# Galois Groups of Radical Extensions

Hendrik Lenstra

## 1. Introduction

Throughout this lecture, $K$ denotes a field, with algebraic closure $\bar{K}$. The following theorem summarizes traditional Kummer theory.

**Theorem 1.1** (Kummer theory)**.** *Let $m \in \mathbb{Z}_{>0}$, and suppose that the subgroup $\mu_m(K) = \{\zeta \in K^* : \zeta^m = 1\}$ of $K^*$ has order $m$. Write $K^{*1/m}$ for the subgroup $\{x \in \bar{K}^* : x^m \in K^*\}$ of $\bar{K}^*$. Then $K(K^{*1/m})$ is the maximal abelian extension of exponent dividing $m$ of $K$ inside $\bar{K}$, and there is an isomorphism $\mathrm{Gal}(K(K^{*1/m})/K) \xrightarrow{\sim} \mathrm{Hom}(K^*, \mu_m(K))$ that sends $\sigma$ to the map sending $\alpha$ to $\sigma(\beta)/\beta$, where $\beta \in K^{*1/m}$ satisfies $\beta^m = \alpha$.*

Kummer theory includes a description of all exponent $m$ extensions of $K$. One can recover it from the theorem by studying the closed subgroups of the group $\mathrm{Hom}(K^*, \mu_m(K))$.

For $K = \mathbb{Q}$ and $m = 2$, one finds the field $\mathbb{Q}(\mathbb{Q}^{*1/2})$ obtained by adjoining the square roots of all rational numbers to $\mathbb{Q}$. From

$$\mathbb{Q}^* \cong \{\pm 1\} \times \bigoplus_{p \text{ prime}} p^{\mathbb{Z}}$$

one sees that $\mathrm{Gal}(\mathbb{Q}(\mathbb{Q}^{*1/2})/\mathbb{Q})$ is isomorphic to

$$\mathrm{Hom}(\mathbb{Q}^*, \{\pm 1\}) \cong \{\pm 1\} \times \prod_{p \text{ prime}} \{\pm 1\}.$$

In the present lecture, we shall extend Kummer theory in two directions. First, if $K$ has infinitely many roots of unity, then the theorem above applies to infinitely many values of $m$. In that case one may wonder how all the fields $K(K^{*1/m})$ and their Galois groups fit together, and whether their union can be described in one stroke. This is similar to the situation in class field theory: every finite abelian extension of a number field is contained in infinitely many ray class fields, and idelic class field theory answers the question how all these ray class fields and their Galois groups fit together. We shall formulate a version of Kummer theory that is valid for suitably defined 'infinite' values of $m$.

Secondly, we shall present a result in which the assumption that $K$ have enough roots of unity is dropped. In that case a description of the Galois group of

$K(K^{*1/m})$ over $K$ is still of great interest for several arithmetic applications. It is not necessarily abelian.

It will be convenient to reformulate the description of $\mathrm{Gal}(K(K^{*1/m})/K)$ given by Kummer theory as follows: there is an isomorphism

$$\mathrm{Gal}(K(K^{*1/m})/K) \xrightarrow{\sim} \mathrm{Aut}_{K^*}(K^{*1/m})$$

that sends each $\sigma$ to its restriction to $K^{*1/m}$; here we denote, for a group $B$ with subgroup $A$, by $\mathrm{Aut}_A B$ the group of group automorphisms of $B$ that are the identity on $A$. To justify the reformulation, we consider the exact sequence

$$1 \to \mu_m(K) \to K^{*1/m} \xrightarrow{m} K^* \to 1.$$

From $\mu_m(K) \subset K^*$ one sees that $\mathrm{Aut}_{K^*}(K^{*1/m})$ may be identified with the group of automorphisms of $K^{*1/m}$ that are the identity on $\mu_m(K)$ and induce the identity on $K^{*1/m}/\mu(K) \cong K^*$. Generally, if $1 \to A \to B \to C \to 1$ is an exact sequence of abelian groups, then the group of automorphisms of $B$ that are the identity on $A$ and induce the identity on $C$ is isomorphic to $\mathrm{Hom}(C, A)$; namely, send $\sigma$ to the homomorphism $C \to A$ mapping $\gamma$ to $\sigma(\beta)/\beta$ (viewed as an element of $A$), where $\beta \in B$ maps to $\gamma \in C$. The conclusion is that $\mathrm{Aut}_{K^*}(K^{*1/m})$ may be identified with $\mathrm{Hom}(K^*, \mu_m(K))$, as required.

