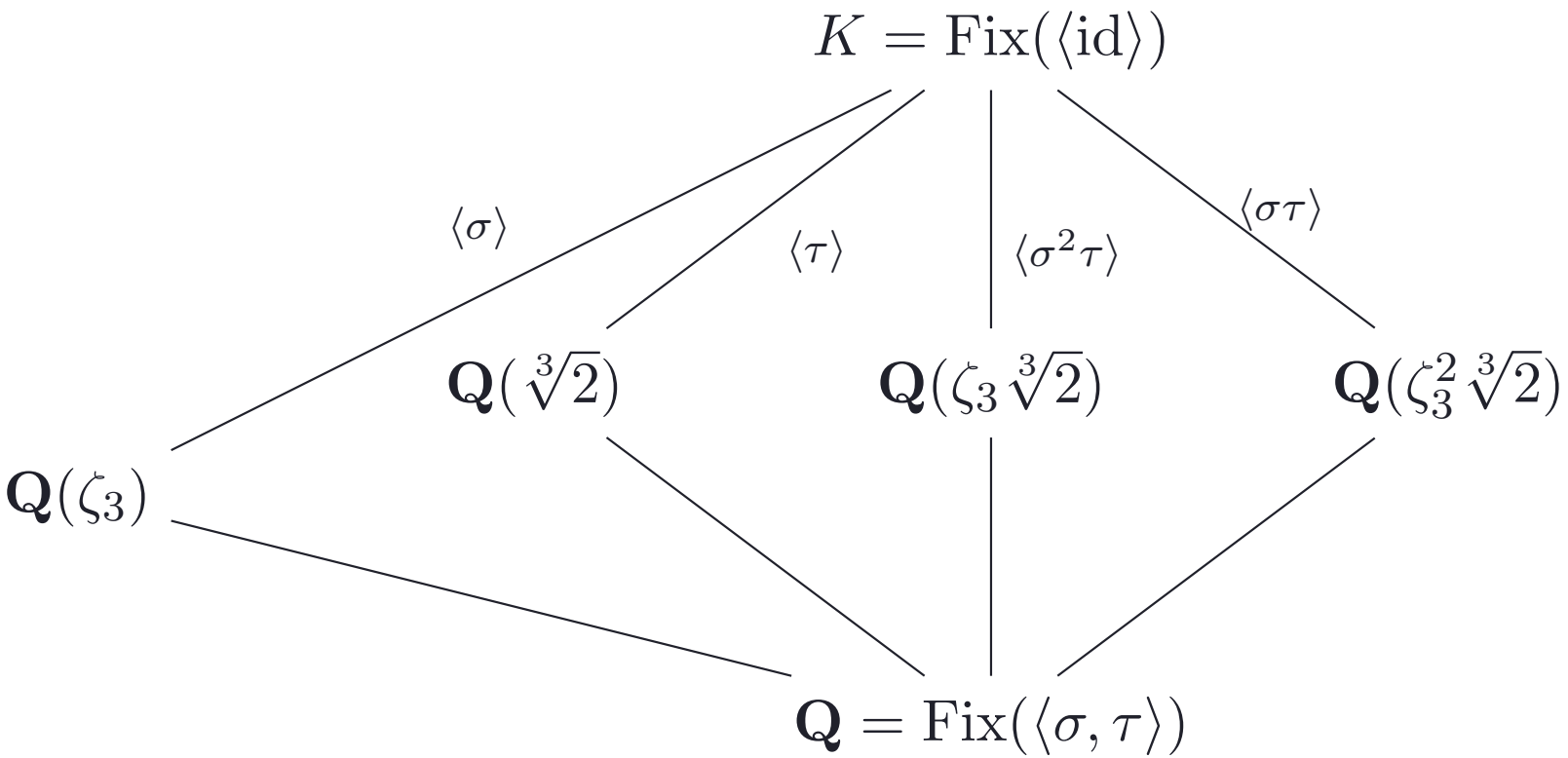
$$\begin{array}{ccc} \{\text{subgroups of } \mathrm{Gal}(L/K)\} & \longrightarrow & \{\text{subextensions of } L/K\} \\ H & \longmapsto & \mathrm{Fix}(H) \\ \mathrm{Gal}(L/F) & \longleftarrow & F \end{array}$$

If $N \lhd \mathrm{Gal}(L/K)$, then $F = \mathrm{Fix}(N)$ is a Galois extension of K with $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K)/N$.

