Entangled radicals and Galois groups

B. de Smit

Mathematisch Instituut
Universiteit Leiden
Netherlands

Joint work with Willem Jan Palenstijn
Let $K$ be a field of characteristic 0.

**Definition.** A field extension $K \subset L$ is a *radical* extension if there is a subgroup $B \subset L^*$ such that

- $K^* \subset B$;
- $B/K^*$ is torsion;
- $L = K(B)$. 
Let $K$ be a field of characteristic 0.

**Definition.** A field extension $K \subset L$ is a **radical** extension if there is a subgroup $B \subset L^*$ such that

- $K^* \subset B$;
- $B/K^*$ is torsion;
- $L = K(B)$.

**Example.** For $B = \sqrt[n]{K^*} = \{x \in K^* : x^n \in K^* \text{ for some } n \geq 1\}$, we have $L = K(B) = K(\sqrt[n]{K^*})$

**Example.** $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[16]{-4} \rangle$. 
Let $K$ be a field of characteristic $0$.

**Definition.** A field extension $K \subset L$ is a radical extension if there is a subgroup $B \subset L^*$ such that

- $K^* \subset B$;
- $B/K^*$ is torsion;
- $L = K(B)$.

**Example.** For $B = \sqrt[n]{K^*} = \{x \in K^* : x^n \in K^* \text{ for some } n \geq 1\}$ we have $L = K(B) = K(\sqrt[n]{K^*})$

**Example.** $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[16]{-4} \rangle$.

**Example.** $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[5]{1}, \sqrt[5]{5} \rangle$. 
Goal: Express field arithmetic of radical extensions $K \subset L = K(B)$ in terms of the group extension $K^* \subset B$. 
Goal: Express field arithmetic of radical extensions $K \subset L = K(B)$ in terms of the group extension $K^* \subset B$.

Example. In the Kummer case we have

$$L \cong K\{B\} = K[B] \otimes_{K[K^*]} K,$$

and $[L : K] = [B : K^*]$, and fields between $K$ and $L$ correspond 1–1 to groups between $K^*$ and $B$. 
Goal: Express field arithmetic of radical extensions $K \subset L = K(B)$ in terms of the group extension $K^* \subset B$.

Example. In the Kummer case we have

$$L \cong K\{B\} = K[B] \otimes_{K[K^*]} K,$$

and $[L : K] = [B : K^*]$, and fields between $K$ and $L$ correspond $1 - 1$ to groups between $K^*$ and $B$.

Next talk: There is a polynomial time algorithm that given $d \geq 1$ and $x_1, \ldots, x_n \in \mathbb{Q}$, computes the degree of $\mathbb{Q}(\mu_d, \sqrt[1]{x_1}, \ldots, \sqrt[1]{x_n})$
Goal: Express field arithmetic of radical extensions $K \subset L = K(B)$ in terms of the group extension $K^* \subset B$.

Example. In the Kummer case we have

$$L \cong K\{B\} = K[B] \otimes_{K[K^*]} K,$$

and $[L : K] = [B : K^*]$, and fields between $K$ and $L$ correspond 1–1 to groups between $K^*$ and $B$.

Next talk: There is a polynomial time algorithm that given $d \geq 1$ and $x_1, \ldots, x_n \in \mathbb{Q}$, computes the degree of $\mathbb{Q}(\mu_d, d\sqrt{x_1}, \ldots, d\sqrt{x_n})$ over $\mathbb{Q}(\mu_d)$. 
Goal: Express field arithmetic of radical extensions $K \subset L = K(B)$ in terms of the group extension $K^* \subset B$.

Example. In the Kummer case we have

$$L \cong K\{B\} = K[B] \otimes_{K[K^*]} K,$$

and $[L : K] = [B : K^*]$, and fields between $K$ and $L$ correspond 1–1 to groups between $K^*$ and $B$.

Next talk: There is a polynomial time algorithm that given $d \geq 1$ and $x_1, \ldots, x_n \in \mathbb{Q}$, computes the degree of $\mathbb{Q}(\mu_d, \sqrt[d]{x_1}, \ldots, \sqrt[d]{x_n})$ over $\mathbb{Q}(\mu_d)$.

This talk: Express $\text{Gal}(L/K)$ in terms of $B, K$. 
Difficulty: radicals can be entangled:
Difficulty: radicals can be entangled:

\[ 1 + 2\sqrt[3]{1} = \sqrt{-3} \]
\[ \zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}, \quad \zeta = \sqrt[5]{1} \]
\[ 2\sqrt[4]{-9} = \sqrt{6} + \sqrt{-6} \]
Difficulty: radicals can be entangled:

\[
1 + 2\sqrt[3]{1} = \sqrt{-3} \\
\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}, \quad \zeta = 5\sqrt{1} \\
2\sqrt[4]{-9} = \sqrt{6} + \sqrt{-6}
\]

Artin’s primitive root conjecture:
Compute the density of primes \( p \) with \( \mathbb{F}_p^* = \langle 5 \rangle \)
Difficulty: radicals can be entangled:

\[
1 + 2^3\sqrt{1} = \sqrt{-3}
\]

\[
\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}, \quad \zeta = \sqrt[5]{1}
\]

\[
2^4\sqrt{-9} = \sqrt{6} + \sqrt{-6}
\]

Artin’s primitive root conjecture:

Compute the density of primes \( p \) with \( \mathbb{F}_p^* = \langle 5 \rangle \), i.e., \( l \nmid [\mathbb{F}_p^* : \langle 5 \rangle] \) for all primes \( l \).
Difficulty: radicals can be entangled:

\[
1 + 2\sqrt[3]{1} = \sqrt{-3}
\]

\[
\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}, \quad \zeta = \sqrt[5]{1}
\]

\[
2\sqrt[4]{-9} = \sqrt{6} + \sqrt{-6}
\]

Artin’s primitive root conjecture:

Compute the density of primes \( p \) with \( \mathbb{F}_p^* = \langle 5 \rangle \), i.e., \( l \nmid [\mathbb{F}_p^* : \langle 5 \rangle] \) for all primes \( l \).

\[
5 \mid [\mathbb{F}_p^* : \langle 5 \rangle] \implies 5 \mid \#\mathbb{F}_p^*
\]

\[
\implies \zeta^5 = 1, \zeta \neq 1, \text{ for some } \zeta \in \mathbb{F}_p^*,
\]

\[
\implies 2 \mid [\mathbb{F}_p^* : \langle 5 \rangle]
\]
Definition. A radical group over $K$ is a group $B$ together with an embedding $K^* \hookrightarrow B$ so that

- $B/K^*$ is torsion;
- each finite subgroup of $B$ is cyclic.
Definition. A radical group over $K$ is a group $B$ together with an embedding $K^* \hookrightarrow B$ so that

- $B/K^*$ is torsion;
- each finite subgroup of $B$ is cyclic.

The maximal radical group over $K$ is the injective hull $\sqrt[\infty]{K^*}$ of

$$K^* \oplus \bigoplus_{\mu_p \not\subset K^*} \mu_p.$$
Definition. A radical group over $K$ is a group $B$ together with an embedding $K^* \hookrightarrow B$ so that

- $B/K^*$ is torsion;
- each finite subgroup of $B$ is cyclic.

The maximal radical group over $K$ is the injective hull $\sqrt[\infty]{K^*}$ of

$$K^* \oplus \bigoplus_{\mu_p \not\subset K^*} \mu_p.$$ 

For instance:

$$\sqrt[\infty]{\mathbb{Q}^*} = 1_{\mathbb{Q}/\mathbb{Z}} \oplus \bigoplus_{p \text{ prime}} p^\mathbb{Q}.$$
Definition. A radical group over $K$ is a group $B$ together with an embedding $K^* \hookrightarrow B$ so that

- $B/K^*$ is torsion;
- each finite subgroup of $B$ is cyclic.

The maximal radical group over $K$ is the injective hull $\sqrt[\infty]{K^*}$ of

$$K^* \oplus \bigoplus_{\mu_p \not\subset K^*} \mu_p.$$ 

For instance:

$$\sqrt[\infty]{\mathbb{Q}^*} = 1^{\mathbb{Q}/\mathbb{Z}} \oplus \bigoplus_{p \text{ prime}} p^{\mathbb{Q}} \quad (1^x = e^{2\pi ix})$$
A morphism $B \rightarrow B'$ of radical groups over $K$ is a group homomorphism which is the identity on $K^*$. 
A morphism $B \to B'$ of radical groups over $K$ is a group homomorphism which is the identity on $K^*$.

**Definition.** A radical group $B$ over $K$ is **Galois** if all injective morphisms $B \to \sqrt[n]{K^*}$ have the same image.
A morphism $B \to B'$ of radical groups over $K$ is a group homomorphism which is the identity on $K^*$. 

**Definition.** A radical group $B$ over $K$ is **Galois** if all injective morphisms $B \to \sqrt[n]{K^*}$ have the same image.

Equivalently, for each $b \in B$ there is an $n \geq 1$ so that $b^n \in K^*$ and $B$ contains an element of order $n$. 
A morphism $B \to B'$ of radical groups over $K$ is a group homomorphism which is the identity on $K^*$.

**Definition.** A radical group $B$ over $K$ is **Galois** if all injective morphisms $B \to \sqrt[n]{K^*}$ have the same image.

Equivalently, for each $b \in B$ there is an $n \geq 1$ so that $b^n \in K^*$ and $B$ contains an element of order $n$.

**Proposition.** For radical groups $B \subset C$ over $K$ which are both Galois, the sequence

$$ 0 \to \text{Aut}_B(C) \to \text{Aut}_{K^*}(C) \to \text{Aut}_{K^*}(B) \to 0 $$

is an exact sequence of profinite groups.
Proposition. Suppose that $B, B' \subset C$ are radical groups over $K$ which are all Galois. Then the groups $BB'$ and $B \cap B'$ are also Galois over $K$.
Proposition. Suppose that \( B, B' \subset C \) are radical groups over \( K \) which are all Galois. Then the groups \( BB' \) and \( B \cap B' \) are also Galois over \( K \).
Proposition. Suppose that $B, B' \subset C$ are radical groups over $K$ which are all Galois. Then the groups $BB'$ and $B \cap B'$ are also Galois over $K$ and

$$\text{Aut}_{K^*}(BB') = \boxed{\text{ } \times \boxed{\text{ } \times \boxed{\text{ } \text{ }}}.$$
Suppose $B$ is a radical group over $K$ which is Galois. In two easy cases $\text{Aut}_{K^*}(B)$ is abelian:

**Case 1:** we say $B$ is *Kummer* if for all $x \in B$ there is an $n \geq 1$ so that $\mu_n \subset K^*$ and $b^n \in K^*$.
Suppose \( B \) is a radical group over \( K \) which is Galois. In two easy cases \( \text{Aut}_{K^*}(B) \) is abelian:

**Case 1:** we say \( B \) is Kummer if for all \( x \in B \) there is an \( n \geq 1 \) so that \( \mu_n \subset K^* \) and \( b^n \in K^* \). Then

\[
\text{Aut}_{K^*}(B) \cong \text{Hom}(B/K^*, \mu_K).
\]
Suppose $B$ is a radical group over $K$ which is Galois. In two easy cases $\text{Aut}_{K^*}(B)$ is abelian:

**Case 1:** we say $B$ is Kummer if for all $x \in B$ there is an $n \geq 1$ so that $\mu_n \subset K^*$ and $b^n \in K^*$. Then

\[ \text{Aut}_{K^*}(B) \cong \text{Hom}(B/K^*, \mu_K). \]

**Case 2:** we say $B$ is cyclotomic if $B = B_{\text{tor}}K^*$. If $B_{\text{tor}} = \mu_n$ with $n$ finite, and $\mu_w = \mu_n \cap K^*$ then

\[ 0 \rightarrow \text{Aut}_{K^*}(B) \rightarrow (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/w\mathbb{Z})^* \rightarrow 0. \]
Suppose $B$ is a radical group over $K$ which is Galois. In two easy cases $\text{Aut}_{K^*}(B)$ is abelian:

**Case 1:** we say $B$ is Kummer if for all $x \in B$ there is an $n \geq 1$ so that $\mu_n \subset K^*$ and $b^n \in K^*$. Then

$$\text{Aut}_{K^*}(B) \cong \text{Hom}(B/K^*, \mu_K).$$

**Case 2:** we say $B$ is cyclotomic if $B = B_{\text{tor}}K^*$. If $B_{\text{tor}} = \mu_n$ with $n$ finite, and $\mu_w = \mu_n \cap K^*$ then

$$0 \rightarrow \text{Aut}_{K^*}(B) \rightarrow (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/w\mathbb{Z})^* \rightarrow 0.$$

**Corollary.** If $n = [B : K^*]$ is finite then

$$\#\text{Aut}_{K^*}(B) = n \prod_{\mu_p \subset B, \mu_p \not\subset K^*} \frac{p - 1}{p}.$$
Given a radical group $B$ over $K$, and a $K^*$-embedding

$$\sigma : B \rightarrow \bar{K}^*$$

we can consider the field extension $L = K(\sigma B)$ of $K$.

If $B$ is Galois, then $L$ does not depend on the choice of $\sigma$. 
Given a radical group $B$ over $K$, and a $K^*$-embedding

$$\sigma : B \rightarrow K^*$$

we can consider the field extension $L = K(\sigma B)$ of $K$.

If $B$ is Galois, then $L$ does not depend on the choice of $\sigma$.

For $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[3]{2} \rangle$ the field $L$ depends on $\sigma$, but all choices give isomorphic fields.
Given a radical group $B$ over $K$, and a $K^*$-embedding

$$\sigma : B \to \overline{K}^*$$

we can consider the field extension $L = K(\sigma B)$ of $K$.

If $B$ is Galois, then $L$ does not depend on the choice of $\sigma$.

For $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[3]{2} \rangle$ the field $L$ depends on $\sigma$, but all choices give isomorphic fields.

For $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[4]{16-4} \rangle$ the number of primes lying over 5 in $L$ depends on $\sigma$. So the notation $\mathbb{Q}(\sqrt[4]{16-4})$ is ambiguous.
Given a radical group $B$ over $K$, and a $K^*$-embedding

$$\sigma : B \rightarrow \overline{K}^*$$

we can consider the field extension $L = K(\sigma B)$ of $K$.

If $B$ is Galois, then $L$ does not depend on the choice of $\sigma$.

For $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[3]{2} \rangle$ the field $L$ depends on $\sigma$, but all choices give isomorphic fields.

For $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \sqrt[16]{-4} \rangle$ the number of primes lying over 5 in $L$ depends on $\sigma$. So the notation $\mathbb{Q}(\sqrt[16]{-4})$ is ambiguous.

**Proposition.** The field degree $[L : K]$ does not depend on $\sigma$. 
Theorem 1. Let $B$ be a radical group over $K$ which is Galois. Then there is an abelian profinite quotient $E(B)$ of $\text{Aut}_{K^*}(B)$ so that for every embedding $\sigma : B \to \bar{K}^*$ the sequence

$$0 \to \text{Gal}(K(\sigma B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0$$

$$\tau \mapsto \sigma^{-1} \tau \sigma$$

is exact.
Theorem 1. Let $B$ be a radical group over $K$ which is Galois. Then there is an abelian profinite quotient $E(B)$ of $\text{Aut}_{K^*}(B)$ so that for every embedding $\sigma : B \to \bar{K}^*$ the sequence

$$0 \to \text{Gal}(K(\sigma B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0$$

$$\tau \mapsto \sigma^{-1} \tau \sigma$$

is exact.

$E(B)$ is the entanglement group of $B$ over $K$. 

