Radicals in arithmetic

Palenstijn, W.J.

Chapter 3

The absolute entanglement group

3.1 Introduction

Let K be a field, and choose a fixed separable closure K^{sep}. Define $\sqrt[\infty]{K^*} \subset K^{\mathrm{sep}*}$ as the group of all radicals over K^* inside $K^{\mathrm{sep}*}$. The entanglement group of $\sqrt[\infty]{K^*}$ with the action of the absolute Galois group G of K is of particular interest. We refer to this entanglement group as the *absolute entanglement group* of K, and write $E_{\mathrm{abs}}(K)$. Recall from Theorem 2.25 and Definition 2.26 that we have the following exact sequence that defines $E_{\mathrm{abs}}(K)$:

$$G \to \mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*}) \to E_{\mathrm{abs}}(K) \to 1.$$

If K has characteristic 0, this maximal radical extension $\sqrt[\infty]{K^*}$ coincides with the group $\overline{K^*}$ defined in section 2.2. For characteristic $p > 0$, the same is true if we make the adjustments mentioned in Remark 2.11.

If $B \subset \sqrt[\infty]{K^*}$ is any Galois radical extension of K^*, then the restriction map from $\mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*})$ to $\mathrm{Aut}_{K^*}(B)$ induces a surjection $E_{\mathrm{abs}}(K) \to E(B)$, so every entanglement group over K^* is a quotient of $E_{\mathrm{abs}}(K)$.

Before stating the main results of this chapter in Section 3.3, we first cover preliminaries on $\hat{\mathbf{Z}}$-ideals and Steinitz numbers in Section 3.2. The proofs of the main results are in Section 3.3 and Section 3.4, with the latter section treating the case of positive characteristic.

The result for characteristic zero was already announced in the lecture notes for Colloquium Lectures by H.W. Lenstra on Entangled Radicals [19] at the AMS Annual Meeting in 2006.

3.2 Preliminaries

In order to state the main results of this chapter, we first introduce some concepts related to the profinite groups concerned.

We define Z to be the endomorphism ring $\mathrm{End}(\mu)$ of the group μ of roots of unity of K^{sep}. The automorphism group $\mathrm{Aut}(\mu)$ is then equal to Z^*. Note that if K has characteristic 0, then Z is isomorphic to $\hat{\mathbf{Z}} \cong \prod_l \mathbf{Z}_l$, and if K has characteristic $p > 0$, then it is isomorphic to $\prod_{l \neq p} \mathbf{Z}_l$.

A convenient way to describe closed $\hat{\mathbf{Z}}$-ideals (and Z-ideals) is given by *Steinitz numbers*.

By unique factorization a positive integer can be uniquely written as a product $\prod_l l^{n(l)}$, where l ranges over the prime numbers, and $n(l)$ is a non-negative integer that is zero at all but finitely many l.

A Steinitz number is a formal expression of the form $\prod_l l^{n(l)}$, where $n(l)$ is an element of $\mathbf{Z}_{\geq 0} \cup \{\infty\}$ and l again ranges over the primes. Here infinitely many $n(l)$ may be non-zero. Steinitz numbers form a multiplicative monoid, containing the positive integers.

Given a Steinitz number n and an (additively written) profinite abelian group A, we define the $\hat{\mathbf{Z}}$-submodule nA of A by

$$nA = \bigcap_{\substack{m \mid n \\ m \in \mathbf{Z}_{\geq 1}}} mA.$$

Using that A is a product of pro-l-groups, one sees that nA equals $(n\hat{\mathbf{Z}})A$. If A is a profinite ring, then nA is in fact a closed A-ideal. For multiplicatively written A, we write A^n instead of nA.

One can check that this gives rise to an isomorphism between the monoid of Steinitz numbers and the monoid of closed $\hat{\mathbf{Z}}$-ideals given by $n \mapsto n\hat{\mathbf{Z}}$. If I is a closed $\hat{\mathbf{Z}}$-ideal, then I is equal to $n\hat{\mathbf{Z}}$ for the Steinitz number $n = \prod_l l^{n(l)}$ defined by

$$n(l) = \sup\{k \in \mathbf{Z}_{\geq 0} : I \subset l^k \hat{\mathbf{Z}}\}.$$

Let us write

$$\mathcal{S} = \{\text{Steinitz numbers } n = \prod_l l^{n(l)} \text{ with } n(p) = 0 \text{ if } p = \mathrm{char}(K) > 0\}.$$

We obtain a bijection

$$\mathcal{S} \longrightarrow \{\text{closed } Z\text{-ideals}\}$$

that sends n to nZ.

