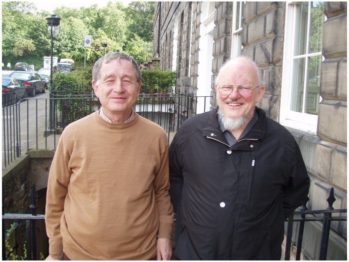
Composita of symmetric extensions of $\mathbb{Q}$

W.D. Geyer M. Jarden A. Razon



MSRI definability seminar - 18 November 2020

Outline

1. Group Theory
   - What and why
   - The formation $\mathcal{F}$ of subdirect products of symmetric groups
   - The embedding property: Realization of $G \in \mathcal{F}$ as a Galois group
   - Free pro-$\mathcal{F}$-groups: A theorem of Iwasawa (group theory)
2. Application to Arithmetical Field Theory
   - Galois groups
   - Theorem of Iwasawa (number theory)
   - The field $\mathbb{Q}_{\mathrm{symm}}$

Outline

Motivation

The focus of our work is the study of the field K_{symm}, the compositum of all finite Galois extensions of a field K with Galois group a symmetric group.

For $K = \mathbb{Q}$ we can describe explicitly the groups $\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}_{\mathrm{symm}})$ and $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$.

Moreover, the theory $\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}})$ of $\mathbb{Q}_{\mathrm{symm}}$ in the first order language of rings is primitive recursively decidable.

Motivation

The focus of our work is the study of the field K_{symm}, the compositum of all finite Galois extensions of a field K with Galois group a symmetric group.

For $K = \mathbb{Q}$ we can describe explicitly the groups $\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}_{\mathrm{symm}})$ and $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$.

Moreover, the theory $\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}})$ of $\mathbb{Q}_{\mathrm{symm}}$ in the first order language of rings is primitive recursively decidable.

Motivation

The focus of our work is the study of the field K_{symm}, the compositum of all finite Galois extensions of a field K with Galois group a symmetric group.

For $K = \mathbb{Q}$ we can describe explicitly the groups $\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}_{\mathrm{symm}})$ and $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$.

Moreover, the theory $\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}})$ of $\mathbb{Q}_{\mathrm{symm}}$ in the first order language of rings is primitive recursively decidable.

Properties of the base field

Remark 1

We need only the following properties of $\mathbb{Q}$:

- $\mathbb{Q}$ is **Hilbertian**, i.e. the following holds: If $f \in \mathbb{Q}[X, Y]$ is an irreducible polynomial, separable, monic, and of degree at least 2 in Y, then there is $x \in \mathbb{Q}$ such that $f(x, Y) \in \mathbb{Q}[Y]$ is irreducible [FrJ08, Prop. 13.2.2].
- $\mathbb{Q}$ is countable.
- $\operatorname{char} \mathbb{Q} \neq 2$.

All infinite fields (of characteristic $\neq 2$) which are finitely generated over their prime fields have these properties.

Properties of the base field

Remark 1

We need only the following properties of $\mathbb{Q}$:

- $\mathbb{Q}$ is **Hilbertian**, i.e. the following holds: If $f \in \mathbb{Q}[X, Y]$ is an irreducible polynomial, separable, monic, and of degree at least 2 in Y, then there is $x \in \mathbb{Q}$ such that $f(x, Y) \in \mathbb{Q}[Y]$ is irreducible [FrJ08, Prop. 13.2.2].
- $\mathbb{Q}$ is countable.
- $\operatorname{char} \mathbb{Q} \neq 2$.

All infinite fields (of characteristic $\neq 2$) which are finitely generated over their prime fields have these properties.

Properties of the base field

Remark 1

We need only the following properties of $\mathbb{Q}$:

- $\mathbb{Q}$ is **Hilbertian**, i.e. the following holds: If $f \in \mathbb{Q}[X, Y]$ is an irreducible polynomial, separable, monic, and of degree at least 2 in Y, then there is $x \in \mathbb{Q}$ such that $f(x, Y) \in \mathbb{Q}[Y]$ is irreducible [FrJ08, Prop. 13.2.2].
- $\mathbb{Q}$ is countable.
- $\operatorname{char} \mathbb{Q} \neq 2$.

All infinite fields (of characteristic $\neq 2$) which are finitely generated over their prime fields have these properties.

Properties of the base field

Remark 1

We need only the following properties of $\mathbb{Q}$:

- $\mathbb{Q}$ is **Hilbertian**, i.e. the following holds: If $f \in \mathbb{Q}[X, Y]$ is an irreducible polynomial, separable, monic, and of degree at least 2 in Y, then there is $x \in \mathbb{Q}$ such that $f(x, Y) \in \mathbb{Q}[Y]$ is irreducible [FrJ08, Prop. 13.2.2].
- $\mathbb{Q}$ is countable.
- $\mathrm{char}\,\mathbb{Q} \neq 2$.

All infinite fields (of characteristic $\neq 2$) which are finitely generated over their prime fields have these properties.

Properties of the base field

Remark 1

We need only the following properties of $\mathbb{Q}$:

- $\mathbb{Q}$ is **Hilbertian**, i.e. the following holds: If $f \in \mathbb{Q}[X, Y]$ is an irreducible polynomial, separable, monic, and of degree at least 2 in Y, then there is $x \in \mathbb{Q}$ such that $f(x, Y) \in \mathbb{Q}[Y]$ is irreducible [FrJ08, Prop. 13.2.2].
- $\mathbb{Q}$ is countable.
- $\mathrm{char}\,\mathbb{Q} \neq 2$.

All infinite fields (of characteristic $\neq 2$) which are finitely generated over their prime fields have these properties.

Subdirect product of symmetric groups

Remark 2

Let K be a field and L_i/K be Galois extensions with $\mathrm{Gal}(L_i/K) = \mathfrak{S}_{n_i}$. Let $L = L_1 \cdots L_r$. Then

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_{i=1}^{r} \mathrm{Gal}(L_i/K)$$

is a subdirect product of symmetric groups.

Subdirect product of symmetric groups

Definition (Birkhoff 1944)

A finite group G is a **subdirect product of symmetric groups** ($G \in \mathcal{F} = \mathcal{F}_{\mathrm{symm}}$), if there is an embedding

$$G \hookrightarrow S = \prod_{i=1}^{r} \mathfrak{S}_{n_i} \quad \text{with} \quad \mathrm{pr}_i(G) = \mathfrak{S}_{n_i} \tag{1}$$

We call such a presentation **minimal**, if r is minimal and $|S|$ is minimal. Such a minimal presentation is (up to reordering the factors) unique.

Minimal normal subgroup of $\mathfrak{S}_n$

Proposition

Let $1 \neq G \in \mathcal{F}$ and (1) minimal. Then $G_i = G \cap \mathfrak{S}_{n_i}$ is $\neq 1$ and normal in G and $\mathfrak{S}_{n_i}$. So

$$G_i \geq \mathfrak{A}_{(n_i)} = \left\{ \begin{array}{ll} \mathfrak{S}_2 & \text{if } n_i = 2 \\ \mathfrak{V}_4 & \text{if } n_i = 4 \\ \mathfrak{A}_{n_i} & \text{otherwise} \end{array} \right\} = \begin{array}{l} \text{minimal normal subgroup} \\ \text{of } \mathfrak{S}_{n_i} \end{array}$$

Here $\mathfrak{V}_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ is the **Klein four-group**.

Hence $S \geq G \geq A = \prod_{i=1}^{r} \mathfrak{A}_{(n_i)}$ *with* $S/A = \mathfrak{S}_2^u \times \mathfrak{S}_3^v$.

Structure of $G \in \mathcal{F}$

Corollary

$$G = H \ltimes A\,, \quad H = H_2 \ltimes H_3$$

where H_2 and H_3 are the elementary abelian p-Sylow subgroups of H for $p = 2$ and $p = 3$, respectively.

