Radical extensions and Galois groups

een wetenschappelijke proeve op het gebied van
de Natuurwetenschappen, Wiskunde en Informatica

Proefschrift

ter verkrijging van de graad van doctor
aan de Radboud Universiteit Nijmegen
op gezag van de Rector Magnificus prof. dr. C.W.P.M. Blom,
volgens besluit van het College van Decanen
in het openbaar te verdedigen op
dinsdag 17 mei 2005
des namiddags om 3.30 uur precies

door
Mascha Honsbeek

geboren op 25 oktober 1971
te Haarlem

Promotor:	prof. dr. F.J. Keune
Copromotores:	dr. W. Bosma
	dr. B. de Smit (*Universiteit Leiden*)
Manuscriptcommissie:	prof. dr. F. Beukers (*Universiteit Utrecht*)
	prof. dr. A.M. Cohen (*Technische Universiteit Eindhoven*)
	prof. dr. H.W. Lenstra (*Universiteit Leiden*)

Dankwoord

Zoals iedereen aan mijn CV kan zien, is het schrijven van dit proefschrift niet helemaal volgens schema gegaan. De eerste drie jaar wilde het niet echt lukken om resultaten te krijgen. Toch heb ik in die tijd heel fijn samengewerkt met Frans Keune en Wieb Bosma. Al klopte ik drie keer per dag aan de deur, steeds maakten ze de tijd voor mij. Frans en Wieb, dank je voor jullie vriendschap en begeleiding.

Op het moment dat ik dacht dat ik het schrijven van een proefschrift misschien maar op moest geven, kwam ik in contact met Bart de Smit. Hij keek net een beetje anders tegen de wiskunde waarmee ik bezig was aan en hielp me daarmee weer op weg. Samen met Hendrik Lenstra kwam hij met het voorstel voor het onderzoek dat ik heb uitgewerkt in het eerste hoofdstuk, de kern van dit proefschrift. Daarnaast heeft Bart mij ook vanaf dat moment als copromotor begeleid. Bart, Hendrik, dank je wel voor jullie steun en goede ideeën.

In 1999 kwam ik ook in contact met Alice Gee. Samen schreven we het artikel dat als hoofdstuk 5 opgenomen is in dit proefschrift. Alice, dank je voor het nemen van dit initiatief en de goede samenwerking.

Daarnaast wil ik ook graag mijn leescommissie bedanken. Hendrik, Arjeh en Frits, dank je wel voor jullie inzet en goede suggesties.

Ook vanuit mijn vrienden en ouders heb ik veel steun ontvangen. Voorzichtig informeerden ze soms of het eind al in zicht was. Speciaal wil ik Arnoud, Kirsten en Timo noemen. Pap, mam en al die anderen die er met mij in zijn blijven geloven, dank je wel.

Verder ontwierp Jan een schitterende kaft voor dit proefschrift. Helaas kreeg ik geen toestemming om deze Nijntje-afbeelding te gebruiken.

Tot slot, Richard, wil ik jou bedanken voor alle steun en hulp. Zonder jou had het proefschrift er niet zo mooi uitgezien.

Mascha

Contents

Introduction

The use of symbolic computing is one of the characteristics of a computer algebra package. For example, the number $\sqrt{2}$ is represented as a symbol with the property that its square is 2. This enables us to do exact calculations. Compared to numerical calculations, there also are some drawbacks concerning computations with radical expressions. For example, algebraically, one will not be able to distinguish between the positive and the negative square root of 2. If one wants to do a computation for one specific choice of these roots sometimes a numerical estimate is necessary. Moreover, we often get complicated expressions although there is a simpler expression for the number that we are interested in. The simplification of radical expressions was an important motivation for the research in this thesis.

Look at

$$\alpha = \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2},$$

where, as in the rest of this introduction, when we take a root of a positive real number, we mean the real positive root of this number. A numerical estimate of α is given by

$$\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2} = 1.618033988\ldots - 0.618033988\ldots.$$

We see that α is approximately equal to 1. Using symbolic computations we prove that α actually equals 1. One can check that α is a root of the polynomial $x^3 + 3x - 4 = (x-1)(x^2+x+4)$, which has only a single real root. Therefore α has to equal 1. Intuitively the notation 1 is simpler than $\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$. To make this precise we introduce the notion of radicals and nesting depth.