Theorem 1. Let $B$ be a radical group over $K$ which is Galois. Then there is an abelian profinite quotient $E(B)$ of $\text{Aut}_{K^*}(B)$ so that for every embedding $\sigma : B \to \overline{K^*}$ the sequence

$$0 \to \text{Gal}(K(\sigma B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0$$

$$\tau \mapsto \sigma^{-1} \tau \sigma$$

is exact.

$E(B)$ is the entanglement group of $B$ over $K$.

To prove the theorem we may fix $\sigma$, and take $B \subset \overline{K^*}$. 
First examples of entanglement groups

\[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Example.** We have \( E(B) = 0 \) in two cases:

- \( B \) is **cyclotomic**, i.e., \( B = \mathbb{Q}^*B_{\text{tor}} \), and \( K = \mathbb{Q} \);
First examples of entanglement groups «

\[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Example.** We have \( E(B) = 0 \) in two cases:

- \( B \) is **cyclotomic**, i.e., \( B = Q^*B_{\text{tor}} \), and \( K = Q \);
- \( B \) is **Kummer**.
First examples of entanglement groups

\[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Example.** We have \( E(B) = 0 \) in two cases:
- \( B \) is cyclotomic, i.e., \( B = \mathbb{Q}^*B_{\text{tor}} \), and \( K = \mathbb{Q}; \)
- \( B \) is Kummer.

**Example.** Suppose that \( p \) is prime and that \( \mu_p \not\subset K^* \) then for \( B = \langle K^*, \mu_p \rangle \) we have \( \text{Aut}_{K^*}(B) = \text{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^* \).
» First examples of entanglement groups «

\[ 0 \rightarrow \text{Gal}(K(B)/K) \rightarrow \text{Aut}_{K^*}(B) \rightarrow E(B) \rightarrow 0 \]

**Example.** We have \( E(B) = 0 \) in two cases:
- \( B \) is **cyclo metric**, i.e., \( B = \mathbb{Q}^*B_{\text{tor}} \), and \( K = \mathbb{Q} \);
- \( B \) is **Kummer**.

**Example.** Suppose that \( p \) is prime and that \( \mu_p \not\subset K^* \) then for \( B = \langle K^*, \mu_p \rangle \) we have \( \text{Aut}_{K^*}(B) = \text{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^* \).

\[
\begin{align*}
\text{Gal}(K(\mu_p)/K) & \rightarrow \text{Aut}(\mu_p) \\
\downarrow & \\
\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) & \sim
\end{align*}
\]
» First examples of entanglement groups «

\[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Example.** We have \( E(B) = 0 \) in two cases:
- \( B \) is cyclotomic, i.e., \( B = \mathbb{Q}^* B_{\text{tor}} \), and \( K = \mathbb{Q} \);
- \( B \) is Kummer.

**Example.** Suppose that \( p \) is prime and that \( \mu_p \not\subset K^* \) then for \( B = \langle K^*, \mu_p \rangle \) we have \( \text{Aut}_{K^*}(B) = \text{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^* \).

\[
\begin{align*}
\text{Gal}(K(\mu_p)/K) \quad &\quad \text{Aut}(\mu_p) \\
\downarrow &\quad \sim \\
\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p) \cap K) &\quad \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})
\end{align*}
\]
First examples of entanglement groups

\[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Example.** We have \( E(B) = 0 \) in two cases:

- \( B \) is *cyclo
tomic*, i.e., \( B = \mathbb{Q}^*B_{\text{tor}} \), and \( K = \mathbb{Q} \);
- \( B \) is *Kummer*.

**Example.** Suppose that \( p \) is prime and that \( \mu_p \not\subset K^* \) then for \( B = \langle K^*, \mu_p \rangle \) we have \( \text{Aut}_{K^*}(B) = \text{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^* \).

\[
\text{Gal}(K(\mu_p)/K) \to \text{Aut}(\mu_p) \quad \Downarrow \quad \sim \\
\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p) \cap K) \quad \Leftarrow \quad \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})
\]

It follows that \( E(B) \cong \text{Gal}(\mathbb{Q}(\mu_p) \cap K/\mathbb{Q}) \).
Let $B$ be a radical group over $K$. Define the subgroup of abelian radicals of $B$ by

$$B_{ab} = \{ x \in B : \exists w \geq 1 : x^w \in K^* B_{tor} \text{ and } \mu_w \subset K^* \} ,$$

Then $B_{ab}$ is Galois and $\text{Aut}_{K^*}(B_{ab})$ is abelian.
Let $B$ be a radical group over $K$. Define the subgroup of abelian radicals of $B$ by

$$B_{ab} = \{ x \in B : \exists w \geq 1 : x^w \in K^* B_{tor} \text{ and } \mu_w \subset K^* \},$$

Then $B_{ab}$ is Galois and $\text{Aut}_{K^*}(B_{ab})$ is abelian.

**Proposition.** For $n \geq 1$, and $x$ in $B$ with $y = x^n \in K^*$ and $\mu_n \subset B$ and $\sigma : B \to \overline{K}^*$ an embedding, we have

$$x \in B_{ab} \iff \text{Aut}_{K^*}(\langle K^*, \mu_n, x \rangle) \text{ is abelian} \iff \text{Gal}(K(\mu_n, \sigma x)/K) \text{ is abelian}.$$
Let $B$ be a radical group over $K$. Define the subgroup of abelian radicals of $B$ by

$$B_{ab} = \{x \in B : \exists w \geq 1 : x^w \in K^*B_{tor} \text{ and } \mu_w \subset K^*\},$$

Then $B_{ab}$ is Galois and $\text{Aut}_{K^*}(B_{ab})$ is abelian.