Outline

1. Group Theory
   - What and why
   - The formation $\mathcal{F}$ of subdirect products of symmetric groups
   - The embedding property: Realization of $G \in \mathcal{F}$ as a Galois group
   - Free pro-$\mathcal{F}$-groups: A theorem of Iwasawa (group theory)
2. Application to Arithmetical Field Theory
   - Galois groups
   - Theorem of Iwasawa (number theory)
   - The field $\mathbb{Q}_{\mathrm{symm}}$

Formation

Definition

A non empty class $\mathcal{F}$ of finite groups is called a **formation** if the following holds:

$$N \trianglelefteq G \in \mathcal{F} \implies G/N \in \mathcal{F}$$

$$G/N_1, G/N_2 \in \mathcal{F} \implies G/(N_1 \cap N_2) \in \mathcal{F}$$

Proposition

$\mathcal{F} = \mathcal{F}_{\mathrm{symm}}$ *is a formation, the smallest formation containing all symmetric groups.*

Formation

Definition

A non empty class $\mathcal{F}$ of finite groups is called a **formation** if the following holds:

$$N \trianglelefteq G \in \mathcal{F} \implies G/N \in \mathcal{F}$$

$$G/N_1, G/N_2 \in \mathcal{F} \implies G/(N_1 \cap N_2) \in \mathcal{F}$$

Proposition

$\mathcal{F} = \mathcal{F}_{\mathrm{symm}}$ is a formation, the smallest formation containing all symmetric groups.

Proof

Step 1

$\mathcal{F}$ is closed under fiber products:

$$G/N_1 \hookrightarrow \prod_i \mathfrak{S}_{n_i}\,, \quad G/N_2 \hookrightarrow \prod_j \mathfrak{S}_{m_j}$$

$$\Rightarrow \quad G/(N_1 \cap N_2) \hookrightarrow \prod_i \mathfrak{S}_{n_i} \times \prod_j \mathfrak{S}_{m_j}$$

Step 2

$\mathcal{F}$ is closed under taking quotients.
Sketch of proof: It is enough to assume N is minimal.

Proof

Step 1

$\mathcal{F}$ is closed under fiber products:

$$G/N_1 \hookrightarrow \prod_i \mathfrak{S}_{n_i}\,, \qquad G/N_2 \hookrightarrow \prod_j \mathfrak{S}_{m_j}$$

$$\Rightarrow \quad G/(N_1 \cap N_2) \hookrightarrow \prod_i \mathfrak{S}_{n_i} \times \prod_j \mathfrak{S}_{m_j}$$

Step 2

$\mathcal{F}$ is closed under taking quotients.
Sketch of proof: It is enough to assume N is minimal.

Lemma

Lemma

Let $G \in \mathcal{F}$, say $G \leq \prod_{i \in I} \mathfrak{S}_{n_i}$. Then a minimal normal subgroup N of G is of the following form:

(i) $\exists i_0 \in I$: $N = \mathfrak{A}_{(n_{i_0})}$, *or*

(ii) $\exists J \subseteq I$ *with* $|J| = s > 1$, *and* $\exists m$: $2 \leq m \leq 4$ *such that* $n_j = m$ *for* $j \in J$ *and*

$$N = \{(\alpha, \ldots, \alpha) \in \mathfrak{A}^s_{(m)} \mid \alpha \in \mathfrak{A}_{(m)}\}$$

up to an automorphism of S.

Lemma

Lemma

Let $G \in \mathcal{F}$, say $G \leq \prod_{i \in I} \mathfrak{S}_{n_i}$. Then a minimal normal subgroup N of G is of the following form:

(i) $\exists i_0 \in I\colon \ N = \mathfrak{A}_{(n_{i_0})}$, *or*

(ii) $\exists J \subseteq I$ *with* $|J| = s > 1$, *and* $\exists m\colon \ 2 \leq m \leq 4$ *such that* $n_j = m$ *for* $j \in J$ *and*

$$N = \{(\alpha, \dots, \alpha) \in \mathfrak{A}^s_{(m)} \mid \alpha \in \mathfrak{A}_{(m)}\}$$

up to an automorphism of S.

Lemma

Lemma

Let $G \in \mathcal{F}$, say $G \leq \prod_{i\in I} \mathfrak{S}_{n_i}$. Then a minimal normal subgroup N of G is of the following form:

(i) $\exists i_0 \in I\colon\;\; N = \mathfrak{A}_{(n_{i_0})}$, *or*

(ii) $\exists J \subseteq I$ *with* $|J| = s > 1$, *and* $\exists m\colon\;\; 2 \leq m \leq 4$ *such that* $n_j = m$ *for* $j \in J$ *and*

$$N = \{(\alpha, \dots, \alpha) \in \mathfrak{A}^s_{(m)} \mid \alpha \in \mathfrak{A}_{(m)}\}$$

up to an automorphism of S.

Proof of the Lemma

Proof

N minimal, so $N_i := \mathrm{pr}_i(N) = 1$ or $= \mathfrak{A}_{(n_i)}$.

Let $J = \{i \in I \mid N_i \neq 1\}$. $|J| = 1$ is case (i).

Let $|J| > 1$. For $j \in J$ we have $\mathrm{pr}_j : N \xrightarrow{\cong} N_j$ since $N \cap \mathrm{Ker}(\mathrm{pr}_j) = 1$. So all $n_j = m$ and N has the above form, up to an automorphism of S.

If $m > 4$, then $\mathfrak{A}_m$ is not abelian, so N is not normal in A, so not in G. $\square$

Proof of the Lemma

Proof

N minimal, so $N_i := \mathrm{pr}_i(N) = 1$ or $= \mathfrak{A}_{(n_i)}$.

Let $J = \{i \in I \mid N_i \neq 1\}$. $|J| = 1$ is case (i).

Let $|J| > 1$. For $j \in J$ we have $\mathrm{pr}_j \colon N \xrightarrow{\cong} N_j$ since $N \cap \mathrm{Ker}(\mathrm{pr}_j) = 1$. So all $n_j = m$ and N has the above form, up to an automorphism of S.

If $m > 4$, then $\mathfrak{A}_m$ is not abelian, so N is not normal in A, so not in G. □

Proof of the Lemma

Proof

N minimal, so $N_i := \mathrm{pr}_i(N) = 1$ or $= \mathfrak{A}_{(n_i)}$.

Let $J = \{i \in I \mid N_i \neq 1\}$. $|J| = 1$ is case (i).

Let $|J| > 1$. For $j \in J$ we have $\mathrm{pr}_j\colon N \xrightarrow{\cong} N_j$ since $N \cap \mathrm{Ker}(\mathrm{pr}_j) = 1$. So all $n_j = m$ and N has the above form, up to an automorphism of S.

If $m > 4$, then $\mathfrak{A}_m$ is not abelian, so N is not normal in A, so not in G. □

Proof of the Lemma

Proof

N minimal, so $N_i := \mathrm{pr}_i(N) = 1$ or $= \mathfrak{A}_{(n_i)}$.

Let $J = \{i \in I \mid N_i \neq 1\}$. $|J| = 1$ is case (i).

Let $|J| > 1$. For $j \in J$ we have $\mathrm{pr}_j \colon N \xrightarrow{\cong} N_j$ since $N \cap \mathrm{Ker}(\mathrm{pr}_j) = 1$. So all $n_j = m$ and N has the above form, up to an automorphism of S.

If $m > 4$, then $\mathfrak{A}_m$ is not abelian, so N is not normal in A, so not in G. $\square$

Use of the lemma

Proof that G/N is a subdirect product of symmetric groups

In case (i) we have $G/N \hookrightarrow \prod_{i \neq i_0} \mathfrak{S}_{n_i} \times (\mathfrak{S}_{n_{i_0}}/\mathfrak{A}_{(n_{i_0})})$ and

$$\mathrm{Sgn}\colon \mathfrak{S}_n \to \mathfrak{S}_n/\mathfrak{A}_{(n)} = \left\{ \begin{array}{ll} \mathfrak{S}_3 & \text{if } n = 4 \\ \mathfrak{S}_1 & \text{if } n = 2 \\ \mathfrak{S}_2 & \text{otherwise} \end{array} \right\}$$

Moreover, $\mathfrak{S}_m/\mathfrak{A}_{(m)} = \mathrm{Aut}\,\mathfrak{A}_{(m)}$ for $m \leq 4$.

In case (ii) we assume $J = I$. The normalizer of N in S is

$$\{(\alpha_1, \dots, \alpha_s) \in \mathfrak{S}_m^s \mid \mathrm{Sgn}\,\alpha_1 = \cdots = \mathrm{Sgn}\,\alpha_s\} = G\,.$$

Then $G = M \ltimes N$ with $M = \{\alpha \in G \mid \alpha_1 \in \mathfrak{S}_{m-1}\}$, so $G/N \hookrightarrow \mathfrak{S}_{m-1} \times \mathfrak{S}_m^{s-1}$.