For a positive integer m, we write $\mu_m \subset \bar{K}^*$ for the m-th roots of unity in $\bar{K}$. If n is a Steinitz number in $\mathcal{S}$, we define μ_n as the union of all finite subgroups μ_m for $m \in \mathbf{Z}_{\geq 1}$ with $m \mid n$. Every subgroup of μ is of this form for a unique $n \in \mathcal{S}$, and the annihilator $\mathrm{Ann}_Z(\mu_n)$ of μ_n in Z is equal to nZ.

3.3 Main results

We use the notation of μ, Z, $\mathcal{S}$ from the previous section. The absolute Galois group G of K acts on μ, and we define Γ to be the image of G in Z^* of this action:

$$\Gamma = \operatorname{im}\left[\operatorname{Gal}(K^{\mathrm{sep}}/K) \longrightarrow \operatorname{Aut}(\mu) = Z^*\right] \subset Z^*.$$

Also define W as

$$W = \{x \in \sqrt[\infty]{K^*} : \exists w \in \mathbf{Z}_{>0} : x^w \in K^* \text{ and } K^* \text{ contains an element of order } w\},$$

the "Kummer part" of $\sqrt[\infty]{K^*}$ over K^*.

Finally, we define $w \in \mathcal{S}$ to be the Steinitz number for which wZ is the closure of the Z-ideal generated by $\{1-\gamma : \gamma \in \Gamma\}$. If n is a positive integer not divisible by the characteristic of K, then we have the equivalences

$$n \mid w \Leftrightarrow \forall \gamma \in \Gamma : \gamma \equiv 1 \bmod n \Leftrightarrow \mu_n \subset \mu \cap K.$$

From this we conclude that $\mu \cap K$ equals μ_w.

Theorem 3.1. *There is an isomorphism*

$$E_{\mathrm{abs}}(K) \xrightarrow{\sim} \left(Z^* \cap (1 + w^2 Z)\right) / \Gamma^w,$$

that, for each $\sigma \in \operatorname{Aut}_{K^*}(\sqrt[\infty]{K^*})$ and $g \in G$ with $g|_W = \sigma|_W$, sends $\bar{\sigma} \in E_{\mathrm{abs}}(K)$ to $\sigma|_\mu (g|_\mu)^{-1}$.

In characteristic $p > 0$ there is in fact an alternative easier description of $E_{\mathrm{abs}}(K)$ since all entanglement turns out to be visible on the roots of unity.

Proposition 3.2. *If K is of characteristic $p > 0$, the natural restriction map $E_{\mathrm{abs}}(K) \to E(\mu)$ is an isomorphism.*

Corollary 3.3. *Suppose K has characteristic $p > 0$. Define the Steinitz number a by*

$$\forall m \in \mathbf{Z}_{\geq 1} : \; m \mid a \Leftrightarrow \mathbf{F}_{p^m} \subset K.$$

Then the restriction map $\operatorname{Aut}(\sqrt[\infty]{K^*}) \to \operatorname{Aut}(\mu)$ induces an isomorphism of the absolute entanglement group of K to

$$\left(Z^* \cap (1 + wZ)\right) / p^a \hat{\mathbf{Z}},$$

where p is considered as an element of the $\hat{\mathbf{Z}}$-module Z^*.

The Steinitz number a defined in this Corollary satisfies that for positive integers m we have $m \mid a \Leftrightarrow p^m - 1 \mid w$, so the Steinitz numbers w and a uniquely determine each other.

Example 3.4.

We compute the absolute entanglement group of $\mathbf{Q}$ as an illustration of Theorem 3.1.

We are in characteristic zero, so Z simply equals $\hat{\mathbf{Z}}$. Also, since $\mathbf{Q}$ has exactly two roots of unity, w is the integer 2. The restriction map of $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q})$ to $\mathrm{Aut}(\mu)$ is an isomorphism, so the image Γ of the action of the absolute Galois group of $\mathbf{Q}$ in $\mathrm{Aut}(\mu) \cong \hat{\mathbf{Z}}^*$ is the full group $\hat{\mathbf{Z}}^*$.