One may reinterpret the isomorphism

$$\mathrm{Gal}(K(K^{*1/m})/K) \xrightarrow{\sim} \mathrm{Aut}_{K^*}(K^{*1/m})$$

by saying that the multiplicative relations between elements of $K^{*1/m}$ are the only ones one needs to care about; somehow the additive relations, which also need to be preserved by elements of the Galois group, take care of themselves.

In our extensions of Kummer theory below, we shall likewise describe Galois groups by means of groups of group automorphisms. The problem of 'computing' those automorphisms groups will hardly be touched upon. Note that the group $\mathrm{Hom}(K^*, \mu_m(K))$ is defined purely in terms of $K$ itself, without reference to $\bar{K}$; to achieve the same for $\mathrm{Aut}_{K^*}(K^{*1/m})$, it would suffice to give a purely group theoretic description of the group $K^{*1/m}$, starting from $K^*$ and $m$ alone. This can indeed be done (see Exercise 4.8).

## 2. Steinitz numbers

We now generalize to the situation where $K$ may contain infinitely many roots of unity. To say 'how many' roots of unity $K$ has, we make the following definition: a *Steinitz number* is a formal expression

$$m = \prod_{p \text{ prime}} p^{m(p)}$$

with each $m(p) \in \{0, 1, 2, \ldots, \infty\}$. Every ordinary positive integer is a Steinitz number, but Steinitz numbers generalize this in two ways: one may take infinitely many $m(p)$ different from 0, and one may take $m(p)$ equal to $\infty$ for one or more $p$.

One may interpret the 'number' of roots of unity in $K$ as a Steinitz number: for each $p$, let $p^{m(p)}$ be the number of roots of unity of $p$-power order in $K$ if that number is finite, and put $m(p) = \infty$ otherwise.

Given two Steinitz numbers, one can form their product, their greatest common divisor, and their least common multiple, and one can define when one divides the other, all in a perfectly obvious manner.

There are several alternative ways of thinking about the set of Steinitz numbers. There is a bijection $\{\text{Steinitz numbers}\} \xrightarrow{\sim} \{\text{closed subgroups of } \widehat{\mathbb{Z}}\}$ that sends $m = \prod_p p^{m(p)}$ to the subgroup of $\widehat{\mathbb{Z}}$ that under the isomorphism $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ corresponds to $\prod_p p^{m(p)}\mathbb{Z}_p$, where $p^\infty\mathbb{Z}_p = 0$; we write $m\widehat{\mathbb{Z}}$ for this subgroup. Note that $m\widehat{\mathbb{Z}} = \bigcap_{n|m,\, n<\infty} n\widehat{\mathbb{Z}}$. One has $\{\text{closed subgroups of } \widehat{\mathbb{Z}}\} = \{\text{principal ideals of } \widehat{\mathbb{Z}}\}$, and since there is a bijection $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^* \xrightarrow{\sim} \{\text{principal ideals of } \widehat{\mathbb{Z}}\}$ mapping $m\widehat{\mathbb{Z}}^*$ to $m\widehat{\mathbb{Z}}$, one concludes that the set of Steinitz numbers may be identified with the set $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^*$ of $\widehat{\mathbb{Z}}^*$-orbits of $\widehat{\mathbb{Z}}$, the action being given by multiplication. One also has a bijection $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^* \xrightarrow{\sim} \{\text{subgroups of } \mathbb{Q}/\mathbb{Z}\}$ that sends $m\widehat{\mathbb{Z}}^*$ to $\{x \in \mathbb{Q}/\mathbb{Z} : mx = 0\}$, where $\mathbb{Q}/\mathbb{Z}$ is viewed as a $\widehat{\mathbb{Z}}$-module (see Exercise 4.2); we shall write $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$ for this subgroup. Note that $\frac{1}{m}\mathbb{Z}/\mathbb{Z} = \bigcup_{n|m,\, n<\infty} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Our bijections show that the set of closed subgroups of $\widehat{\mathbb{Z}}$ is in bijective correspondence with the set of all subgroups of $\mathbb{Q}/\mathbb{Z}$. This reflects a duality between the category of profinite abelian groups with the category of torsion abelian groups, under which $\widehat{\mathbb{Z}}$ corresponds to $\mathbb{Q}/\mathbb{Z}$.