Let K be a field of characteristic 0 and let $\bar{K}$ be some fixed algebraic closure of K. We say that $\alpha \in \bar{K}$ is a *radical* over K if there exists some $n \in \mathbb{Z}_{>0}$ with $\alpha^n \in K$. We denote by $K^{(0)}$ the field K itself and inductively define the fields $K^{(k)}$ for $k \geq 1$ as

$$K^{(k)} = K^{(k-1)}(\{\alpha \in \bar{K} \text{ with } \alpha^n \in K^{(k-1)} \text{ for some } n \in \mathbb{Z}_{>0}\}).$$

We say that $\alpha \in \bar{K}$ is a *nested radical over* K if there exists some $k \in \mathbb{Z}_{>0}$ with $\alpha \in K^{(k)}$. We say that α has *nesting depth* k *over* K if $\alpha \in K^{(k)} \setminus K^{(k-1)}$.

It is desirable for the computer to produce the simplest possible expression for the outcome of a computation with nested radicals. Richard Zippel [40] gave the following identity

$$\sqrt[6]{7\sqrt[3]{20}-19} = \sqrt[3]{5/3} - \sqrt[3]{2/3}. \tag{1}$$

Following [5], [20], [21], [28], [40] we say that the right hand side of this equation is a denesting of the left hand side; the equality shows that some element that is clearly contained in $K^{(2)}$ is even contained in $K^{(1)}$.

The element $\alpha \in \bar{K}$ is a nested radical if and only if there exists a Galois extension L/K with $\alpha \in L$ and a chain of field extensions

$$K = K_0 \subset K_1 \subset \ldots \subset K_t = L,$$

such that for $1 \leq i \leq t$ the field K_i is generated by radicals over K_{i-1}. For example, if we take the nested radical $\alpha = \sqrt[6]{7\sqrt[3]{20}-19}$ from equality (1) over $\mathbb{Q}$, then an obvious choice for the first fields in this chain would be

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{20}\right) \subset \mathbb{Q}\left(\sqrt[3]{20}, \sqrt[6]{7\sqrt[3]{20}-19}\right) = \mathbb{Q}\left(\sqrt[6]{7\sqrt[3]{20}-19}\right).$$

In general we have to adjoin all conjugates of α to obtain a Galois extension. In this case however, it turns out that $\mathbb{Q}\left(\sqrt[6]{7\sqrt[3]{20}-19}, \zeta_6\right)$ is Galois over $\mathbb{Q}$. One can check this using a computer algebra package or by using equality (2) below.

If we adjoin sufficiently many roots of unity in the first step of the chain, then we see that K_i/K_{i-1} is abelian for all $i \geq 1$. In our example:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_6) \subset \mathbb{Q}\left(\sqrt[3]{20}, \zeta_6\right) \subset \mathbb{Q}\left(\sqrt[6]{7\sqrt[3]{20}-19}, \zeta_6\right).$$

As K is a field of characteristic 0, an element α is a nested radical if and only if the Galois group of the normal closure of $K(\alpha)$ over K is solvable ([22] Chapter VI). Given a chain of field extensions $K = K_0 \subset K_1 \subset \ldots \subset K_s$, for which K_i/K_{i-1}, for $i \in \mathbb{Z}_{>0}$, is generated by a radical, and an element $\alpha \in K_s$ of nesting depth $t \leq s$ Susan Landau [20] provides an algorithm that computes a symbolic representation for α in $K^{(d)}$, where d is the length of the derived series of the Galois closure of K_s/K. We have $t \leq d \leq t+1$.

Carl Cotner [7] improved this result. He showed that the nesting depth of α is computable and gave an algorithm to find a symbolic representation of minimal nesting depth.

For specific types of nested radicals it is possible to give a simple algorithm to compute a symbolic representation of minimal depth. This we will do in chapters 3 and 4 for certain elements of $K^{(2)}$. Given a subfield L of $K^{(1)}$, an element δ of L, and some $n \in \mathbb{Z}_{\geq 2}$ we will prove that $\sqrt[n]{\delta} \in K^{(1)}$ implies that δ satisfies a strong condition

which may be phrased as 'δ is almost an n-th power in L'. Indeed, equality (1) holds because '$7\sqrt[3]{20}-19$ is almost a sixth power in $\mathbb{Q}(\sqrt[3]{20})$'; we have

$$7\sqrt[3]{20}-19=\frac{1}{144}\left(\sqrt[3]{20}-2\right)^6 \tag{2}$$

and

$$\sqrt[6]{\frac{1}{144}}\left(\sqrt[3]{20}-2\right)=\sqrt[3]{1/12}\left(\sqrt[3]{20}-\sqrt[3]{8}\right)=\sqrt[3]{5/3}-\sqrt[3]{2/3}.$$