**Proposition.** For $n \geq 1$, and $x$ in $B$ with $y = x^n \in K^*$ and $\mu_n \subset B$ and $\sigma : B \to \overline{K}^*$ an embedding, we have

$$x \in B_{ab} \iff \text{Aut}_{K^*}(\langle K^*, \mu_n, x \rangle) \text{ is abelian} \iff \text{Gal}(K(\mu_n, \sigma x)/K) \text{ is abelian}$$

**Proof.** Put $\mu_w = \mu_n \cap K^*$ then by Schinzel’s theorem:

$$K(\mu_n, \sigma x) \text{ is abelian over } K \iff y^w \in (K^*)^n$$
Let $B$ be a radical group over $K$. Define the subgroup of abelian radicals of $B$ by

$$B_{ab} = \{x \in B : \exists w \geq 1 : x^w \in K^*B_{tor} \text{ and } \mu_w \subset K^* \}.$$ 

Then $B_{ab}$ is Galois and $\text{Aut}_{K^*}(B_{ab})$ is abelian.

**Proposition.** For $n \geq 1$, and $x$ in $B$ with $y = x^n \in K^*$ and $\mu_n \subset B$ and $\sigma : B \to \overline{K}^*$ an embedding, we have

$$x \in B_{ab} \iff \text{Aut}_{K^*}(\langle K^*, \mu_n, x \rangle) \text{ is abelian} \iff \text{Gal}(K(\mu_n, \sigma x)/K) \text{ is abelian}$$

**Proof.** Put $\mu_w = \mu_n \cap K^*$ then by Schinzel’s theorem:

$$K(\mu_n, \sigma x) \text{ is abelian over } K \iff y^w \in (K^*)^n \iff \sigma x \in \mu_{nw}^w \sqrt{K^*}$$
Let $B$ be a radical group over $K$. Define the subgroup of abelian radicals of $B$ by

$$B_{ab} = \{ x \in B : \exists w \geq 1 : x^w \in K^* B_{tor} \text{ and } \mu_w \subset K^* \} ,$$

Then $B_{ab}$ is Galois and $\text{Aut}_{K^*}(B_{ab})$ is abelian.

**Proposition.** For $n \geq 1$, and $x$ in $B$ with $y = x^n \in K^*$ and $\mu_n \subset B$ and $\sigma : B \to \overline{K}^*$ an embedding, we have

$$x \in B_{ab} \iff \text{Aut}_{K^*}(\langle K^*, \mu_n, x \rangle) \text{ is abelian} \iff \text{Gal}(K(\mu_n, \sigma x)/K) \text{ is abelian}$$

**Proof.** Put $\mu_w = \mu_n \cap K^*$ then by Schinzel’s theorem:

$$K(\mu_n, \sigma x) \text{ is abelian over } K \iff y^w \in (K^*)^n \iff \sigma x \in \mu_n w \sqrt{K^*} \iff \sigma x^w \in \mu_n K^* \implies x \in B_{ab}$$
Theorem 1: \[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]
Proof of Theorem 1

**Theorem 1:** \[ 0 \rightarrow \text{Gal}(K(B)/K) \rightarrow \text{Aut}_{K^*}(B) \rightarrow E(B) \rightarrow 0 \]

**Proof.** Put \( A = B_{ab} \), then we have an exact sequence

\[
\begin{array}{cccccc}
0 & \rightarrow & \text{Aut}_A(B) & \rightarrow & \text{Aut}_{K^*}(B) & \rightarrow & \text{Aut}_{K^*}(A) & \rightarrow & 0 \\
& \uparrow f & & \uparrow g & & \uparrow h & \\
0 & \rightarrow & \text{Gal}(\frac{K(B)}{K(A)}) & \rightarrow & \text{Gal}(\frac{K(B)}{K}) & \rightarrow & \text{Gal}(\frac{K(A)}{K}) & \rightarrow & 0
\end{array}
\]
Proof of Theorem 1

**Theorem 1:** \[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Proof.** Put \( A = B_{ab} \), then we have an exact sequence

\[
\begin{array}{cccccc}
0 & \longrightarrow & \text{Aut}_A(B) & \longrightarrow & \text{Aut}_{K^*}(B) & \longrightarrow & \text{Aut}_{K^*}(A) & \longrightarrow & 0 \\
& & \uparrow f & & \uparrow g & & \uparrow h & & \\
0 & \longrightarrow & \text{Gal}(\frac{K(B)}{K(A)}) & \longrightarrow & \text{Gal}(\frac{K(B)}{K}) & \longrightarrow & \text{Gal}(\frac{K(A)}{K}) & \longrightarrow & 0
\end{array}
\]

By Kummer theory the image of \( f \) is \( \text{Aut}_{B \cap K(A)}(B) \).
By Schinzel \( B \cap K(A) = A \), so \( f \) is an isomorphism.
Theorem 1:  \[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Proof.** Put \( A = B_{ab} \), then we have an exact sequence

\[
\begin{array}{ccccccc}
0 & \longrightarrow & \text{Aut}_A(B) & \longrightarrow & \text{Aut}_{K^*}(B) & \longrightarrow & \text{Aut}_{K^*}(A) & \longrightarrow & 0 \\
\uparrow f & & \uparrow g & & \uparrow h & & \uparrow & \\
0 & \longrightarrow & \text{Gal}(\frac{K(B)}{K(A)}) & \longrightarrow & \text{Gal}(\frac{K(B)}{K}) & \longrightarrow & \text{Gal}(\frac{K(A)}{K}) & \longrightarrow & 0
\end{array}
\]