We shall, coming back to the field $K$, always restrict to Steinitz numbers that are not divisible by $\operatorname{char} K$, in case $\operatorname{char} K \neq 0$. For such a Steinitz number $m$, we define

$$\mu_m = \{\zeta \in \bar{K}^* : \text{there exists } n \mid m,\ n < \infty \text{ with } \zeta^n = 1\} = \bigcup_{n|m,\, n<\infty} \mu_n.$$

We define the 'Tate module' $\widehat{\mu}_m$ to be $\varprojlim_{n|m,\, n<\infty} \mu_n$, the restriction maps $\mu_n \to \mu_{n'}$ sending $\zeta$ to $\zeta^{n/n'}$, for $n'$ dividing $n$. Finally, we put

$$K^{*1/m} = \{x \in \bar{K}^* : \text{there exists } n \mid m,\ n < \infty \text{ with } x^n \in K^*\},$$

which is the same as $\bigcup_{n|m,\, n<\infty} K^{*1/n}$.

We are now prepared to state the main theorem of Kummer theory for Steinitz numbers.

**Theorem 2.1** (Kummer theory for Steinitz numbers)**.** *With $K$ and $m$ as above, assume that $\mu_m$ is contained in $K^*$. Then $K(K^{*1/m})$ is the maximal abelian extension with Galois group annihilated by $m$ of $K$ inside $\bar{K}$, and there are isomorphisms*

$$\operatorname{Gal}(K(K^{*1/m})/K) \cong \operatorname{Aut}_{K^*} K^{*1/m} \cong \operatorname{Hom}(K^*, \widehat{\mu}_m).$$

Every profinite abelian group is a module over $\widehat{\mathbb{Z}}$, just as every abelian group is a module over $\mathbb{Z}$. Therefore it makes sense to talk about abelian Galois groups

being annihilated by the Steinitz number $m$. Notice that $\widehat{\mu}_m = \mu_m$ when $m$ is finite, so the new theorem includes the theorem given in the introduction.

To prove the theorem, one simply takes the projective limit of the isomorphisms $\mathrm{Gal}(K(K^{*1/n})/K) \cong \mathrm{Aut}_{K^*}(K^{*1/n}) \cong \mathrm{Hom}(K^*, \mu_n(K))$, with $n$ ranging over the finite divisors $n$ of $m$. The transition maps between the Hom-groups turn out to be induced by the maps $\mu_n \to \mu_{n'}$ defined above, and this is how one arrives at $\widehat{\mu}_m$ as opposed to $\mu_m$.

## 3. Maximal radical extensions

From now on, we let $m = \prod_p p^\infty$, the product ranging over all prime numbers $p$ different from $\mathrm{char}\, K$. This is the 'largest' Steinitz number we may take. We write $\mu = \mu_m$, which is the group of all roots of unity in $\bar{K}$, and we do not assume that $\mu$ is contained in $K$. We write $\widehat{\mu} = \widehat{\mu}_m$, and $M = K^{*1/m}$; so $M$ is the group of those $x \in \bar{K}^*$ for which there exists a positive integer $n$ not divisible by $\mathrm{char}\, K$ with $x^n \in K^*$. The field $K(M)$ may be called the maximal radical extension of $K$. Its Galois group $\mathrm{Gal}(K(M)/K)$ clearly maps injectively to the group $\mathrm{Aut}_{K^*} M$, and we shall describe the image.

In the case $K = \mathbb{Q}$ one has an isomorphism $\mathbb{Q}^* \xrightarrow{\sim} (\frac{1}{2}\mathbb{Z}/\mathbb{Z}) \oplus \bigoplus_p \mathbb{Z}$ of abelian groups, which can be extended to an isomorphism $M \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z}) \oplus \bigoplus_p \mathbb{Q}$. One may check that $\mathrm{Aut}_{\mathbb{Q}^*} M$ is isomorphic to the semidirect product $(\prod_p \widehat{\mathbb{Z}}) \rtimes \widehat{\mathbb{Z}}^*$, where $\widehat{\mathbb{Z}}^*$ acts by componentwise multiplication on $\prod_p \widehat{\mathbb{Z}}$.