S_3 field

The field $K = \mathbf{Q}(\zeta_3, \sqrt[3]{2})$ has Galois group $G \simeq S_3$.

$$\begin{array}{rccc} \sigma\colon & K & \longrightarrow & K \\ & \sqrt[3]{2} & \longmapsto & \zeta_3\sqrt[3]{2} \\ & \zeta_3 & \longmapsto & \zeta_3 \end{array} \qquad \begin{array}{rccc} \tau\colon & K & \longrightarrow & K \\ & \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \\ & \zeta_3 & \longmapsto & \zeta_3^2 \end{array}$$



Solvable groups

Derived Subgroup

Let G be a group. The derived subgroup G' is the subgroup generated by the elements of the form $aba^{-1}b^{-1}$ for $a, b \in G$.

G/G' is abelian and G' is the smallest subgroup with this property.

Solvable groups

Derived Subgroup

Let G be a group. The derived subgroup G' is the subgroup generated by the elements of the form $aba^{-1}b^{-1}$ for $a, b \in G$.

G/G' is abelian and G' is the smallest subgroup with this property.

Solvable Group

Let G be a finite group and consider the series of subgroups

$$\begin{cases} G_0 = G' \\ G_{i+1} = G_i' \end{cases}$$

G is called solvable if eventually $G_i = \{e\}$.

Dihedral group

Every dihedral group D_n is solvable. We consider it as generated by two elements r, s such that $r^n = e$, $s^2 = e$ and $rs = sr^{-1}$. The derived subgroup is generated by r^2 and we get the series:

$$D_n \triangleright \langle r^2 \rangle \triangleright \{e\}$$

Symmetric group

The symmetric group S_n is not solvable for $n \geq 5$. The derived subgroup is A_n, which is non-abelian and simple, so $(A_n)' = A_n$. The derived series is therefore

$$S_n \triangleright A_n = A_n = \dots$$

Let K be a field with $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Tower of fields	**Derived series**
K	$\{e\}$
$\vert$	$\vert$
$K_{n-1} = \mathrm{Fix}(G_{n-1})$	$G_{n-1} = G'_{n-2}$
$\vert$	$\vert$
$\vdots$	$\vdots$
$K_1 = \mathrm{Fix}(G_1)$	$G_1 = G'$
$\vert$	$\vert$
$\mathbf{Q}$	G

Let K be a field with $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Tower of fields	**Derived series**
K	$\{e\}$
$\vert$	$\vert$
$K_{n-1} = \mathrm{Fix}(G_{n-1})$	$G_{n-1} = G'_{n-2}$
$\vert$	$\vert$
$\vdots$	$\vdots$
$K_1 = \mathrm{Fix}(G_1)$	$G_1 = G'$
$\vert$	$\vert$
$\mathbf{Q}$	G

The Galois group of the intermediate extensions is

$$\mathrm{Gal}(K_i/K_{i-1}) \simeq G_{i-1}/G_i$$

Let K be a field with $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Tower of fields	**Derived series**
K	$\{e\}$
$\vert$	$\vert$
$K_{n-1} = \mathrm{Fix}(G_{n-1})$	$G_{n-1} = G'_{n-2}$
$\vert$	$\vert$
$\vdots$	$\vdots$
$K_1 = \mathrm{Fix}(G_1)$	$G_1 = G'$
$\vert$	$\vert$
$\mathbf{Q}$	G

The Galois group of the intermediate extensions is

$$\mathrm{Gal}(K_i/K_{i-1}) \simeq G_{i-1}/G_i \leftarrow \text{Abelian!}$$

General strategy

1. Compute the derived series $\{G_i\}_{i\in\{0,\dots,n\}}$ of G

General strategy

1. Compute the derived series $\{G_i\}_{i\in\{0,\dots,n\}}$ of G
2. Construct $H = G/G_{n-1}$.

General strategy

1. Compute the derived series $\{G_i\}_{i\in\{0,\dots,n\}}$ of G
2. Construct $H = G/G_{n-1}$.
3. Compute recursively the set S of number fields with Galois group H.