We now turn to the expression from Theorem 3.1 for the absolute entanglement group of $\mathbf{Q}$.

$$E_{\mathrm{abs}}(\mathbf{Q}) \cong \left(Z^* \cap (1 + w^2 Z)\right) / \Gamma^w$$

Rewriting this with the observations made above, we obtain the following.

$$E_{\mathrm{abs}}(\mathbf{Q}) \cong \left(\hat{\mathbf{Z}}^* \cap (1 + 4\hat{\mathbf{Z}})\right) \Big/ (\hat{\mathbf{Z}}^*)^2$$

Using the fact that we can identify $\hat{\mathbf{Z}}^*$ with $\prod_p \mathbf{Z}_p^*$, we see that $\hat{\mathbf{Z}}^* \cap (1+4\hat{\mathbf{Z}})$ corresponds to $(1+4\mathbf{Z}_2) \times \prod_{p \text{ odd}} \mathbf{Z}_p^*$, since 4 is invertible in Z_p^* for odd primes p. Also, $(\hat{\mathbf{Z}}^*)^2$ corresponds to $(1 + 8\mathbf{Z}_2) \times \prod_{p \text{ odd}} (\mathbf{Z}_p^*)^2$.

At the prime 2, the quotient $(1 + 4\mathbf{Z}_2)/(1 + 8\mathbf{Z}_2)$ is isomorphic to $\mathbf{Z}/2\mathbf{Z}$, and at odd primes p, the quotient $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^2$ is also isomorphic to $\mathbf{Z}/2\mathbf{Z}$. If we write $\mathcal{P}$ for the set of primes, we conclude that the absolute entanglement group of $\mathbf{Q}$ is isomorphic to

$$E = \{\pm 1\}^{\mathcal{P}}.$$

An explicit map from $A = \mathrm{Aut}_{\mathbf{Q}^*}(\sqrt[\infty]{\mathbf{Q}^*})$ to E can also be derived from the theorem.

We start with some notation. For $a \in \hat{\mathbf{Z}}^*$ and p a prime number, we let $(\frac{a}{p}) \in \{\pm 1\}$ be the Kronecker symbol. Recall that for odd p we have $(\frac{a}{p}) = 1$ if and only if a is a square mod p, and $(\frac{a}{2}) = 1$ if and only if $k \equiv \pm 1 \bmod 8$.

Then, for a prime p, write $p^* = (\frac{-1}{p})p$. Finally, given $\sigma \in A$, define $a_\sigma \in \hat{\mathbf{Z}}^*$ as the image of $\sigma|_\mu$ under the isomorphism $\mathrm{Aut}(\mu) \cong \hat{\mathbf{Z}}^*$. Note that for $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and p prime, we have $(\frac{a_\sigma}{p}) = 1 \Leftrightarrow \sigma(\sqrt{p^*}) = \sqrt{p^*}$.

The homomorphism from A to E is then given by

$$\begin{array}{ccc} A & \longrightarrow & \{\pm 1\}^{\mathcal{P}} = E \\ \sigma & \longmapsto & \left(p \mapsto \dfrac{\sigma(\sqrt{p^*})}{\sqrt{p^*}} \cdot \left(\dfrac{a_\sigma}{p}\right)\right) \end{array}$$

In the remainder of this section we will prove Theorem 3.1. The other two results on positive characteristic are the topic of Section 3.4.

Proof of Theorem 3.1. The absolute entanglement group E_{abs} is equal to the entanglement group $E(B_{\mathrm{ab}})$ of the maximal abelian part B_{ab} of $B = \sqrt[\infty]{K^*}$ by Corollary 2.27.

To determine this entanglement group we proceed via Corollary 2.29.

Recall the definition of B_{ab}, transformed into the typical multiplicative notation for K^*:

$$B_{\mathrm{ab}} = \{x \in B : \exists w \in \mathbf{Z}_{>0} : x^w \in B_{\mathrm{tors}} \cdot B^G \text{ and } B^G \text{ has an element of order } w\}.$$

In our situation the abelian group B_{tors} is divisible by integers coprime to the characteristic p, so we have $B_{\mathrm{ab}} = \mu \cdot W$.

The Kummer part W has no entanglement as $E(W)$ is trivial by Theorem 2.14, so with $D = \mu$ and $C = W$ we can invoke Corollary 2.29 to get an expression for the entanglement group $E(B_{\mathrm{ab}})$ and corresponding map from $\mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*})$.