For general $K$, we break up the extension $K \subset K(M)$ as $K \subset K(\mu) \subset K(M)$, where the first extension is cyclotomic, and the second extension is a Kummer extension with base field $K(\mu)$.

For the cyclotomic piece, we have a natural injection $\mathrm{Gal}(K(\mu)/K) \rightarrowtail \mathrm{Aut}\, \mu$, where

$$\mathrm{Aut}\, \mu \cong (\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^* \cong \begin{cases} \widehat{\mathbb{Z}}^*, & \mathrm{char}\, K = 0 \\ \prod_{p \neq \mathrm{char}\, K} \mathbb{Z}_p^*, & \text{in general.} \end{cases}$$

Let $H \subset \mathrm{Aut}\, \mu$ be the image of $\mathrm{Gal}(K(\mu)/K)$, so that $\mathrm{Gal}(K(\mu)/K) \cong H$. In the case $\mathrm{char}\, K = 0$, there is little one can say about $H$ beyond the fact that it is a closed subgroup of $\mathrm{Aut}\, \mu$ (see Exercise 4.10(a)); however, in the case of non-zero characteristic, the possibilities for $H$ are severely restricted (see Exercise 4.10(b)). We shall just take knowledge of $H$ for granted.

Clearly, the image of $\mathrm{Gal}(K(M)/K)$ in $\mathrm{Aut}_{K^*} M$ is contained in the subgroup

$$\mathrm{Aut}_{K^*,H} M = \{\sigma \in \mathrm{Aut}_{K^*} M : \text{the restriction of } \sigma \text{ to } \mu \text{ belongs to } H\}.$$

In general, the injection

$$\mathrm{Gal}(K(M)/K) \rightarrowtail \mathrm{Aut}_{K^*,H} M$$

is not an isomorphism; indeed, in the case $\mathrm{char}\, K = 0$ it is *never* an isomorphism, unless $\mu \subset K^*$ (see Exercise 4.14). This is caused by additive relations that may

exist between radicals and roots of unity. For example, over $\mathbb{Q}$ we have $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$. It turns out that, for general $K$, the only such additive relations that one needs to worry about involve radicals that are obtained from Kummer theory; thus, for $K = \mathbb{Q}$, only the square roots create difficulties.

To make the above remarks precise, define $w$ to be the unique Steinitz number (not divisible by $\operatorname{char} K$) with $\mu_w = \mu \cap K^*$. For example, for $K = \mathbb{Q}$ one has $w = 2$. Let $L$ be the maximal extension of $K$ inside $K(\mu)$ for which $w$ annihilates $\operatorname{Gal}(L/K)$. We have $\operatorname{Gal}(L/K) \cong H/H^w$. The field $L$ is the maximal subextension of $K(\mu)$ that may be described by Kummer theory over $K$; that is, we have $L = K(K^{*1/w}) \cap K(\mu)$. In the case $K = \mathbb{Q}$ one has $L = \mathbb{Q}(\mathbb{Q}^{*1/2})$.

We can now define two surjective group homomorphisms from $\operatorname{Aut}_{K^*,H} M$ to $\operatorname{Gal}(L/K)$. To obtain the first, restrict automorphisms of $M$ to $\mu$ to get a map $\operatorname{Aut}_{K^*,H} M \to H$, and compose it with the natural map $H \twoheadrightarrow H/H^w \cong \operatorname{Gal}(L/K)$. To obtain the second, restrict automorphisms of $M$ to the subgroup $K^{*1/w}$ of $M$ to get a map $\operatorname{Aut}_{K^*,H} M \to \operatorname{Aut}_K^*(K^{*1/w})$, and compose it with the natural map $\operatorname{Aut}_K^*(K^{*1/w}) \xrightarrow{\sim} \operatorname{Gal}(K(K^{*1/w})/K) \twoheadrightarrow \operatorname{Gal}(L/K)$.

**Theorem 3.1.** *Let $K$ be a field, and let $M$, $H$, $L$, and $\operatorname{Aut}_{K^*,H} M$ be as defined above. Then the natural map $\operatorname{Gal}(K(M)/K) \to \operatorname{Aut}_{K^*,H} M$ induces an isomorphism between $\operatorname{Gal}(K(M)/K)$ and the subgroup of $\operatorname{Aut}_{K^*,H} M$ consisting of those elements that have the same image under the two maps $\operatorname{Aut}_{K^*,H} M \to \operatorname{Gal}(L/K)$ just defined.*

The proof of this result depends on a theorem of Schinzel that one finds in Exercise 4.11.