General strategy

1. Compute the derived series $\{G_i\}_{i\in\{0,\dots,n\}}$ of G
2. Construct $H = G/G_{n-1}$.
3. Compute recursively the set S of number fields with Galois group H.
4. For every field K in S,

General strategy

1. Compute the derived series $\{G_i\}_{i\in\{0,\dots,n\}}$ of G
2. Construct $H = G/G_{n-1}$.
3. Compute recursively the set S of number fields with Galois group H.
4. For every field K in S,
   - Compute the set S_K of abelian extensions of K with Galois group over K isomorphic to G_{n-1}/G_n.

General strategy

1. Compute the derived series $\{G_i\}_{i\in\{0,\dots,n\}}$ of G
2. Construct $H = G/G_{n-1}$.
3. Compute recursively the set S of number fields with Galois group H.
4. For every field K in S,
   - Compute the set S_K of abelian extensions of K with Galois group over K isomorphic to G_{n-1}/G_n.
   - Find the subset of S_K given by the number field with Galois group isomorphic to G.

Dihedral extensions

Task

Construct number fields with Galois group D_4.

- The derived series of D_4 is

$$D_4 \triangleright \langle r^2 \rangle \triangleright \{e\}$$

Dihedral extensions

Task

Construct number fields with Galois group D_4.

- The derived series of D_4 is

$$D_4 \triangleright \langle r^2 \rangle \triangleright \{e\}$$

- Construct number fields with Galois group isomorphic to $D_4/\langle r^2 \rangle \simeq C_2 \times C_2$.

Dihedral extensions

Task

Construct number fields with Galois group D_4.

- The derived series of D_4 is

$$D_4 \triangleright \langle r^2 \rangle \triangleright \{e\}$$

- Construct number fields with Galois group isomorphic to $D_4/\langle r^2 \rangle \simeq C_2 \times C_2$.
- Extend every number field K obtained in the first step with number fields with Galois group over K isomorphic to $C_2 \simeq \langle r^2 \rangle$.

Dihedral extensions

Task

Construct number fields with Galois group D_4.

- The derived series of D_4 is

$$D_4 \triangleright \langle r^2 \rangle \triangleright \{e\}$$

- Construct number fields with Galois group isomorphic to $D_4/\langle r^2 \rangle \simeq C_2 \times C_2$.
- Extend every number field K obtained in the first step with number fields with Galois group over K isomorphic to $C_2 \simeq \langle r^2 \rangle$.
- Determine the number fields with Galois group over $\mathbf{Q}$ isomorphic to D_4.

Dihedral extensions

Task

Construct number fields with Galois group D_4.

- The derived series of D_4 is

$$D_4 \triangleright \langle r^2 \rangle \triangleright \{e\}$$

- Construct number fields with Galois group isomorphic to $D_4/\langle r^2 \rangle \simeq C_2 \times C_2$. ← infinitely many!
- Extend every number field K obtained in the first step with number fields with Galois group over K isomorphic to $C_2 \simeq \langle r^2 \rangle$.
- Determine the number fields with Galois group over $\mathbf{Q}$ isomorphic to D_4.

Ring of integers

Ring of integers

Let K be a number field. The ring of integers $\mathcal{O}_K$ is the subring of K given by the elements whose (monic) minimal polynomial lies in $\mathbf{Z}[x]$.

It is a free $\mathbf{Z}$-module of rank equal to the degree of K.

Ring of integers

Ring of integers

Let K be a number field. The ring of integers $\mathcal{O}_K$ is the subring of K given by the elements whose (monic) minimal polynomial lies in $\mathbf{Z}[x]$.

It is a free $\mathbf{Z}$-module of rank equal to the degree of K.

Let $K = \mathbf{Q}(\sqrt{5})$. Then $\mathbf{Z}[\sqrt{5}] \subseteq \mathcal{O}_K$. The minimal polynomial of $\beta = (1+\sqrt{5})/2$ is

$$f_\beta = x^2 - x - 1$$

so $\beta \in \mathcal{O}_K$.