We get the isomorphism

$$\varphi : E_{\mathrm{abs}} \xrightarrow{\sim} \mathrm{Aut}_{\mu \cap W}(\mu)/\mathrm{im}(G_W), \tag{3.5}$$

where G_W is the kernel of the map $G \to \mathrm{Aut}(W)$ induced by the action of G. Still according to Corollary 2.29, for any $\bar{\sigma} \in E(B_{\mathrm{ab}})$ with $\sigma \in \mathrm{Aut}(B)$, there exists $g \in G$ such that $\sigma|_W = g|_W$, and $\varphi(\bar{\sigma})$ is given by $\sigma|_\mu (g|_\mu)^{-1}$.

To reach the expression from the present Theorem, we will use the following proposition.

Proposition 3.6. *The ideal wZ is the annihilator in Z of $\mu \cap K$, and $w^2 Z$ is the annihilator in Z of $\mu \cap W$.*

Proof. Since $\mu \cap W$ equals μ_w, we find that $\mathrm{Ann}_Z(\mu \cap K)$ equals wZ.

Next, we remark that because the action of G is continuous, annihilators are closed Z-ideals and are therefore given by Steinitz numbers, and a Steinitz number is uniquely defined by the set of positive integers dividing it.

For the second statement, it suffices to show that $\mu \cap W$ equals μ_{w^2}, or equivalently, that for every positive integer n, the finite group μ_n is contained in $\mu \cap W$ if and only if n divides w^2.

Suppose $\mu \cap W$ contains an element of order n. Then there exists m such that we have $x^m \in \mu \cap K$ and $\mu_m \subset K$. This implies that n divides wm and m divides w, so n divides w^2.

Conversely, if n divides w^2, then there is a positive integer $m \mid n$ such that $m \mid w$ and $\frac{n}{m} \mid w$, which is easy to see per prime. Then any element x of order dividing n satisfies $x^m \in \mu \cap K$ and $\mu_m \subset K$, so x is in $\mu \cap W$. □

A direct corollary of this proposition is that if the number of roots of unity $\#(\mu \cap K)$ in K is finite, then w is the integer $\#(\mu \cap K)$.

We now continue with the proof of the main Theorem 3.1.

Since $w^2 Z$ is the annihilator in Z of $\mu \cap W$, the elements of Z^* that are 1 mod $w^2 Z$ are exactly those that fix $\mu \cap W$ pointwise. Therefore $Z^* \cap (1 + w^2 Z)$ is equal to $\mathrm{Aut}_{\mu \cap W}(\mu)$.

Recall that G_W is the kernel of the map $G \to \mathrm{Aut}(W)$ induced by the Galois action, i.e., the subgroup of G corresponding to the maximal Kummer extension of K in K^{sep}. This subgroup G_W is the intersection of all subgroups of G corresponding

to Kummer extensions of finite exponent, which are given by G^n with n ranging over the positive integers dividing the Steinitz number w.

We conclude that G_W is equal to G^w. Since the image of G in $\mathrm{Aut}(\mu)$ is defined to be Γ, the image of G_W in Aut_μ is given by Γ^w.

The expression from this theorem now immediately follows from the map 3.5. □

3.4 Positive characteristic

We continue with the proofs of Proposition 3.2 and Corollary 3.3, for the case where the characteristic p of K is positive.

Proof of Proposition 3.2. Applying the combination of Theorem 2.28 and Equation 2.30 to $C = \mu$ and $D = W$, we can observe that the absolute entanglement group fits into the following short exact sequence:

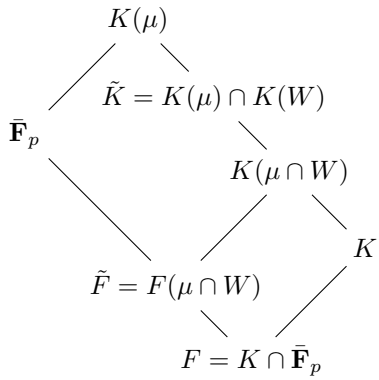
$$1 \to \mathrm{Aut}_{B^G(\mu \cap W)}(W^{G_\mu}) \to E_{\mathrm{abs}} \to E(\mu) \to 1 \tag{3.7}$$

Both W^{G_μ} and $B^G(\mu \cap W)$ are Kummer radical extensions of B^G. We claim these two groups are in fact equal. By Kummer duality there is a natural bijection between Kummer radical extensions of B^G and Kummer field extensions of K, so we can proceed by verifying they are both equal to the group of radicals of the same Kummer (field) extension of K.