In the case $K = \mathbb{Q}$, one deduces that $\operatorname{Gal}(\mathbb{Q}(M)/\mathbb{Q})$ is isomorphic to the subgroup of $(\prod_p \widehat{\mathbb{Z}}) \rtimes \widehat{\mathbb{Z}}^*$ consisting of those elements $((a_p)_p, u)$ (with $a_p \in \widehat{\mathbb{Z}}$, $u \in \widehat{\mathbb{Z}}^*$) that satisfy the following conditions: the quadratic symbol $\left(\frac{2}{u}\right)$ (which depends only on $u \bmod 8$) equals $(-1)^{a_2}$, and for each odd prime number $p$ the quadratic symbol $\left(\frac{u}{p}\right)$ (which depends only on $u \bmod p$) equals $(-1)^{(u-1)(p-1)/4} \cdot (-1)^{a_p}$.

The theorem implies that there is an exact sequence

$$1 \to \operatorname{Gal}(K(M)/K) \to \operatorname{Aut}_{K^*,H} M \to H/H^w \to 1$$

of profinite groups. Since $w$ can be read off from $H$ (see Exercise 4.12), it follows that the extent to which $\operatorname{Gal}(K(M)/K)$ differs from $\operatorname{Aut}_{K^*} M$ is in fact completely determined by $H$ as a subgroup of $\operatorname{Aut} \mu$. There is also a sense in which the field $L$ appearing above depends only on $H$. For example, suppose that $H = \operatorname{Aut} \mu$. Then one has $\operatorname{char} K = 0$ and, just as in the case $K = \mathbb{Q}$, one obtains the field $L$ by adjoining $\mathbb{Q}^{*1/2}$ to $K$, and in fact one has $L \cong \mathbb{Q}(\mathbb{Q}^{*1/2}) \otimes_{\mathbb{Q}} K$.

## Exercises

**Exercise 4.1**. Let

$$0 \to A \xrightarrow{i} B \xrightarrow{h} C \to 0$$

be a short exact sequence of abelian groups. Prove that there is a group isomorphism $\mathrm{Hom}(C, A) \xrightarrow{\sim} \{\sigma \in \mathrm{Aut}\, B : \sigma i = i,\ h\sigma = h\}$ that sends $f \in \mathrm{Hom}(C, A)$ to the map $B \to B$ mapping $b \in B$ to $b + ifh(b)$.

**Exercise 4.2**.

(a) Let $A$ be an additively written abelian group all of whose elements have finite order (a *torsion* abelian group). Prove that $A$ has a unique $\widehat{\mathbb{Z}}$-module structure, and that it is given by $a \cdot x = a_m x$ for $a = (a_n)_{n=1}^{\infty} \in \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$ and $x \in A$; here $m$ is such that $mx = 0$.

(b) Show that each profinite abelian group $A$ has a unique $\widehat{\mathbb{Z}}$-module structure with the property that the map $\widehat{\mathbb{Z}} \times A \to A$ giving the scalar multiplication is continuous.

**Exercise 4.3**. Prove the following statements.

(a) There is a bijection $\{\text{Steinitz numbers}\} \to \{\text{closed subgroups of } \widehat{\mathbb{Z}}\}$ sending $m$ to $m\widehat{\mathbb{Z}} = \bigcap_{n|m,\, n<\infty} n\widehat{\mathbb{Z}}$.

(b) $\{\text{closed subgroups of } \widehat{\mathbb{Z}}\} = \{\text{principal ideals of } \widehat{\mathbb{Z}}\}$.

(c) Let $\widehat{\mathbb{Z}}^*$ act by multiplication on $\widehat{\mathbb{Z}}$, and denote by $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^*$ the set of orbits. Then there is a bijection $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^* \to \{\text{principal ideals of } \widehat{\mathbb{Z}}\}$ sending $m\widehat{\mathbb{Z}}^*$ to $m\widehat{\mathbb{Z}}$.

(d) There is a bijection $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^* \to \{\text{subgroups of } \mathbb{Q}/\mathbb{Z}\}$ sending $m\widehat{\mathbb{Z}}^*$ to $\{x \in \mathbb{Q}/\mathbb{Z} : mx = 0\}$.