Use of the lemma

Proof that G/N is a subdirect product of symmetric groups

In case (i) we have $G/N \hookrightarrow \prod_{i \neq i_0} \mathfrak{S}_{n_i} \times (\mathfrak{S}_{n_{i_0}}/\mathfrak{A}_{(n_{i_0})})$ and

$$\mathrm{Sgn}\colon \mathfrak{S}_n \to \mathfrak{S}_n/\mathfrak{A}_{(n)} = \left\{ \begin{array}{ll} \mathfrak{S}_3 & \text{if } n = 4 \\ \mathfrak{S}_1 & \text{if } n = 2 \\ \mathfrak{S}_2 & \text{otherwise} \end{array} \right\}$$

Moreover, $\mathfrak{S}_m/\mathfrak{A}_{(m)} = \mathrm{Aut}\,\mathfrak{A}_{(m)}$ for $m \leq 4$.

In case (ii) we assume $J = I$. The normalizer of N in S is

$$\{(\alpha_1, \dots, \alpha_s) \in \mathfrak{S}_m^s \,|\, \mathrm{Sgn}\,\alpha_1 = \cdots = \mathrm{Sgn}\,\alpha_s\} = G.$$

Then $G = M \ltimes N$ with $M = \{\alpha \in G \,|\, \alpha_1 \in \mathfrak{S}_{m-1}\}$, so $G/N \hookrightarrow \mathfrak{S}_{m-1} \times \mathfrak{S}_m^{s-1}$. □

Use of the lemma

Proof that G/N is a subdirect product of symmetric groups

In case (i) we have $G/N \hookrightarrow \prod_{i \neq i_0} \mathfrak{S}_{n_i} \times (\mathfrak{S}_{n_{i_0}}/\mathfrak{A}_{(n_{i_0})})$ and

$$\mathrm{Sgn}\colon \mathfrak{S}_n \to \mathfrak{S}_n/\mathfrak{A}_{(n)} = \left\{ \begin{array}{ll} \mathfrak{S}_3 & \text{if } n = 4 \\ \mathfrak{S}_1 & \text{if } n = 2 \\ \mathfrak{S}_2 & \text{otherwise} \end{array} \right\}$$

Moreover, $\mathfrak{S}_m/\mathfrak{A}_{(m)} = \mathrm{Aut}\,\mathfrak{A}_{(m)}$ for $m \leq 4$.

In case (ii) we assume $J = I$. The normalizer of N in S is

$$\{(\alpha_1, \ldots, \alpha_s) \in \mathfrak{S}_m^s \mid \mathrm{Sgn}\,\alpha_1 = \cdots = \mathrm{Sgn}\,\alpha_s\} = G\,.$$

Then $G = M \ltimes N$ with $M = \{\boldsymbol{\alpha} \in G \mid \alpha_1 \in \mathfrak{S}_{m-1}\}$, so $G/N \hookrightarrow \mathfrak{S}_{m-1} \times \mathfrak{S}_m^{s-1}$. $\square$

A stronger result

Proposition (Geyer, Jarden, R. 2019) [GJR19, Prop. 4.4]

If N is a normal subgroup of some $G \in \mathcal{F}_{\mathrm{symm}}$, then N has a **complement** *M in G, i.e. $M \cap N = \mathbf{1}$ and $MN = G$. Moreover, $G/N \cong M \in \mathcal{F}_{\mathrm{symm}}$.*

Roots of polynomials in $\mathbb{Q}_{\mathrm{symm}}$

Corollary (Geyer, Jarden, R. 2019) [GJR19, Lemma 8.1]

We can effectively check whether a polynomial f in $\mathbb{Q}[X]$ has a root in $\mathbb{Q}_{\mathrm{symm}}$. Thus, the set of monic polynomials in $\mathbb{Q}[X]$ that have a root in $\mathbb{Q}_{\mathrm{symm}}$ is primitive recursive.

Proof

We can effectively decompose f over $\mathbb{Q}$ into a product of irreducible polynomials. Thus, we can assume that f is irreducible in $\mathbb{Q}[X]$ and effectively construct the splitting field N of f over $\mathbb{Q}$. Moreover, we can effectively find all symmetric extensions $L_1, \dots, L_r$ of $\mathbb{Q}$ in N and check whether $N = \prod_{i=1}^r L_i$ which is equivalent to $N \subset \mathbb{Q}_{\mathrm{symm}}$ since then $\mathrm{Gal}(N/\mathbb{Q})$ is a quotient of some $G \in \mathcal{F}_{\mathrm{symm}}$, hence in $\mathcal{F}_{\mathrm{symm}}$.

Roots of polynomials in $\mathbb{Q}_{\mathrm{symm}}$

Corollary (Geyer, Jarden, R. 2019) [GJR19, Lemma 8.1]

We can effectively check whether a polynomial f in $\mathbb{Q}[X]$ has a root in $\mathbb{Q}_{\mathrm{symm}}$. Thus, the set of monic polynomials in $\mathbb{Q}[X]$ that have a root in $\mathbb{Q}_{\mathrm{symm}}$ is primitive recursive.

Proof

We can effectively decompose f over $\mathbb{Q}$ into a product of irreducible polynomials. Thus, we can assume that f is irreducible in $\mathbb{Q}[X]$ and effectively construct the splitting field N of f over $\mathbb{Q}$. Moreover, we can effectively find all symmetric extensions $L_1, \ldots, L_r$ of $\mathbb{Q}$ in N and check whether $N = \prod_{i=1}^{r} L_i$ which is equivalent to $N \subset \mathbb{Q}_{\mathrm{symm}}$ since then $\mathrm{Gal}(N/\mathbb{Q})$ is a quotient of some $G \in \mathcal{F}_{\mathrm{symm}}$, hence in $\mathcal{F}_{\mathrm{symm}}$.

Outline

The embedding property

Definition

Let K be a field with absolute Galois group $\mathrm{Gal}(K) = \mathrm{Gal}(K_{\mathrm{sep}}/K)$ and $\mathcal{F}$ be a formation of finite groups. We say: K has the **embedding property** with respect to $\mathcal{F}$, if every embedding problem

(2)
$$\begin{tikzcd} & \mathrm{Gal}(K) \arrow[d, "\beta"] \\ G \arrow[r, "\alpha"] & \bar{G} \end{tikzcd}$$

with epimorphisms α and β and $G \in \mathcal{F}$ has a proper solution, i.e. there is an epimorphism $\gamma\colon \mathrm{Gal}(K) \to G$ with $\beta = \alpha \circ \gamma$.

$\mathbb{Q}$ has the embedding property with respect to $\mathcal{F}_{\mathrm{symm}}$

Theorem

The field $\mathbb{Q}$ (or any Hilbertian field with $\mathrm{char} \neq 2$) has the embedding property with respect to $\mathcal{F}_{\mathrm{symm}}$.

Example instead of proof

Put $G = \{(\sigma, \tau) \in \mathfrak{S}_5 \times \mathfrak{S}_6 \mid \mathrm{sgn}\,\sigma = \mathrm{sgn}\,\tau\}$ and $\bar{G} = \mathfrak{S}_6$ and let $\alpha\colon G \to \bar{G}$ be the second projection. So $\mathrm{Ker}\,\alpha = \mathfrak{A}_5$. There are many realizations $\beta\colon \mathrm{Gal}(\mathbb{Q}) \to \bar{G}$ of $\mathfrak{S}_6$ as $\mathrm{Gal}(N/\mathbb{Q})$. Let $L = \mathbb{Q}(\sqrt{d})$ be the fixed field of $\mathfrak{A}_6$ in N. Now we use a theorem of Brink.

$\mathbb{Q}$ has the embedding property with respect to $\mathcal{F}_{\rm symm}$

Theorem

The field $\mathbb{Q}$ (or any Hilbertian field with $\mathrm{char} \neq 2$) has the embedding property with respect to $\mathcal{F}_{\rm symm}$.

Example instead of proof

Put $G = \{(\sigma, \tau) \in \mathfrak{S}_5 \times \mathfrak{S}_6 \mid \mathrm{sgn}\,\sigma = \mathrm{sgn}\,\tau\}$ and $\bar{G} = \mathfrak{S}_6$ and let $\alpha\colon G \to \bar{G}$ be the second projection. So $\mathrm{Ker}\,\alpha = \mathfrak{A}_5$. There are many realizations $\beta\colon \mathrm{Gal}(\mathbb{Q}) \to \bar{G}$ of $\mathfrak{S}_6$ as $\mathrm{Gal}(N/\mathbb{Q})$. Let $L = \mathbb{Q}(\sqrt{d})$ be the fixed field of $\mathfrak{A}_6$ in N. Now we use a theorem of Brink.