To prove our claim in general we use Galois groups of radical extensions. If the ground field K contains the appropriate roots of unity and the extension is finite then we have a Kummer extension and the Galois group is well known. We discuss Kummer theory in chapter 1. Moreover, we discuss non-finite Kummer extensions and describe the Galois group for certain radical extensions for which the ground field K does not contain the appropriate roots of unity. We show that the Galois group of

$$L=K(\{\alpha\in\bar{K}^* \text{ with } \alpha^n\in K \text{ for some } n\in\mathbb{Z}_{>0}\})$$

over K can be embedded in a semidirect product of two explicitly described groups. An important reason to study Galois groups of radical extensions is to gain insight in the structure of subfields of the extension.

Let L/K be a Kummer extension generated by radicals $\alpha_1,\alpha_2,\ldots$ over K. By Kummer theory all subfields of $L=K(\alpha_1,\alpha_2,\ldots)/K$ are generated by a subgroup of $W=\langle K^*,\alpha_1,\alpha_2,\ldots\rangle$. This also holds for pure radical extensions. (A field extension L/K is pure if every primitive p-th root of unity contained in L is in fact contained in K, for prime numbers p and for p equal to 4.) However, this is not true in general. For example, the Galois extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ has two non-trivial subfields, $\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ and $\mathbb{Q}(\sqrt{-7})$, which are not generated by a power of ζ_7.

In chapter 2 we study the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ for some radical $\alpha\in\mathbb{C}$ and give a both necessary and sufficient condition for the subfields of $\mathbb{Q}(\alpha)$ to be generated by a subgroup of $\langle\mathbb{Q}^*,\alpha\rangle$. This gives us also some non-pure extensions for which all subfields are generated by a subgroup of $\langle\mathbb{Q}^*,\alpha\rangle$, like $\mathbb{Q}(\alpha)/\mathbb{Q}$ where α is a complex number with $\alpha^4=-3$.

Above we considered the simplification of nested radicals. Another problem concerning nested radicals is finding a representation of some element as a radical expression. The element can, for example, be given as the root of a solvable polynomial or can be given by an analytic expression. For singular values of the Rogers-Ramanujan continued fraction we determine radical expressions in chapter 5.

Below we give a more detailed description of this thesis in an overview per chapter.

Chapter 1

For ease of exposition we consider a perfect field K in this introduction. In chapter 1 we will have a slightly weaker condition on K. Let $\bar{K}$ be a fixed algebraic closure

of K. We define the group of radicals over K as

$$A = \{\alpha \in \bar{K}^* : \alpha^n \in K \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

In chapter 1 we describe the Galois group of the extension $K(A)/K$. In the case $K = \mathbb{Q}$ and $\bar{K} \subset \mathbb{C}$, the group A is the direct product of $\mu(\mathbb{C})$, the group of roots of unity in $\mathbb{C}$, and the group R of real positive radicals in A. The group $\mathrm{Aut}_{\mathbb{Q}^*}(A)$ of group automorphisms of A that are the identity on $\mathbb{Q}^*$ is isomorphic to $\mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu}) \rtimes \mathrm{Aut}(\mu(\mathbb{C}))$, where $\hat{\mu}$ denotes $\varprojlim_n \mu_n(\mathbb{C})$, the inverse limit of the groups of n-th roots of unity in $\mathbb{C}$ for all $n \in \mathbb{Z}_{>0}$, with respect to the maps $\mu_n(\mathbb{C}) \longrightarrow \mu_m(\mathbb{C}) \colon \zeta \mapsto \zeta^{n/m}$, for all $m \mid n \in \mathbb{Z}_{>0}$. The map

$$\mathrm{Aut}_{\mathbb{Q}^*}(A) \longrightarrow \Gamma = \mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu}) \rtimes \mathrm{Aut}(\mu(\mathbb{C}))$$

is given by

$$\sigma \mapsto \left(a \mapsto \left(\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\right)_{n \in \mathbb{Z}_{>0}}, \sigma_{|_{\mu(\mathbb{C})}}\right),$$