By Kummer theory the image of \( f \) is \( \text{Aut}_{B \cap K(A)}(B) \).
By **Schinzel** \( B \cap K(A) = A \), so \( f \) is an isomorphism.
The image of \( h \) is normal, because \( \text{Aut}_{K^*}(A) \) is abelian.
Thus, \( g \) has normal image, and \( \text{cok}(g) \cong \text{cok}(h) \) is abelian. \( \square \)
Theorem 1:  \[ 0 \to \text{Gal}(K(B)/K) \to \text{Aut}_{K^*}(B) \to E(B) \to 0 \]

**Proof.** Put \( A = B_{ab} \), then we have an exact sequence

\[
\begin{array}{cccccc}
0 & \longrightarrow & \text{Aut}_A(B) & \longrightarrow & \text{Aut}_{K^*}(B) & \longrightarrow & \text{Aut}_{K^*}(A) & \longrightarrow & 0 \\
& & f & & g & & h \\
0 & \longrightarrow & \text{Gal}\left(\frac{K(B)}{K(A)}\right) & \longrightarrow & \text{Gal}\left(\frac{K(B)}{K}\right) & \longrightarrow & \text{Gal}\left(\frac{K(A)}{K}\right) & \longrightarrow & 0
\end{array}
\]

By Kummer theory the image of \( f \) is \( \text{Aut}_{B \cap K(A)}(B) \).
By **Schinzel** \( B \cap K(A) = A \), so \( f \) is an isomorphism.
The image of \( h \) is normal, because \( \text{Aut}_{K^*}(A) \) is abelian.
Thus, \( g \) has normal image, and \( \text{cok}(g) \cong \text{cok}(h) \) is abelian. \( \Box \)

**Corollary.** The restriction map \( E(B) \to E(B_{ab}) \) is an isomorphism.
For a radical group $B$ over $K$ which is Galois, we put

$$K\{B\} = K[B] \otimes_{K[K^*]} K$$

$$K\langle B \rangle = S^{-1}K\{B\}, \quad S = \langle x - 1 : x \in B, x \neq 1 \rangle$$

$$K[B] \rightarrow K\{B\} \rightarrow K\langle B \rangle \rightarrow K(\sigma B) \subset \overline{K} \quad \sigma : B \rightarrow \overline{K}^*$$
For a radical group $B$ over $K$ which is Galois, we put

$$K\{B\} = K[B] \otimes_{K[K^*]} K$$

$$K\langle B \rangle = S^{-1}K\{B\}, \quad S = \langle x - 1: \ x \in B, x \neq 1 \rangle$$

$$K[B] \to K\{B\} \to K\langle B \rangle \to K(\sigma B) \subset \bar{K} \quad \sigma: \ B \to \bar{K}^*$$

If $B$ is Galois, then $K\langle B \rangle$ is a Galois algebra with group $\text{Aut}_{K^*}(B)$. Its invariants $K\langle B \rangle_{\text{spl}}$ under $\text{Gal}(K(\sigma B)/K)$ form a split $K$-algebra, whose components form an $E(B)$-torsor.
For a radical group $B$ over $K$ which is Galois, we put

$$K\{B\} = K[B] \otimes_{K[K^*]} K$$

$$K\langle B \rangle = S^{-1}K\{B\}, \quad S = \langle x - 1: \ x \in B, x \neq 1 \rangle$$

$$K[B] \to K\{B\} \to K\langle B \rangle \to K(\sigma B) \subset \bar{K} \quad \sigma: \ B \to \bar{K}^*$$

If $B$ is Galois, then $K\langle B \rangle$ is a Galois algebra with group $\text{Aut}_{K^*}(B)$. Its invariants $K\langle B \rangle_{\text{spl}}$ under $\text{Gal}(K(\sigma B)/K)$ form a split $K$-algebra, whose components form an $E(B)$-torsor.

**Example.** For $B = \langle \mathbb{Q}^*, \sqrt{-3}, \zeta \rangle$ with $\zeta = \sqrt[3]{1}$ we have $\mathbb{Q}\langle B \rangle_{\text{spl}} = \mathbb{Q} \oplus x\mathbb{Q}$ where $x = (\zeta - \zeta^2)\sqrt{-3}$ satisfies $x^2 = 9$. 
For a radical group $B$ over $K$ which is Galois, we put

$$K\{B\} = K[B] \otimes_{K[K^*]} K$$

$$K\langle B \rangle = S^{-1}K\{B\}, \quad S = \langle x - 1 : x \in B, x \neq 1 \rangle$$

$$K[B] \to K\{B\} \to K\langle B \rangle \to K(\sigma B) \subset \overline{K} \quad \sigma: B \to \overline{K}^*$$

If $B$ is Galois, then $K\langle B \rangle$ is a Galois algebra with group $\text{Aut}_{K^*}(B)$. Its invariants $K\langle B \rangle_{\text{spl}}$ under $\text{Gal}(K(\sigma B)/K)$ form a split $K$-algebra, whose components form an $E(B)$-torsor.