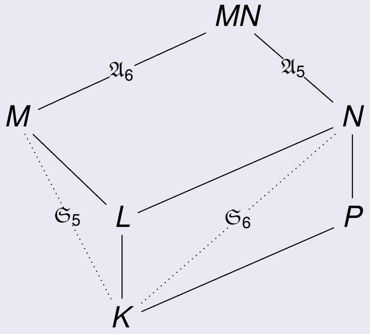
A theorem of Brink

Lemma [Brink 2004]

Let $n \geq 3$ be an integer, let K be a Hilbertian field with $\operatorname{char} K \neq 2$, let L/K be a quadratic extension and P/K be an algebraic extension with $L \not\subseteq P$. Then there are extensions M/L with $\operatorname{Gal}(M/K) = \mathfrak{S}_n$ and $M \cap P = K$.

Solving the embedding problem of the example

Diagram



which gives $\mathrm{Gal}(MN/K) = G$ and solves the embedding problem (2). $\square$

Corollary

Corollary

Any $G \in \mathcal{F}_{\mathrm{symm}}$ is a Galois group over $\mathbb{Q}$.

Outline

Definition of a free pro-$\mathcal{F}$-group

Definition

Let $\mathcal{F}$ be a formation of finite groups.

(a) A **pro-$\mathcal{F}$-group** G is a projective limit of groups in $\mathcal{F}$, i.e. a profinite group whose finite quotient groups are in $\mathcal{F}$: $\mathrm{Im}(G) \subseteq \mathcal{F}$.

(b) The **free pro-$\mathcal{F}$-group** $\hat{F}_n(\mathcal{F})$ **on n generators** $x_1, \ldots, x_n$ is a pro-$\mathcal{F}$-group, (topol.) generated by $X = \{x_1, \ldots, x_n\}$ with the following universal property:

> Let G be a pro-$\mathcal{F}$-group and $\varphi \colon X \to G$ be a map with $G = \langle \varphi(X) \rangle$. Then φ has a unique extension $\hat{\varphi} \colon \hat{F}_n(\mathcal{F}) \to G$ which is an epimorphism.

(c) "Similarly" one defines the free pro-$\mathcal{F}$-group $\hat{F}_\omega(\mathcal{F})$ with countably many generators.

Definition of a free pro-$\mathcal{F}$-group

Definition

Let $\mathcal{F}$ be a formation of finite groups.

(a) A **pro-$\mathcal{F}$-group** G is a projective limit of groups in $\mathcal{F}$, i.e. a profinite group whose finite quotient groups are in $\mathcal{F}$: $\mathrm{Im}(G) \subseteq \mathcal{F}$.

(b) The **free pro-$\mathcal{F}$-group** $\hat{F}_n(\mathcal{F})$ **on n generators** $x_1, \ldots, x_n$ is a pro-$\mathcal{F}$-group, (topol.) generated by $X = \{x_1, \ldots, x_n\}$ with the following universal property:

Let G be a pro-$\mathcal{F}$-group and $\varphi\colon X \to G$ be a map with $G = \langle \varphi(X) \rangle$. Then φ has a unique extension $\hat{\varphi}\colon \hat{F}_n(\mathcal{F}) \to G$ which is an epimorphism.

(c) "Similarly" one defines the free pro-$\mathcal{F}$-group $\hat{F}_\omega(\mathcal{F})$ with countably many generators.

Definition of a free pro-$\mathcal{F}$-group

Definition

Let $\mathcal{F}$ be a formation of finite groups.

(a) A **pro-$\mathcal{F}$-group** G is a projective limit of groups in $\mathcal{F}$, i.e. a profinite group whose finite quotient groups are in $\mathcal{F}$: $\mathrm{Im}(G) \subseteq \mathcal{F}$.

(b) The **free pro-$\mathcal{F}$-group** $\hat{F}_n(\mathcal{F})$ **on n generators** $x_1, \dots, x_n$ is a pro-$\mathcal{F}$-group, (topol.) generated by $X = \{x_1, \dots, x_n\}$ with the following universal property:

> Let G be a pro-$\mathcal{F}$-group and $\varphi \colon X \to G$ be a map with $G = \langle \varphi(X) \rangle$. Then φ has a unique extension $\hat{\varphi} \colon \hat{F}_n(\mathcal{F}) \to G$ which is an epimorphism.

(c) "Similarly" one defines the free pro-$\mathcal{F}$-group $\hat{F}_\omega(\mathcal{F})$ with countably many generators.

Definition of a free pro-$\mathcal{F}$-group

Definition

Let $\mathcal{F}$ be a formation of finite groups.

(a) A **pro-$\mathcal{F}$-group** G is a projective limit of groups in $\mathcal{F}$, i.e. a profinite group whose finite quotient groups are in $\mathcal{F}$: $\mathrm{Im}(G) \subseteq \mathcal{F}$.

(b) The **free pro-$\mathcal{F}$-group** $\hat{F}_n(\mathcal{F})$ **on n generators** $x_1, \ldots, x_n$ is a pro-$\mathcal{F}$-group, (topol.) generated by $X = \{x_1, \ldots, x_n\}$ with the following universal property:

> Let G be a pro-$\mathcal{F}$-group and $\varphi\colon X \to G$ be a map with $G = \langle \varphi(X) \rangle$. Then φ has a unique extension $\hat{\varphi}\colon \hat{F}_n(\mathcal{F}) \to G$ which is an epimorphism.

(c) "Similarly" one defines the free pro-$\mathcal{F}$-group $\hat{F}_\omega(\mathcal{F})$ with countably many generators.

Definition of a free pro-$\mathcal{F}$-group

Definition

Let $\mathcal{F}$ be a formation of finite groups.

(a) A **pro-$\mathcal{F}$-group** G is a projective limit of groups in $\mathcal{F}$, i.e. a profinite group whose finite quotient groups are in $\mathcal{F}$: $\mathrm{Im}(G) \subseteq \mathcal{F}$.

(b) The **free pro-$\mathcal{F}$-group** $\hat{F}_n(\mathcal{F})$ **on n generators** $x_1, \dots, x_n$ is a pro-$\mathcal{F}$-group, (topol.) generated by $X = \{x_1, \dots, x_n\}$ with the following universal property:

> Let G be a pro-$\mathcal{F}$-group and $\varphi\colon X \to G$ be a map with $G = \langle \varphi(X) \rangle$. Then φ has a unique extension $\hat{\varphi}\colon \hat{F}_n(\mathcal{F}) \to G$ which is an epimorphism.

(c) "Similarly" one defines the free pro-$\mathcal{F}$-group $\hat{F}_\omega(\mathcal{F})$ with countably many generators.

Small profinite groups

Definition

A profinite group G is **small** if for any n there are only finitely many normal subgroups of index n.
Example: Every finitely generated profinite group is small.

Facts

1. Let H, G be profinite groups with $\mathrm{Im}(H) = \mathrm{Im}(G)$. If H is small we have $H \cong G$.
2. $G \cong \hat{F}_n(\mathcal{F}) \iff \mathrm{Im}(G) = \{A \in \mathcal{F} \mid A \text{ has } n \text{ generators}\}$
3. $\mathrm{Im}(\hat{F}_\omega(\mathcal{F})) = \mathcal{F}$. But for $\mathcal{F} = \{\text{abelian } p\text{-groups}\}$ we have
$$G = \prod_n C_{p^n} \not\cong \hat{F}_\omega(\mathcal{F}) = \prod_n \hat{\mathbb{Z}}_p \quad \text{and} \quad \mathrm{Im}(G) = \mathcal{F}.$$

Small profinite groups

Definition

A profinite group G is **small** if for any n there are only finitely many normal subgroups of index n.
Example: Every finitely generated profinite group is small.

Facts

1. Let H, G be profinite groups with $\mathrm{Im}(H) = \mathrm{Im}(G)$. If H is small we have $H \cong G$.
2. $G \cong \hat{F}_n(\mathcal{F}) \Longleftrightarrow \mathrm{Im}(G) = \{A \in \mathcal{F} \mid A \text{ has } n \text{ generators}\}$
3. $\mathrm{Im}(\hat{F}_\omega(\mathcal{F})) = \mathcal{F}$. But for $\mathcal{F} = \{\text{abelian } p\text{-groups}\}$ we have
$$G = \prod_n C_{p^n} \ncong \hat{F}_\omega(\mathcal{F}) = \prod_n \hat{\mathbb{Z}}_p \quad \text{and} \quad \mathrm{Im}(G) = \mathcal{F}.$$

Small profinite groups

Definition

A profinite group G is **small** if for any n there are only finitely many normal subgroups of index n.
Example: Every finitely generated profinite group is small.