**Exercise 4.4**. Let $\widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^*$ be given the quotient topology from $\widehat{\mathbb{Z}}$. Define a metric on the set $\mathcal{S}$ of Steinitz numbers such that the bijection $\mathcal{S} \cong \widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}^*$ obtained from Exercise 4.3 becomes a homeomorphism.

**Exercise 4.5**. Let $G$ be a profinite group, let $\sigma$ be an element of $G$, and let $\overline{\langle\sigma\rangle}$ be the closure of the subgroup of $G$ generated by $\sigma$. Prove that there is a unique Steinitz number $m$ such that $\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}} \cong \overline{\langle\sigma\rangle}$. (This Steinitz number is called the *order* of $\sigma$.)

In the following exercises, $K$ will be a field, with algebraic closure $\overline{K}$. By $m$ we always denote a Steinitz number such that $m$ is not divisible by $\mathrm{char}\, K$ if $\mathrm{char}\, K \neq 0$. We write $K^{*1/m} = \{x \in \overline{K}^* : \text{there exists } n|m,\ n < \infty, \text{ with } x^n \in K^*\}$; this is a subgroup of $\overline{K}^*$. Also, we put $\mu_m = \{x \in \overline{K}^* : \text{there exists } n|m,\ n < \infty, \text{ with } x^n = 1\}$, and $\widehat{\mu}_m = \varprojlim \mu_n$, the limit ranging over the set of all $n|m$ with $n < \infty$, and the transition map $\mu_{n'} \to \mu_n$, for $n|n'$, sending $x$ to $x^{n'/n}$.

**Exercise 4.6**.

(a) Write $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$ for the subgroup of $\mathbb{Q}/\mathbb{Z}$ corresponding to $m$ (see Exercise 4.3(d)). Prove: $\mu_m \cong \frac{1}{m}\mathbb{Z}/\mathbb{Z}$ as groups, and $\widehat{\mu}_m \cong \widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}}$ as topological groups.
(b) Exhibit group isomorphisms $\widehat{\mu}_m \xrightarrow{\sim} \mathrm{Hom}(\frac{1}{m}\mathbb{Z}/\mathbb{Z}, \mu_m)$ and $\mathrm{Aut}\,\mu_m \xrightarrow{\sim} (\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^*$.

**Exercise 4.7**. Let $m$ be the Steinitz number $\prod_{p \text{ prime}} p^\infty$. Show that there exists a group isomorphism $\mathbb{Q}^{*1/m} \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z}) \oplus \bigoplus_{p \text{ prime}} \mathbb{Q}$ that restricts to an isomorphism $\mathbb{Q}^* \xrightarrow{\sim} (\frac{1}{2}\mathbb{Z}/\mathbb{Z}) \oplus \bigoplus_{p \text{ prime}} \mathbb{Z}$.

**Exercise 4.8**. Let $A$ be a multiplicatively written abelian group such that every finite subgroup of $A$ is cyclic. By an *$m$-th root* of $A$ we mean an abelian group $B$ that contains $A$ as a subgroup, such that (i) for every $b \in B$ there exists $n|m$, $n < \infty$, with $b^n \in A$, and (ii) for every $a \in A$ and every $n|m$ with $n < \infty$, the set $\{b \in B : b^n = a\}$ has cardinality $n$.

(a) Prove: an $m$-th root of $A$ exists, and it is unique up to an isomorphism that is the identity on $A$.
(b) Prove: $K^{*1/m}$ is an $m$-th root of $K^*$.

**Exercise 4.9**. (Kummer theory for Steinitz numbers.) Assume $\mu_m \subset K$. Prove that the natural map $\mathrm{Gal}(K(K^{*1/m})/K) \to \mathrm{Aut}_{K^*}(K^{*1/m})$ is an isomorphism, and exhibit an isomorphism $\mathrm{Aut}_{K^*}(K^{*1/m}) \xrightarrow{\sim} \mathrm{Hom}(K^*, \widehat{\mu}_m)$.