We first look at W^{G_μ}. The kernel G_μ of the map $G \to \mathrm{Aut}(\mu)$ is the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K(\mu))$, so W^{G_μ} equals $W \cap K(\mu)$. Now consider the Kummer extension $K(W) \cap K(\mu)$ over K. Its radical group is given by $(K(W) \cap K(\mu))^* \cap W = W \cap K(\mu)^* = W^{G_\mu}$, so we conclude by Kummer duality that $K(W^{G_\mu}) = K(W) \cap K(\mu)$.

Next we turn to $B^G(\mu \cap W)$. This group generates the field $K(B^G(\mu \cap W)) = K(\mu \cap W)$.

We will now prove that the fields $K(\mu \cap W)$ and $K(W) \cap K(\mu)$ are one and the same. To see this, we take the intersection with $\bar{\mathbf{F}}_p$.



Since $\bar{\mathbf{F}}_p$ equals $\mu \cup \{0\}$, the maximal Kummer extension $\tilde{F}$ of F inside $\bar{\mathbf{F}}_p$ is generated by roots of unity. Since all roots of unity of K are contained in $F = K \cap \bar{\mathbf{F}}_p$, this implies that $\tilde{F} = F(\mu \cap W)$. The maximal Kummer extension of K inside $K(\mu)$ is given by $\tilde{K} = K(\mu) \cap K(W)$.

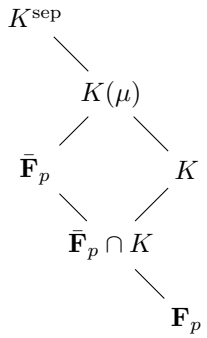
Because the roots of unity of K are exactly the roots of unity of F, the maximal Kummer extension of K inside $K(\mu)$ corresponds with the maximal Kummer extension of F inside $F(\mu) = \bar{\mathbf{F}}_p$ when taking intersections with $\bar{\mathbf{F}}_p$. We get the identity $\tilde{F} = \tilde{K} \cap \bar{\mathbf{F}}_p$, or, $F(\mu \cap W) = \tilde{K} \cap \bar{\mathbf{F}}_p$. We conclude that $\tilde{K}$ equals $K(\mu \cap W)$, as desired.

Combining these results leads to the fact that the group $\mathrm{Aut}_{B^G(\mu \cap W)}(W^{G_\mu})$ is trivial, and E_{abs} is equal to $E(\mu)$ according to the sequence 3.7. □

Proof of Corollary 3.3. It follows from Proposition 3.2 that the restriction map of $\mathrm{Aut}_{K^*}(\sqrt[\infty]{K^*})$ to $\mathrm{Aut}(\mu)$ induces an isomorphism of E_{abs} to $\mathrm{Aut}_{\mu \cap K}(\mu)/\Gamma$.

Since wZ is the annihilator of $(\mu \cap K)$, the elements of Z^* that fix $\mu \cap K$ pointwise are exactly those that are 1 mod wZ. Therefore $Z^* \cap (1 + wZ)$ is equal to $\mathrm{Aut}_{\mu \cap K}(\mu)$.

To conclude, recall that Γ is defined as the image of the restriction homomorphism $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\mu)$. Since $\bar{\mathbf{F}}_p$ equals $\mu \cup \{0\}$, this map factors via the Galois group $\mathrm{Gal}(\bar{\mathbf{F}}_p \cap K(\mu)/\bar{\mathbf{F}}_p \cap K) = \mathrm{Gal}(\bar{\mathbf{F}}_p/\bar{\mathbf{F}}_p \cap K)$.



The group $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ is pro-cyclic, and is generated by Frob_p. It has $H = \mathrm{Gal}(\bar{\mathbf{F}}_p/\bar{\mathbf{F}}_p \cap K)$ as a subgroup. Because $\bar{\mathbf{F}}_p \cap K$ is the union of its finite subfields, we have

$$H = \bigcap_{\substack{\mathbf{F}_{p^m} \subset K \\ m \in \mathbf{Z}_{\geq 1}}} \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_{p^m}).$$

Recall that we defined the Steinitz number $a \in \mathcal{S}$ by

$$\forall m \in \mathbf{Z}_{\geq 1} : \ m \mid a \Leftrightarrow \mathbf{F}_{p^m} \subset K.$$

Since $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_{p^m})$ is generated by $(\mathrm{Frob}_p)^m$, we can then conclude that H is generated by $(\mathrm{Frob}_p)^{a\hat{\mathbf{Z}}}$ and Γ by $p^{a\hat{\mathbf{Z}}}$. □