Facts

1. Let H, G be profinite groups with $\mathrm{Im}(H) = \mathrm{Im}(G)$. If H is small we have $H \cong G$.
2. $G \cong \hat{F}_n(\mathcal{F}) \Longleftrightarrow \mathrm{Im}(G) = \{A \in \mathcal{F} \mid A \text{ has } n \text{ generators}\}$
3. $\mathrm{Im}(\hat{F}_\omega(\mathcal{F})) = \mathcal{F}$. But for $\mathcal{F} = \{\text{abelian } p\text{-groups}\}$ we have $G = \prod_n C_{p^n} \not\cong \hat{F}_\omega(\mathcal{F}) = \prod_n \hat{\mathbb{Z}}_p$ and $\mathrm{Im}(G) = \mathcal{F}$.

Small profinite groups

Definition

A profinite group G is **small** if for any n there are only finitely many normal subgroups of index n.
Example: Every finitely generated profinite group is small.

Facts

1. Let H, G be profinite groups with $\mathrm{Im}(H) = \mathrm{Im}(G)$. If H is small we have $H \cong G$.
2. $G \cong \hat{F}_n(\mathcal{F}) \Longleftrightarrow \mathrm{Im}(G) = \{A \in \mathcal{F} \mid A \text{ has } n \text{ generators}\}$
3. $\mathrm{Im}(\hat{F}_\omega(\mathcal{F})) = \mathcal{F}$. But for $\mathcal{F} = \{\text{abelian } p\text{-groups}\}$ we have $G = \prod_n C_{p^n} \not\cong \hat{F}_\omega(\mathcal{F}) = \prod_n \hat{\mathbb{Z}}_p$ and $\mathrm{Im}(G) = \mathcal{F}$.

Small profinite groups

Definition

A profinite group G is **small** if for any n there are only finitely many normal subgroups of index n.
Example: Every finitely generated profinite group is small.

Facts

1. Let H, G be profinite groups with $\mathrm{Im}(H) = \mathrm{Im}(G)$. If H is small we have $H \cong G$.
2. $G \cong \hat{F}_n(\mathcal{F}) \Longleftrightarrow \mathrm{Im}(G) = \{A \in \mathcal{F} \mid A \text{ has } n \text{ generators}\}$
3. $\mathrm{Im}(\hat{F}_\omega(\mathcal{F})) = \mathcal{F}$. But for $\mathcal{F} = \{\text{abelian } p\text{-groups}\}$ we have
$$G = \prod_n C_{p^n} \ncong \hat{F}_\omega(\mathcal{F}) = \prod_n \hat{\mathbb{Z}}_p \quad \text{and} \quad \mathrm{Im}(G) = \mathcal{F}\,.$$

The embedding property of a pro-$\mathcal{F}$ group

Definition

A profinite group G has the **embedding property**, if to epimorphisms $\alpha\colon H \to \bar{H}$ and $\beta\colon G \to \bar{H}$ with $H \in \mathrm{Im}(G)$ there is an epimorphism $\gamma\colon G \to H$ with $\beta = \alpha \circ \gamma$.

Example

The groups $\hat{F}_n(\mathcal{F})$ and $\hat{F}_\omega(\mathcal{F})$ have the embedding property, the Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$ too.

The embedding property of a pro-$\mathcal{F}$ group

Definition

A profinite group G has the **embedding property**, if to epimorphisms $\alpha\colon H \to \bar{H}$ and $\beta\colon G \to \bar{H}$ with $H \in \mathrm{Im}(G)$ there is an epimorphism $\gamma\colon G \to H$ with $\beta = \alpha \circ \gamma$.

Example

The groups $\hat{F}_n(\mathcal{F})$ and $\hat{F}_\omega(\mathcal{F})$ have the embedding property, the Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$ too.

A theorem of Iwasawa

Proposition (Iwasawa) [FrJ08, Lemma 24.4.7]

Let H, G be profinite groups with countably many generators and the embedding property. Then

$$\mathrm{Im}(G) = \mathrm{Im}(H) \Longrightarrow G \cong H\,.$$

Corollary 1 [FrJ08, Thm. 24.8.1]

If G is an ω-generated pro-$\mathcal{F}$-group, then $G \cong \hat{F}_\omega(\mathcal{F})$ iff $\mathrm{Im}(G) = \mathcal{F}$ and G has the embedding property.

Corollary 2 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$$\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q}) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$$

A theorem of Iwasawa

Proposition (Iwasawa) [FrJ08, Lemma 24.4.7]

Let H, G be profinite groups with countably many generators and the embedding property. Then

$$\mathrm{Im}(G) = \mathrm{Im}(H) \Longrightarrow G \cong H\,.$$

Corollary 1 [FrJ08, Thm. 24.8.1]

If G is an ω-generated pro-$\mathcal{F}$-group, then $G \cong \hat{F}_\omega(\mathcal{F})$ iff $\mathrm{Im}(G) = \mathcal{F}$ and G has the embedding property.

Corollary 2 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$$\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q}) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$$

A theorem of Iwasawa

Proposition (Iwasawa) [FrJ08, Lemma 24.4.7]

Let H, G be profinite groups with countably many generators and the embedding property. Then

$$\mathrm{Im}(G) = \mathrm{Im}(H) \Longrightarrow G \cong H\,.$$

Corollary 1 [FrJ08, Thm. 24.8.1]

If G is an ω-generated pro-$\mathcal{F}$-group, then $G \cong \hat{F}_\omega(\mathcal{F})$ iff $\mathrm{Im}(G) = \mathcal{F}$ and G has the embedding property.

Corollary 2 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$$\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q}) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$$

Outline

Determination of fields by Galois groups

Theorem [Neukirch 1970]

Let K and L be finite extensions of $\mathbb{Q}$. Then

$$G(K) \cong G(L) \Longrightarrow K \cong L$$

Remark 1

The maximal solvable quotient groups $\mathrm{Gal}(K_{\mathrm{solv}}/K)$ determine the number field K up to conjugation.

Remark 2 [Uchida 1977]

The same holds for global fields in all characteristics.

Remark 3 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$ is the same for all number fields K.

Determination of fields by Galois groups

Theorem [Neukirch 1970]

Let K and L be finite extensions of $\mathbb{Q}$. Then

$$G(K) \cong G(L) \Longrightarrow K \cong L$$

Remark 1

The maximal solvable quotient groups $\mathrm{Gal}(K_{\mathrm{solv}}/K)$ determine the number field K up to conjugation.

Remark 2 [Uchida 1977]

The same holds for global fields in all characteristics.

Remark 3 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$ is the same for all number fields K.

Determination of fields by Galois groups

Theorem [Neukirch 1970]

Let K and L be finite extensions of $\mathbb{Q}$. Then

$$G(K) \cong G(L) \Longrightarrow K \cong L$$

Remark 1

The maximal solvable quotient groups $\mathrm{Gal}(K_{\mathrm{solv}}/K)$ determine the number field K up to conjugation.

Remark 2 [Uchida 1977]

The same holds for global fields in all characteristics.

Remark 3 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$ is the same for all number fields K.

Determination of fields by Galois groups

Theorem [Neukirch 1970]

Let K and L be finite extensions of $\mathbb{Q}$. Then

$$G(K) \cong G(L) \Longrightarrow K \cong L$$

Remark 1

The maximal solvable quotient groups $\mathrm{Gal}(K_{\mathrm{solv}}/K)$ determine the number field K up to conjugation.

Remark 2 [Uchida 1977]

The same holds for global fields in all characteristics.

Remark 3 (Geyer, Jarden, R. 2019) [GJR19, Thm. 7.5]

$\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{symm}})$ is the same for all number fields K.

Twaddling

Twaddling

By van der Waerden [1933] asymptotically 100% of all $f \in \mathbb{Z}[X]$ of degree n have Galois group $\mathfrak{S}_n$ over $\mathbb{Q}$. They form the plebs, the common folk, the lower class of polynomials, compared to the polynomials with solvable Galois group which are full of arithmetical significance, the aristocratic upper class. But the highest class with the most arithmetical properties are the polynomials with abelian Galois group as class field theory and the following theorem indicate.