**Exercise 4.10**. Let $H$ be a closed subgroup of $(\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^*$.

(a) Prove: there is a field $K$ with $\mathrm{char}\, K = 0$ such that $H$ equals the image of the natural map $\mathrm{Gal}(K(\mu_m)/K) \to \mathrm{Aut}\,\mu_m \cong (\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^*$.
(b) Let $\ell$ be a prime number not dividing $m$. Prove that the following two statements are equivalent: (i) there is a field $K$ with $\mathrm{char}\, K = \ell$ such that $H$ equals the image of the natural map $\mathrm{Gal}(K(\mu_m)/K) \to \mathrm{Aut}\,\mu_m \cong (\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^*$; and (ii) $H$ is contained in the closure of the subgroup of $(\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^*$ generated by $(\ell \bmod m\widehat{\mathbb{Z}})$.

**Exercise 4.11**. Let $K$ be a field and let $n$ be a positive integer not divisible by the characteristic of $K$. Denote the number of $n$-th roots of unity in $K$ by $w$, and fix an element $a$ of $K^*$. The goal of this exercise is to prove the following theorem of Schinzel: *the splitting field $L$ of $X^n - a$ over $K$ is abelian over $K$ if and only if $a^w = b^n$ for some $b \in K$.*

(a) Prove the "if" part by showing that $K(\mu_{nw}, b^{1/w})$ is abelian over $K$.
(b) Let $\sigma \in \mathrm{Gal}(L/K)$, and let $k = k_\sigma \in \mathbb{Z}$ be such that $\sigma$ raises every $n$-th root of unity to the power $k$. For $\alpha \in L$ with $\alpha^n = a$, show that $\alpha^k/\sigma(\alpha)$ is Galois-invariant so that it lies in $K$. Deduce that $a^{k-1}$ is an $n$-th power in $K$.
(c) Let $g$ be the the greatest common divisor of the number $n$ and the numbers $k_\sigma - 1$ as $\sigma$ runs over $\mathrm{Gal}(L/K)$. Show that $a^g$ is an $n$-th power in $K$.

(d) Show that $g = w$, and deduce Schinzel's theorem.

In Exercises 4.12–4.14, we use the following additional notation. By $\mu$ we denote the group of all roots of unity in $\overline{K}^*$, and by $w$ the unique Steinitz number (not divisible by $\operatorname{char} K$ if $\operatorname{char} K \neq 0$) with $\mu_w = \mu \cap K^*$. By $H$ we denote the image of the natural map $\operatorname{Gal}(K(\mu)/K) \to \operatorname{Aut} \mu$. Further, we write $M = \{x \in \overline{K}^* :$ there is a positive integer $n$ not divisible by $\operatorname{char} K$ such that $x^n \in K^*\}$, and $\operatorname{Aut}_{K^*,H} M$ for the group of all $\sigma \in \operatorname{Aut} M$ that are the identity on $K^*$ and whose restriction to $\mu$ belongs to $H$.

**Exercise 4.12**.

(a) Suppose $\operatorname{char} K = 0$, and let $\varphi\colon \operatorname{Aut} \mu \to \widehat{\mathbb{Z}}^*$ be the natural isomorphism. Prove that $w\widehat{\mathbb{Z}}$ is the closure of the $\widehat{\mathbb{Z}}$-ideal generated by $\{\varphi(h)-1 : h \in H\}$.

(b) Verify the result of (a) numerically for $K = \mathbb{Q}$.

(c) Formulate and prove a result similar to (a) in the case $\operatorname{char} K \neq 0$.

**Exercise 4.13**. Prove that there is a short exact sequence of profinite groups

$$1 \to \operatorname{Gal}(K(M)/K) \to \operatorname{Aut}_{K^*,H} M \to H/H^w \to 1.$$

**Exercise 4.14**. Suppose $\operatorname{char} K = 0$. Prove that the following statements are equivalent:

(i) the natural map $\operatorname{Gal}(K(M)/K) \to \operatorname{Aut}_{K^*,H} M$ is an isomorphism;

(ii) $H/H^w = 1$;

(iii) $H = 1$;

(iv) $\mu \subset K$.

**Exercise 4.15**. For a prime number $p$, let $R_p = \{x \in \overline{\mathbb{Q}} : x^{2^n} = p$ for some non-negative integer $n\}$. Prove: if $p$ is odd, then $\operatorname{Gal}(\mathbb{Q}(R_p)/\mathbb{Q}) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2^*$, with $\mathbb{Z}_2^*$ acting on $\mathbb{Z}_2$ by multiplication. What can you say about the case $p = 2$?

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
*E-mail address*: hwl@math.leidenuniv.nl