**Example.** For $B = \langle \mathbb{Q}^*, \sqrt{-3}, \zeta \rangle$ with $\zeta = \sqrt[3]{1}$ we have $\mathbb{Q}\langle B \rangle_{\text{spl}} = \mathbb{Q} \oplus x\mathbb{Q}$ where $x = (\zeta - \zeta^2)\sqrt{-3}$ satisfies $x^2 = 9$.

**Note.** Even if $B$ is not Galois, $B_{\text{ab}}$ is Galois, and the components of $K\langle B \rangle$ are an $E(B_{\text{ab}})$-torsor.
Let $B$ be a radical group over $K$, let $\mu \subset B_{\text{tor}}$ and let $W \subset B$ be a radical group over $K$ which is Kummer, i.e., for all $x \in W$ there is a $w \geq 1$ with $x^w \in K$ and $\mu_w \subset K^*$.

**Theorem 2.** We have a natural isomorphism

$$E(\mu W) \to \text{Gal}(\mathbb{Q}(\mu) \cap K(W)/\mathbb{Q}(\mu \cap W))$$.
Let $B$ be a radical group over $K$, let $\mu \subset B_{\text{tor}}$ and let $W \subset B$ be a radical group over $K$ which is Kummer, i.e., for all $x \in W$ there is a $w \geq 1$ with $x^w \in K$ and $\mu_w \subset K^*$.

**Theorem 2.** We have a natural isomorphism

$$E(\mu W) \rightarrow \text{Gal}(\mathbb{Q}(\mu) \cap K(W)/\mathbb{Q}(\mu \cap W)).$$

Taking $K = \mathbb{Q}$ and $W = \langle \sqrt[p]{p} : p \text{ prime} \rangle$, and $\mu$ all roots of unity, we find that $(\sqrt[\infty]{\mathbb{Q}^*})_{\text{ab}} = \mu W$. Combining the two theorems:

$$E_{\mathbb{Q}} = E(\sqrt[\infty]{\mathbb{Q}^*}) = \text{Gal}(\mathbb{Q}(W)/\mathbb{Q}) = \{1, -1\}^{\{\text{primes}\}}$$
\[ \text{Proof of Theorem 2 «}\]

Diagram:
- \( \mu W \) connected to \( \mu K^* \) and \( W \).
- \( \mu K^* \) connected to \( W \) and \( K^* \).
- \( K(\mu W) \) connected to \( K(\mu) \) and \( K(W) \).
- \( K(\mu) \) connected to \( K(W) \) and \( K \).
Proof of Theorem 2

\[ \text{Aut}_{K^*}(\mu W) = \Box \times \Box \times \Box \]

\[ \text{Gal}(K(\mu W)/K) = \Box \times \Box \times \Box \]
Proof of Theorem 2

\[
\text{Aut}_{K^*}(\mu W) = \square \times \square \times \square
\]

\[
\text{Gal}(K(\mu W)/K) = \bigcirc \times \bigcirc \times \bigcirc
\]
Proof of Theorem 2

\[ \text{Aut}_{K^*}(\mu W) = \square \times \square \]

\[ \text{Gal}(K(\mu W)/K) = \square \times \square \]
Proof of Theorem 2

\[
\text{Aut}_{K^*}(\mu W) = \square \times \square
\]

\[
\text{Gal}(K(\mu W)/K) = \square \times \square = \square \times \square
\]
Proof of Theorem 2

\[ \text{Aut}_{K^*}(\mu W) = \]
\[ \text{Gal}(K(\mu W)/K) = \]
Proof of Theorem 2

\[
\text{Aut}_{K^*}(\mu W) = \boxtimes \times \blacksquare \times \mbox{red square}
\]

\[
\text{Gal}(K(\mu W)/K) = \boxtimes \times \blacksquare \times \mbox{red square}
\]
For applications one often needs to understand the map

\[ \text{Aut}_{K^*}(\mu W) \rightarrow E(\mu W) \cong \text{Gal}(\mathbb{Q}(\mu) \cap K(W)/\mathbb{Q}(\mu \cap W)). \]
For applications one often needs to understand the map

$$\text{Aut}_{K^*}(\mu W) \to E(\mu W) \cong \text{Gal}(\mathbb{Q}(\mu) \cap K(W)/\mathbb{Q}(\mu \cap W)).$$

It is the difference of two restriction maps:

$$\text{Aut}_{K^*}(\mu W) \to \text{Aut}(\mu) \cong \text{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}(\mu) \cap K(W)/\mathbb{Q}).$$

and

$$\text{Aut}_{K^*}(\mu W) \to \text{Aut}_{K^*}(W) \cong \text{Gal}(K(W)/K) \to \text{Gal}(K(W) \cap \mathbb{Q}(\mu)/\mathbb{Q}).$$
Suppose that \( a \in \mathbb{Q} \) so that \( a \) and \(-a\) are not squares. Let

\[
B = \langle \mathbb{Q}^*, \sqrt[4]{-a^2} \rangle = B_{ab}
\]

Note that \( \sqrt{-1} \in B \), so \( B \) is Galois.
Suppose that \( a \in \mathbb{Q} \) so that \( a \) and \(-a\) are not squares. Let

\[
B = \langle \mathbb{Q}^*, \sqrt[4]{-a^2} \rangle = B_{ab}
\]