Outline

The formation of all finite solvable groups

Theorem [Iwasawa 1953]

Let $\mathcal{F}_{\mathrm{solv}}$ be the formation of all finite solvable groups. Then $\mathrm{Gal}(\mathbb{Q}_{\mathrm{solv}}/\mathbb{Q}_{\mathrm{ab}}) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{solv}})$.

Idea of proof

Let $G = \mathrm{Gal}(\mathbb{Q}_{\mathrm{solv}}/\mathbb{Q}_{\mathrm{ab}})$. The absolute Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}})$ of $\mathbb{Q}_{\mathrm{ab}} = \mathbb{Q}(\mu_\infty)$ has cohomological dimension 1 by class field theory. Therefore every embedding problem over $\mathbb{Q}_{\mathrm{ab}}$ has a weak solution. Moreover $\mathbb{Q}_{\mathrm{ab}}$ is Hilbertian. Therefore every minimal split $\mathcal{F}_{\mathrm{solv}}$-embedding problem (where the kernel is elementary abelian) is solvable. This implies by group-theoretical considerations that every $\mathcal{F}_{\mathrm{solv}}$-embedding problem is solvable. Therefore $\mathrm{Im}(G) = \mathcal{F}_{\mathrm{solv}}$ and G has the embedding property. This implies $G \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{solv}})$. $\square$

The formation of all finite solvable groups

Theorem [Iwasawa 1953]

Let $\mathcal{F}_{\mathrm{solv}}$ be the formation of all finite solvable groups. Then $\mathrm{Gal}(\mathbb{Q}_{\mathrm{solv}}/\mathbb{Q}_{\mathrm{ab}}) \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{solv}})$.

Idea of proof

Let $G = \mathrm{Gal}(\mathbb{Q}_{\mathrm{solv}}/\mathbb{Q}_{\mathrm{ab}})$. The absolute Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}})$ of $\mathbb{Q}_{\mathrm{ab}} = \mathbb{Q}(\boldsymbol{\mu}_\infty)$ has cohomological dimension 1 by class field theory. Therefore every embedding problem over $\mathbb{Q}_{\mathrm{ab}}$ has a weak solution. Moreover $\mathbb{Q}_{\mathrm{ab}}$ is Hilbertian. Therefore every minimal split $\mathcal{F}_{\mathrm{solv}}$-embedding problem (where the kernel is elementary abelian) is solvable. This implies by group-theoretical considerations that every $\mathcal{F}_{\mathrm{solv}}$-embedding problem is solvable. Therefore $\mathrm{Im}(G) = \mathcal{F}_{\mathrm{solv}}$ and G has the embedding property. This implies $G \cong \hat{F}_\omega(\mathcal{F}_{\mathrm{solv}})$. $\square$

A conjecture of Shafarevich

Remark

This holds for any number field instead of K. If K is a global field of prime characteristic, e.g. $K = \mathbb{F}_p(t)$, then [Pop 1995] showed more: $\mathrm{Gal}(K_{\mathrm{ab}}) \cong \hat{F}_\omega$.

Conjecture [Shafarevich]

$\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}) \cong \hat{F}_\omega$.

A conjecture of Shafarevich

Remark

This holds for any number field instead of K. If K is a global field of prime characteristic, e.g. $K = \mathbb{F}_p(t)$, then [Pop 1995] showed more: $\mathrm{Gal}(K_{\mathrm{ab}}) \cong \hat{F}_\omega$.

Conjecture [Shafarevich]

$\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}) \cong \hat{F}_\omega$.

Outline

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \cdots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\text{symm}} \subset (\mathbb{Q}_{\text{symm}})_{\text{symm}} \subset \cdots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\text{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \cdots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \dots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \dots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \cdots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \dots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Properties of the field K_{symm}

Properties of the field K_{symm}

Let K be a countable Hilbertian field, e.g. $K = \mathbb{Q}$.

(a) K_{symm} is Hilbertian.

Follows from Haran's diamond theorem [1999]. As a consequence we get an infinite sequence

$$\mathbb{Q} \subset \mathbb{Q}_{\mathrm{symm}} \subset (\mathbb{Q}_{\mathrm{symm}})_{\mathrm{symm}} \subset \dots .$$

(b) K_{symm} is **PAC**, i.e. every geometrically integral variety over K_{symm} has a K_{symm}-rational point.

By [Fried-Jarden, 1978] using the stability of fields.

(c) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.

This follows from (a),(b) and the countability: [Fried-Völklein 1992] in char. 0, [Pop 1996] in general.

Primitive recursive decidability lemma

Definition

A field K has **elimination theory** if every finitely generated presented extension L of K has an effective algorithm for factoring each polynomial in $L[X]$ of positive degree into a product of irreducible factors.

Lemma (Jarden-Shlapentokh, 2017) [JaS17]

Let K be a presented field with elimination theory. Let M be a perfect algebraic extension of K such that M is PAC, $\mathrm{Gal}(M)$ has the embedding property, and $\mathrm{Im}(\mathrm{Gal}(M))$ is a primitive recursive subset of the set of all finite groups. Further, suppose the set $\mathrm{Root}(M/K)$ of monic polynomials in $K[X]$ that have a root in M is primitive recursive. Then, $\mathrm{Th}(M)$ is primitive recursive.

Primitive recursive decidability lemma

Definition

A field K has **elimination theory** if every finitely generated presented extension L of K has an effective algorithm for factoring each polynomial in $L[X]$ of positive degree into a product of irreducible factors.

Lemma (Jarden-Shlapentokh, 2017) [JaS17]

Let K be a presented field with elimination theory. Let M be a perfect algebraic extension of K such that M is PAC, $\mathrm{Gal}(M)$ has the embedding property, and $\mathrm{Im}(\mathrm{Gal}(M))$ is a primitive recursive subset of the set of all finite groups. Further, suppose the set $\mathrm{Root}(M/K)$ of monic polynomials in $K[X]$ that have a root in M is primitive recursive. Then, $\mathrm{Th}(M)$ is primitive recursive.

Primitive recursive decidability

Proposition (Geyer, Jarden, R. 2019) [GJR19, Thm. 8.5(b)]

There is a primitively recursive procedure to decide which sentences in the first-order language of rings are true in $\mathbb{Q}_{\mathrm{symm}}$ and which not.

Remark

This is true for all countable Hilbertian fields K, even if we add names of the elements of K to the language, as long as $\mathrm{char}\, K = 0$.
If $\mathrm{char}\, K \neq 0$, then all is true if we replace K_{symm} by its perfect hull $K_{\mathrm{symm,ins}}$.

Primitive recursive decidability

Proposition (Geyer, Jarden, R. 2019) [GJR19, Thm. 8.5(b)]

There is a primitively recursive procedure to decide which sentences in the first-order language of rings are true in $\mathbb{Q}_{\text{symm}}$ and which not.

Remark

This is true for all countable Hilbertian fields K, even if we add names of the elements of K to the language, as long as $\operatorname{char} K = 0$.
If $\operatorname{char} K \neq 0$, then all is true if we replace K_{symm} by its perfect hull $K_{\text{symm,ins}}$.

Undecidability of $\mathbb{Q}^{(2)}$

Theorem (Martinez-Ranero, Utreras, Videla 2020) [MUV20]

The first order theory of $\mathbb{Q}^{(2)}$, the compositum of all quadratic extensions of $\mathbb{Q}$, is undecidable.

Remark

For a positive integer m, let $\mathbb{Q}_{\mathrm{symm}}^{(m)}$ be the compositum of all Galois extensions of $\mathbb{Q}$ with Galois groups $\mathfrak{S}_n$ for some $n \geq m$. In particular, $\mathbb{Q}_{\mathrm{symm}} = \mathbb{Q}_{\mathrm{symm}}^{(2)}$. Also, $\mathbb{Q}_{\mathrm{symm}}^{(m+1)} \subseteq \mathbb{Q}_{\mathrm{symm}}^{(m)}$.

$\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}}^{(m)})$ is primitive recursively decidable [GJR19, Example 9.1].

$\bigcap_m \mathbb{Q}_{\mathrm{symm}}^{(m)} = \mathbb{Q}^{(2)}$ [GJR19, Prop. 9.3].