Minkowski map

Given $K = \mathbf{Q}(\alpha) = \mathbf{Q}[x]/(f)$, let $f = \prod_{i=1}^{n}(x - \alpha_i)$ be the factorization of f over $\mathbf{C}$.

$$\begin{array}{rccc} \sigma_i\colon & K & \longrightarrow & \mathbf{C} \\ & \alpha & \longmapsto & \alpha_i \end{array}$$

All together, we have an embedding

$$\begin{array}{rccc} \sigma\colon & K & \longrightarrow & \mathbf{C}^n \\ & \beta & \longmapsto & (\sigma_1(\beta), \ldots, \sigma_n(\beta)) \end{array}$$

Discriminant

Let $x_1, \ldots, x_n$ be a $\mathbf{Z}$-basis of $\mathcal{O}_K$. The discriminant of the field K is defined as $\det M^2$, where M is the matrix with entries $M_{ij} = \sigma_i(x_j)$.

Minkowski embedding

We order the embeddings: $\sigma_1, \dots, \sigma_r$ are the embedding whose image is contained in $\mathbf{R}$, $\sigma_{r+1}, \bar{\sigma}_{r+1}, \dots, \sigma_{r+2s-1}, \bar{\sigma}_{r+2s-1}$ the others. The Minkowski embedding $\sigma_K \colon K \to \mathbf{R}^n$ is

$$\begin{aligned}\beta \to (&\sigma_1(\beta), \dots, \sigma_r(\beta),\\ &\Re(\sigma_{r+1}(\beta)), \Im(\sigma_{r+1}(\beta)), \dots, \Re(\sigma_{r+s}(\beta)), \Im(\sigma_{r+s}(\beta)))\end{aligned}$$

The image of the ring of integers $\mathcal{O}_K$ via the Minkowski embedding σ is a lattice in $\mathbf{R}^n$.

Proposition

$$|\operatorname{disc} K| = 2^{2s} \operatorname{Vol}(\sigma_K(\mathcal{O}_K))$$

Minkowski embedding

We order the embeddings: $\sigma_1, \dots, \sigma_r$ are the embedding whose image is contained in $\mathbf{R}$, $\sigma_{r+1}, \bar{\sigma}_{r+1}, \dots, \sigma_{r+2s-1}, \bar{\sigma}_{r+2s-1}$ the others. The Minkowski embedding $\sigma_K \colon K \to \mathbf{R}^n$ is

$$\begin{aligned}\beta \to (&\sigma_1(\beta), \dots, \sigma_r(\beta), \\ &\Re(\sigma_{r+1}(\beta)), \Im(\sigma_{r+1}(\beta)), \dots, \Re(\sigma_{r+s}(\beta)), \Im(\sigma_{r+s}(\beta)))\end{aligned}$$

Hermite's theorem

Let B be a positive integer. There are only finitely many number fields K with $|\operatorname{disc}(K)| < B$.

Task

Given a solvable group G, find all the number fields with Galois group isomorphic to G and with absolute discriminant bounded by B.

Task

Given a solvable group G, find all the number fields with Galois group isomorphic to G and with absolute discriminant bounded by B.

Related problems: find

- a number field with Galois group G;

Task

Given a solvable group G, find all the number fields with Galois group isomorphic to G and with absolute discriminant bounded by B.

Related problems: find

- a number field with Galois group G;
- fields with minimal discriminant;

Task

Given a solvable group G, find all the number fields with Galois group isomorphic to G and with absolute discriminant bounded by B.

Related problems: find

- a number field with Galois group G;
- fields with minimal discriminant;
- fields with prescribed ramification.

Size of the primitive element

The size of the primitive element influences the performance.

Example

The following polynomials define the same number field:

$$f = x^4 + 220x^3 + 20038x^2 + 884652x + 15744357$$

$$g = x^4 - 2x^3 + 115x^2 - 114x + 3966$$

Size of the primitive element

The size of the primitive element influences the performance.

Example

The following polynomials define the same number field:

$$f = x^4 + 220x^3 + 20038x^2 + 884652x + 15744357$$

$$g = x^4 - 2x^3 + 115x^2 - 114x + 3966$$

Post-computation reduction

A "small" primitive element corresponds to a "short" vector in the image of the Minkowski embedding. Via the LLL algorithm, we can find short vectors in a lattice.

During the computation...

The primitive element of a cyclic extension L/K comes from the choice of a primitive element for $L(\zeta_n)/K(\zeta_n)$.