Note that \( \sqrt{-1} \in B \), so \( B \) is Galois.
We have \( B \subset \mu_8 W \) with \( W = \langle \mathbb{Q}^*, \sqrt{a} \rangle \) and

\[
E(\mu_8 W) = \text{Gal}(\mathbb{Q}(\mu_8) \cap \mathbb{Q}(\sqrt{a}) / \mathbb{Q}(\mu_8 \cap W))
\]

\[
= 0 \text{ if } 2a, -2a \notin \mathbb{Q}^2
\]

\[
\cong \mathbb{Z}/2\mathbb{Z} \text{ otherwise}
\]
Suppose that $a \in \mathbb{Q}$ so that $a$ and $-a$ are not squares. Let 

$$B = \langle \mathbb{Q}^*, \sqrt[4]{-a^2} \rangle = B_{ab}$$

Note that $\sqrt{-1} \in B$, so $B$ is Galois. We have $B \subset \mu_8 W$ with $W = \langle \mathbb{Q}^*, \sqrt{a} \rangle$ and

$$E(\mu_8 W) = \text{Gal}(\mathbb{Q}(\mu_8) \cap \mathbb{Q}(\sqrt{a})/\mathbb{Q}(\mu_8 \cap W))$$

$$= 0 \text{ if } 2a, -2a \notin \mathbb{Q}^*$$

$$\cong \mathbb{Z}/2\mathbb{Z} \text{ otherwise}$$

We can now compute $E(B)$ from the exact sequence

$$\text{Aut}_B(\mu_8 W) \to E(\mu_8 W) \to E(B) \to 0$$
Goal: “Compute” $E(\sqrt[\infty]{K^*})$.

Let $\Gamma_K$ be the image of $\text{Gal}(\overline{K}/K)$ in $\text{Aut}(\mu) = \hat{\mathbb{Z}}^*$.

Let $w_K = \text{Ann}_{\hat{\mathbb{Z}}}(K^*_{\text{tor}})$, let $\mu = \sqrt[\infty]{K^*_{\text{tor}}}$.

Let $W = \{\text{Kummer radicals}\} = \{x \in \sqrt[\infty]{K^*} : (x \mod K^*)^{w_K} = 1\}$. 

» The absolute entanglement group «

![Diagram]

- $\mathbb{Q}(\mu)$
- $\mathbb{Q}(\mu) \cap K(W)$
- $(1 + w_K) \cap \hat{\mathbb{Z}}^*$
- $\mathbb{Q}(\mu \cap W)$
- $\mathbb{Q}(\mu \cap K)$
- $\mathbb{Q}(\mu \cap K^*)$
- $\Gamma_K$
Goal: “Compute” \( E(\sqrt[\infty]{K^*}) \).

Let \( \Gamma_K \) be the image of \( \text{Gal}(\overline{K}/K) \) in \( \text{Aut}(\mu) = \hat{\mathbb{Z}}^* \).
Let \( w_K = \text{Ann}_{\hat{\mathbb{Z}}}(K_{\text{tor}}^*) \), let \( \mu = \sqrt[\infty]{K_{\text{tor}}^*} \).
Let \( W = \{ \text{Kummer radicals} \} = \{ x \in \sqrt[\infty]{K^*} : (x \mod K^*)^{w_K} = 1 \} \).

\[
E(\sqrt[\infty]{K^*}) = E(\mu W)
\]
Goal: “Compute” $E(\sqrt[\infty]{K^*})$.

Let $\Gamma_K$ be the image of $\text{Gal}(\overline{K}/K)$ in $\text{Aut}(\mu) = \hat{\mathbb{Z}}^*$.
Let $w_K = \text{Ann}_{\hat{\mathbb{Z}}}(K^*_\text{tor})$, let $\mu = \sqrt[\infty]{K^*_\text{tor}}$.
Let $W = \{\text{Kummer radicals}\} = \{x \in \sqrt[\infty]{K^*} : (x \mod K^*)^{w_K} = 1\}$.

$$E(\sqrt[\infty]{K^*}) = E(\mu W)$$
Goal: “Compute” $E(\sqrt[\infty]{K^*)}$.

Let $\Gamma_K$ be the image of $\text{Gal}(\overline{K}/K)$ in $\text{Aut}(\mu) = \hat{\mathbb{Z}}^*$. Let $w_K = \text{Ann}_{\hat{\mathbb{Z}}}(K_{\text{tor}}^*)$, let $\mu = \sqrt[\infty]{K^*}_{\text{tor}}$. Let $W = \{\text{Kummer radicals}\} = \{x \in \sqrt[\infty]{K^*} : (x \mod K^*)^{w_K} = 1\}$.

$$E(\sqrt[\infty]{K^*}) = E(\mu W)$$
Goal: “Compute” $E(\sqrt[K^*]{})$.

Let $\Gamma_K$ be the image of $\text{Gal}(\overline{K}/K)$ in $\text{Aut}(\mu) = \hat{\mathbb{Z}}^*$.
Let $w_K = \text{Ann}_{\hat{\mathbb{Z}}}(K^*_{\text{tor}})$, let $\mu = \sqrt[K^*_{\text{tor}}]{\cdot}$.
Let $W = \{\text{Kummer radicals}\} = \{x \in \sqrt[K^*]{\cdot} : (x \mod K^*)^{w_K} = 1\}$.

$E(\sqrt[K^*]{\cdot}) = E(\mu W)$
$\cong (1 + w_K^2) \cap \hat{\mathbb{Z}}^*/\Gamma_K^{w_K}$