Undecidability of $\mathbb{Q}^{(2)}$

Theorem (Martinez-Ranero, Utreras, Videla 2020) [MUV20]

The first order theory of $\mathbb{Q}^{(2)}$, the compositum of all quadratic extensions of $\mathbb{Q}$, is undecidable.

Remark

For a positive integer m, let $\mathbb{Q}_{\mathrm{symm}}^{(m)}$ be the compositum of all Galois extensions of $\mathbb{Q}$ with Galois groups $\mathfrak{S}_n$ for some $n \geq m$. In particular, $\mathbb{Q}_{\mathrm{symm}} = \mathbb{Q}_{\mathrm{symm}}^{(2)}$. Also, $\mathbb{Q}_{\mathrm{symm}}^{(m+1)} \subseteq \mathbb{Q}_{\mathrm{symm}}^{(m)}$.

$\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}}^{(m)})$ is primitive recursively decidable [GJR19, Example 9.1].

$\bigcap_m \mathbb{Q}_{\mathrm{symm}}^{(m)} = \mathbb{Q}^{(2)}$ [GJR19, Prop. 9.3].

Undecidability of $\mathbb{Q}^{(2)}$

Theorem (Martinez-Ranero, Utreras, Videla 2020) [MUV20]

The first order theory of $\mathbb{Q}^{(2)}$, the compositum of all quadratic extensions of $\mathbb{Q}$, is undecidable.

Remark

For a positive integer m, let $\mathbb{Q}_{\text{symm}}^{(m)}$ be the compositum of all Galois extensions of $\mathbb{Q}$ with Galois groups $\mathfrak{S}_n$ for some $n \geq m$. In particular, $\mathbb{Q}_{\text{symm}} = \mathbb{Q}_{\text{symm}}^{(2)}$. Also, $\mathbb{Q}_{\text{symm}}^{(m+1)} \subseteq \mathbb{Q}_{\text{symm}}^{(m)}$.

$\text{Th}(\mathbb{Q}_{\text{symm}}^{(m)})$ is primitive recursively decidable [GJR19, Example 9.1].

$\bigcap_m \mathbb{Q}_{\text{symm}}^{(m)} = \mathbb{Q}^{(2)}$ [GJR19, Prop. 9.3].

Undecidability of $\mathbb{Q}^{(2)}$

Theorem (Martinez-Ranero, Utreras, Videla 2020) [MUV20]

The first order theory of $\mathbb{Q}^{(2)}$, the compositum of all quadratic extensions of $\mathbb{Q}$, is undecidable.

Remark

For a positive integer m, let $\mathbb{Q}_{\mathrm{symm}}^{(m)}$ be the compositum of all Galois extensions of $\mathbb{Q}$ with Galois groups $\mathfrak{S}_n$ for some $n \geq m$. In particular, $\mathbb{Q}_{\mathrm{symm}} = \mathbb{Q}_{\mathrm{symm}}^{(2)}$. Also, $\mathbb{Q}_{\mathrm{symm}}^{(m+1)} \subseteq \mathbb{Q}_{\mathrm{symm}}^{(m)}$.

$\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}}^{(m)})$ is primitive recursively decidable [GJR19, Example 9.1].

$\bigcap_m \mathbb{Q}_{\mathrm{symm}}^{(m)} = \mathbb{Q}^{(2)}$ [GJR19, Prop. 9.3].

The ring of integers of $\mathbb{Q}_{\mathrm{symm}}$ and of $\mathbb{F}_p(t)_{\mathrm{symm}}$

Theorem (Jarden and R. 2018) [JaR18, Cor. 2.5]

Let K be either $\mathbb{Q}$ or $\mathbb{F}_p(t)$ and let $\mathcal{O}$ be either $\mathbb{Z}$ or $\mathbb{F}_p[t]$, respectively. Let $\mathcal{O}_{\mathrm{symm}}$ (resp., $\mathcal{O}_{\mathrm{symm,ins}}$) be the integral closure of $\mathcal{O}$ in K_{symm} (resp. $K_{\mathrm{symm,ins}}$). Then, K_{symm} is **PAC over** *$\mathcal{O}_{\mathrm{symm}}$, i.e. for each absolutely irreducible polynomial $f \in K_{\mathrm{symm}}[T, X]$ s.t. $\frac{\partial f}{\partial X} \neq 0$ there are infinitely many $(a, b) \in \mathcal{O}_{\mathrm{symm}} \times K_{\mathrm{symm}}$ with $f(a, b) = 0$. Also, $K_{\mathrm{symm,ins}}$ is PAC over $\mathcal{O}_{\mathrm{symm,ins}}$.*

Ingredients of the proof

[GJR17a] applies Konrad Neumann's theorem on the "symmetric stabilization of function fields over K" [Neu98].

[GJR17b] relies on a work of Moret-Bailly on Skolem problems [MoB89].

The ring of integers of $\mathbb{Q}_{\mathrm{symm}}$ and of $\mathbb{F}_p(t)_{\mathrm{symm}}$

Theorem (Jarden and R. 2018) [JaR18, Cor. 2.5]

Let K be either $\mathbb{Q}$ or $\mathbb{F}_p(t)$ and let $\mathcal{O}$ be either $\mathbb{Z}$ or $\mathbb{F}_p[t]$, respectively. Let $\mathcal{O}_{\mathrm{symm}}$ (resp., $\mathcal{O}_{\mathrm{symm,ins}}$) be the integral closure of $\mathcal{O}$ in K_{symm} (resp. $K_{\mathrm{symm,ins}}$). Then, K_{symm} is **PAC over** $\mathcal{O}_{\mathrm{symm}}$*, i.e. for each absolutely irreducible polynomial $f \in K_{\mathrm{symm}}[T, X]$ s.t. $\frac{\partial f}{\partial X} \neq 0$ there are infinitely many $(a, b) \in \mathcal{O}_{\mathrm{symm}} \times K_{\mathrm{symm}}$ with $f(a, b) = 0$. Also, $K_{\mathrm{symm,ins}}$ is PAC over $\mathcal{O}_{\mathrm{symm,ins}}$.*

Ingredients of the proof

[GJR17a] applies Konrad Neumann's theorem on the "symmetric stabilization of function fields over K" [Neu98].

[GJR17b] relies on a work of Moret-Bailly on Skolem problems [MoB89].

The ring of integers of $\mathbb{Q}_{\mathrm{symm}}$ and of $\mathbb{F}_p(t)_{\mathrm{symm}}$

Theorem (Jarden and R. 2018) [JaR18, Cor. 2.5]

Let K be either $\mathbb{Q}$ or $\mathbb{F}_p(t)$ and let $\mathcal{O}$ be either $\mathbb{Z}$ or $\mathbb{F}_p[t]$, respectively. Let $\mathcal{O}_{\mathrm{symm}}$ (resp., $\mathcal{O}_{\mathrm{symm,ins}}$) be the integral closure of $\mathcal{O}$ in K_{symm} (resp. $K_{\mathrm{symm,ins}}$). Then, K_{symm} is **PAC over** $\mathcal{O}_{\mathrm{symm}}$*, i.e. for each absolutely irreducible polynomial $f \in K_{\mathrm{symm}}[T, X]$ s.t. $\frac{\partial f}{\partial X} \neq 0$ there are infinitely many $(a, b) \in \mathcal{O}_{\mathrm{symm}} \times K_{\mathrm{symm}}$ with $f(a, b) = 0$. Also, $K_{\mathrm{symm,ins}}$ is PAC over $\mathcal{O}_{\mathrm{symm,ins}}$.*

Ingredients of the proof

[GJR17a] applies Konrad Neumann's theorem on the “symmetric stabilization of function fields over K" [Neu98].

[GJR17b] relies on a work of Moret-Bailly on Skolem problems [MoB89].

Primitive recursive decidability of $\mathcal{O}_{\mathrm{symm,ins}}$

Lemma (Jarden-R., 2020) [JaR20, Lemma 4.2]

Let M be a perfect algebraic extension of K s.t. M is PAC over its ring of integers $\mathcal{O}_M$, $\mathrm{Gal}(M)$ has the embedding property, $\mathrm{Im}(\mathrm{Gal}(M))$ is primitive recursive, and $\mathrm{Root}(M/K)$ is primitive recursive. Then, $\mathrm{Th}(\mathcal{O}_M)$ is primitive recursively decidable.

Ingredients of the proof

[Raz19] that uses v.d. Dries elimination of quantifiers procedure for the ring of all algebraic integers [Dri88] combined with a generalization of the Galois stratification of [FrJ08, §30].