Kummer theory

A cyclic extension of degree n of $K(\zeta_n)$ can be generated by $\sqrt[n]{\gamma}$ with $\gamma \in K(\zeta_n)$.

Such a γ can be chosen up to n-th powers of $K(\zeta_n)$.

Compact presentation

The compact presentation allows us to take a representative of $[\gamma] \in K(\zeta_n)^\times/(K(\zeta_n)^\times)^n$ of bounded size.

Class field theory

We can effectively parametrize abelian extensions of K in terms of objects in K.

Additional hypothesis

We search for abelian extensions of K that are Galois fields.

The algorithm can be specialized to exploit the action of $\mathrm{Gal}(K/\mathbf{Q})$ on the ideals of $\mathcal{O}_K$.

Subproblem

Let A be a finite abelian group and let G be a group acting on A. Find all the subgroups of A that are invariant under the action of G.

Approach: consider the structure of $\mathbf{Z}/n\mathbf{Z}[G]$-module on A.

Control over the Galois group

The Galois group $\mathrm{Gal}(L/\mathbf{Q})$ of an abelian extension L of K might be not what we want.

Let $K = \mathbf{Q}(\zeta_3)$. Then $L_1 = K(\sqrt[3]{2})$ is an abelian extension of K with Galois group S_3. On the other hand, $L_2 = K(\zeta_7 + \zeta_7^{-1})$ has Galois group C_6.

Control over the Galois group

The Galois group $\mathrm{Gal}(L/\mathbf{Q})$ of an abelian extension L of K might be not what we want.

Let $K = \mathbf{Q}(\zeta_3)$. Then $L_1 = K(\sqrt[3]{2})$ is an abelian extension of K with Galois group S_3. On the other hand, $L_2 = K(\zeta_7 + \zeta_7^{-1})$ has Galois group C_6.

The extension of fields induces an exact sequence

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) \to 1$$

Split extensions

If $[L : K]$ and $[K : \mathbf{Q}]$ are coprime, $\mathrm{Gal}(L/\mathbf{Q})$ is uniquely determined by the action of $\mathrm{Gal}(K/\mathbf{Q})$ on $\mathrm{Gal}(L/K)$.

Obstructions

Given a number field K with Galois group G, we want to find extensions of K with Galois group $\tilde{G}$.

Obstructions

Given a number field K with Galois group G, we want to find extensions of K with Galois group $\tilde{G}$.

In general, impossible!

Obstructions

Given a number field K with Galois group G, we want to find extensions of K with Galois group $\tilde{G}$.

In general, impossible!

C_4 extensions

Let $K = \mathbf{Q}(\sqrt{a})$ be a quadratic field. Then there exists a C_4 field containing K if and only if there exist $\alpha, \beta \in \mathbf{Q}$ such that $a = \alpha^2 + \beta^2$.

$\mathbf{Q}(\sqrt{2})$ can be embedded into a C_4-extension, while this is impossible for $\mathbf{Q}(\sqrt{3})$.

Obstructions

Given a number field K with Galois group G, we want to find extensions of K with Galois group $\tilde{G}$.

In general, impossible!

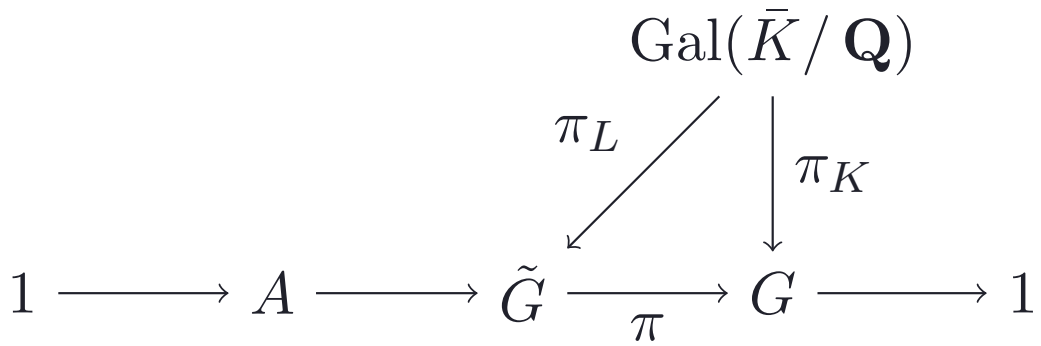
Embedding problem

Let K be a number field with Galois group G. Let $\tilde{G}$ be a finite group and let A be an abelian subgroup of $\tilde{G}$. An embedding problem for $\tilde{G}$ over K is a short exact sequence