Theorem (Jarden-R. 2020) [JaR20, Thm. 4.3]

$\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ is primitive recursive.

Primitive recursive decidability of $\mathcal{O}_{\mathrm{symm,ins}}$

Lemma (Jarden-R., 2020) [JaR20, Lemma 4.2]

Let M be a perfect algebraic extension of K s.t. M is PAC over its ring of integers $\mathcal{O}_M$, $\mathrm{Gal}(M)$ has the embedding property, $\mathrm{Im}(\mathrm{Gal}(M))$ is primitive recursive, and $\mathrm{Root}(M/K)$ is primitive recursive. Then, $\mathrm{Th}(\mathcal{O}_M)$ is primitive recursively decidable.

Ingredients of the proof

[Raz19] that uses v.d. Dries elimination of quantifiers procedure for the ring of all algebraic integers [Dri88] combined with a generalization of the Galois stratification of [FrJ08, §30].

Theorem (Jarden-R. 2020) [JaR20, Thm. 4.3]

$\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ is primitive recursive.

Primitive recursive decidability of $\mathcal{O}_{\mathrm{symm,ins}}$

Lemma (Jarden-R., 2020) [JaR20, Lemma 4.2]

Let M be a perfect algebraic extension of K s.t. M is PAC over its ring of integers $\mathcal{O}_M$, $\mathrm{Gal}(M)$ has the embedding property, $\mathrm{Im}(\mathrm{Gal}(M))$ is primitive recursive, and $\mathrm{Root}(M/K)$ is primitive recursive. Then, $\mathrm{Th}(\mathcal{O}_M)$ is primitive recursively decidable.

Ingredients of the proof

[Raz19] that uses v.d. Dries elimination of quantifiers procedure for the ring of all algebraic integers [Dri88] combined with a generalization of the Galois stratification of [FrJ08, §30].

Theorem (Jarden-R. 2020) [JaR20, Thm. 4.3]

$\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ is primitive recursive.

References I

D. Brink,
On alternating and symmetric groups as Galois groups,
Israel J. Math **142** (2004), 47–60.

L. van den Dries,
Elimination theory for the ring of algebraic integers,
J. reine angew. Math. **388** (1988), 189–205.

M. Fried and M. Jarden,
Field Arithmetic (3rd Edition),
Ergebnisse der Mathematik (3), **11**, Springer, Heidelberg, 2008.

References I

- D. Brink,
  On alternating and symmetric groups as Galois groups,
  Israel J. Math **142** (2004), 47–60.
- L. van den Dries,
  Elimination theory for the ring of algebraic integers,
  J. reine angew. Math. **388** (1988), 189–205.
- M. Fried and M. Jarden,
  Field Arithmetic (3rd Edition),
  Ergebnisse der Mathematik (3), **11**, Springer, Heidelberg, 2008.

References I

D. Brink,
On alternating and symmetric groups as Galois groups,
Israel J. Math **142** (2004), 47–60.

L. van den Dries,
Elimination theory for the ring of algebraic integers,
J. reine angew. Math. **388** (1988), 189–205.

M. Fried and M. Jarden,
Field Arithmetic (3rd Edition),
Ergebnisse der Mathematik (3), **11**, Springer, Heidelberg, 2008.

References II

W.-D. Geyer, M. Jarden, and A. Razon,
On stabilizers of algebraic function fields of one variable,
Advances in Geometry **17**, Issue 2, (2017), 131–174.

W.-D. Geyer, M. Jarden, and A. Razon,
Strong approximation theorem for absolutely integral varieties over PSC Galois extensions of global fields,
New York Journal of Mathematics **23** (2017), 1447–1529.

W.-D. Geyer, M. Jarden, and A. Razon,
Composita of symmetric extensions of $\mathbb{Q}$,
Münster Journal of Mathematics **12** (2019), 139–161.

References II

- W.-D. Geyer, M. Jarden, and A. Razon,
  On stabilizers of algebraic function fields of one variable,
  Advances in Geometry **17**, Issue 2, (2017), 131–174.

- W.-D. Geyer, M. Jarden, and A. Razon,
  Strong approximation theorem for absolutely integral varieties over PSC *Galois extensions of global fields*,
  New York Journal of Mathematics **23** (2017), 1447–1529.

- W.-D. Geyer, M. Jarden, and A. Razon,
  Composita of symmetric extensions of $\mathbb{Q}$,
  Münster Journal of Mathematics **12** (2019), 139–161.

W.-D. Geyer, M. Jarden, and A. Razon,
On stabilizers of algebraic function fields of one variable,
Advances in Geometry **17**, Issue 2, (2017), 131–174.

W.-D. Geyer, M. Jarden, and A. Razon,
Strong approximation theorem for absolutely integral varieties over $\mathrm{PS}\mathbb{C}$ *Galois extensions of global fields*,
New York Journal of Mathematics **23** (2017), 1447–1529.

W.-D. Geyer, M. Jarden, and A. Razon,
Composita of symmetric extensions of $\mathbb{Q}$,
Münster Journal of Mathematics **12** (2019), 139–161.

M. Jarden and A. Razon,
Strong approximation theorem for absolutely integral varieties over the compositum of all symmetric extensions of a global field,
Glasgow Math. J. **61** (2018), 373–380.

M. Jarden and A. Razon,
Primitive recursive decidability for the ring of integers of the compositum of all symmetric extensions of $\mathbb{Q}$,
Glasgow Math. J. (2020),
doi:10.1017/S001708952000018X.

M. Jarden and A. Shlapentokh,
Decidable algebraic fields,
J. Symb. Log. **82** (2017), no. 2, 474–488.

M. Jarden and A. Razon,
Strong approximation theorem for absolutely integral varieties over the compositum of all symmetric extensions of a global field,
Glasgow Math. J. **61** (2018), 373–380.

M. Jarden and A. Razon,
Primitive recursive decidability for the ring of integers of the compositum of all symmetric extensions of $\mathbb{Q}$,
Glasgow Math. J. (2020),
doi:10.1017/S001708952000018X.

M. Jarden and A. Shlapentokh,
Decidable algebraic fields,
J. Symb. Log. **82** (2017), no. 2, 474–488.

References III

M. Jarden and A. Razon,
Strong approximation theorem for absolutely integral varieties over the compositum of all symmetric extensions of a global field,
Glasgow Math. J. **61** (2018), 373–380.

M. Jarden and A. Razon,
Primitive recursive decidability for the ring of integers of the compositum of all symmetric extensions of $\mathbb{Q}$,
Glasgow Math. J. (2020),
doi:10.1017/S001708952000018X.

M. Jarden and A. Shlapentokh,
Decidable algebraic fields,
J. Symb. Log. **82** (2017), no. 2, 474–488.

C. Martinez-Ranero, J. Utreras, and C. R. Videla,
Undecidability of $\mathbb{Q}^{(2)}$,
Proc. Amer. Math. Soc. **148** (2020), 961–964.

L. Moret-Bailly,
Groupes de Picard et problémes de Skolem II,
Annales Scientiques de l'Ecole Normale Superieure (4) **22** (1989), 181–194.

K. Neumann,
Every finitely generated regular field extension has a stable transcendence base,
Israel Journal of Mathematics **104** (1998), 221–260.

References IV

C. Martinez-Ranero, J. Utreras, and C. R. Videla,
Undecidability of $\mathbb{Q}^{(2)}$,
Proc. Amer. Math. Soc. **148** (2020), 961–964.

L. Moret-Bailly,
Groupes de Picard et problémes de Skolem II,
Annales Scientiques de l'Ecole Normale Superieure (4) **22** (1989), 181–194.

K. Neumann,
Every finitely generated regular field extension has a stable transcendence base,
Israel Journal of Mathematics **104** (1998), 221–260.

C. Martinez-Ranero, J. Utreras, and C. R. Videla,
Undecidability of $\mathbb{Q}^{(2)}$,
Proc. Amer. Math. Soc. **148** (2020), 961–964.

L. Moret-Bailly,
Groupes de Picard et problémes de Skolem II,
Annales Scientiques de l'Ecole Normale Superieure (4) **22** (1989), 181–194.

K. Neumann,
Every finitely generated regular field extension has a stable transcendence base,
Israel Journal of Mathematics **104** (1998), 221–260.

References V

A. Razon,
Primitive recursive decidability for large rings of algebraic integers,
Albanian Journal of Mathematics **13** (2019), 3–93.