$$1 \to A \to \tilde{G} \to G \to 1$$

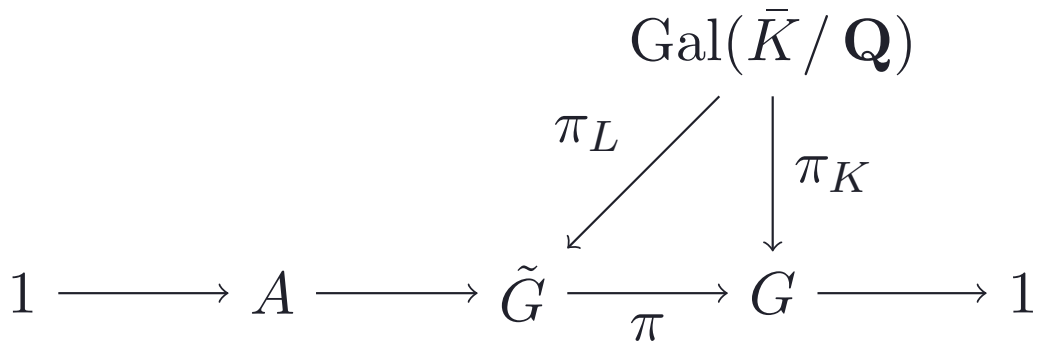
Solvability

Suppose that there exists a Galois field L with Galois group $\tilde{G}$ such that the restriction $\mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ coincides with the map $\tilde{G} \to G$ of the embedding problem.



Solvability

Suppose that there exists a Galois field L with Galois group $\tilde{G}$ such that the restriction $\mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ coincides with the map $\tilde{G} \to G$ of the embedding problem.



Solvability

The embedding problem is solvable if there exists a map $\varphi\colon\ \mathrm{Gal}(\bar{K}/\mathbf{Q}) \to \tilde{G}$ that makes the diagram commute.

Brauer problems

Brauer embedding problem

An embedding problem is said to be of Brauer type if $\zeta_n \in K$ and $A \simeq \langle \zeta_n \rangle$ as a $\mathbf{Z}[G]$-module.

The inclusion $\zeta_n \to K^\times$ induces the following:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle \zeta_n \rangle & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Brauer criterion

The embedding problem is solvable if and only if the induced extension of G by $K^\times$ splits, i.e. $E \simeq K^\times \rtimes G$.

Global to local

$K^\times$ is not finitely generated, so we can't easily decide (algorithmically) if the extension splits.

Global to local

$K^\times$ is not finitely generated, so we can't easily decide (algorithmically) if the extension splits.

Let $K = \mathbf{Q}(\sqrt{2})$ and assume we want to solve the embedding problem over K

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

The completion of K at 7 is the 7-adic field $\mathbf{Q}_7$. Since the local Galois group is trivial, the embedding problem is solvable over $\mathbf{Q}_7$.

Global to local

$K^\times$ is not finitely generated, so we can't easily decide (algorithmically) if the extension splits.

Let $K = \mathbf{Q}(\sqrt{2})$ and assume we want to solve the embedding problem over K

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

The completion of K at 2 is the 2-adic field $\mathbf{Q}_2(\sqrt{2})$. Not so easy in this case.

Global to local

$K^\times$ is not finitely generated, so we can't easily decide (algorithmically) if the extension splits.

Algorithm

The reduction to the local case is trivial for most primes. For the (finite) remaining primes, we have an algorithm to check whether the embedding problems of Brauer type are solvable.

Summarizing...

We have an algorithm that constructs number fields with a given Galois group (solvable).

- Returns polynomials defining the fields of reasonable size.
- Constructs only a "few" subfields during the search.
- Computes the obstructions existing for the intermediate extensions.

Summarizing...

We have an algorithm that constructs number fields with a given Galois group (solvable).

- Returns polynomials defining the fields of reasonable size.
- Constructs only a "few" subfields during the search.
- Computes the obstructions existing for the intermediate extensions.

Thanks for your attention!