where $\sqrt[n]{a}$ denotes the positive real root of a. The Galois group $\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q})$ can be embedded in this group Γ. We know that $\sqrt{x} \in \mathbb{Q}(\mu(\mathbb{C})) \cap \mathbb{Q}(R)$ for all $x \in \mathbb{Q}_{>0}$. This gives a condition that turns out to determine the image of $\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q})$ completely. Any homomorphism f from $\mathbb{Q}_{>0}$ to $\hat{\mu}$ induces a map $\tilde{f}$ from $\mathbb{Q}_{>0}$ to $\langle -1 \rangle$ by composition with the projection map $\hat{\mu} \longrightarrow \langle -1 \rangle$. In section 1.7 we find

$$\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q}) \simeq \left\{(f, z) \in \Gamma \text{ with } \tilde{f}(a) = \left(\frac{a}{z}\right) \text{ for all } a \in \mathbb{Q}_{>0}\right\},$$

where $\left(\frac{a}{z}\right)$ denotes a generalised Jacobi symbol.

In chapter 1, we also give such a description for $\mathrm{Gal}(K(A)/K)$, where K is a perfect field and

$$A = \langle \alpha \in \bar{K}^* : \alpha^n \in K \text{ for some } n \in I \rangle,$$

with $I \neq \emptyset$ an arbitrary subset of $\mathbb{Z}_{>0}$. In general we cannot give a splitting of A, but we can give a splitting of $A/\mu(K)$. We fix a choice for this splitting and follow the lines of the proof sketched above to give a similar description of $\mathrm{Gal}(L/K)$.

Chapter 2

In chapter 2 we determine all radicals $\alpha \in \mathbb{C}$ for which the subfields of $\mathbb{Q}(\alpha)$ are all generated over $\mathbb{Q}$ by a power of α.

For instance, if we take for α a primitive fifth root of unity, ζ_5, then there exist a subfield $\mathbb{Q}(\sqrt{5})$ of $\mathbb{Q}(\alpha)$ that is not generated by a power of α. If we take $\alpha = \zeta_5 \cdot \sqrt{5}$, then all subfields of $\mathbb{Q}(\alpha)/\mathbb{Q}$ are generated by a power of α.

To find the subfields of $\mathbb{Q}(\alpha)$ we study the Galois group of $\mathbb{Q}(\zeta_n, \alpha)$ over $\mathbb{Q}$, where n is the least positive integer with $\alpha^n \in \mathbb{Q}$. The group $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q})$ can be embedded in $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$ and its image G is determined by the intersection

field $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$. For every radical $\alpha \in \mathbb{C}$ this field is of the form $\mathbb{Q}(\alpha^d)$ for some divisor d of n. The number of n-th roots of unity in this intersection field, $\#\mu_n\big(\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)\big)$, splits the problem in different cases. We identify some radicals for which evidently subfields exist that are not generated by a power of α. It turns out that there are no other radicals for which such subfields exist. This gives us the following necessary condition on α for all subfields of $\mathbb{Q}(\alpha)$ to be generated by a power of α:

(i) $\#\mu_n\big(\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)\big) \leq 2$ and we have $6 \nmid n$ or $\sqrt{-3} \notin \langle \mathbb{Q}^*, \alpha \rangle$ *or*

(ii) $\#\mu_n\big(\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)\big) = 3$ *or*

(iii) $\#\mu_n\big(\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)\big) = 4$ and $1 + i \in \langle \mathbb{Q}^*, \alpha \rangle$ *or*

(iv) $\#\mu_n\big(\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)\big) = 6$ and $\sqrt{-3} \in \langle \mathbb{Q}^*, \alpha \rangle$ *or*

(v) $\#\mu_n\big(\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)\big) = 10$ and both $4 \nmid n$ and $\sqrt{5} \in \langle \mathbb{Q}^*, \alpha \rangle$.

If $H \subset G$ is such that $\mathbb{Q}(\zeta_n, \alpha)^H = \mathbb{Q}(\alpha)$, then there is a one-to-one correspondence between subgroups of G containing H and subfields of $\mathbb{Q}(\alpha)$. We prove in each of the five cases above that all subgroups of G containing H are of the form $G \cap \big(d\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*\big)$ for some divisor d of n. These groups correspond to the fields $\mathbb{Q}(\alpha^{n/d})$, which showes that the above condition is also sufficient.

Chapter 3

At the beginning of the 20th century Ramanujan ([1]) gave the following denesting formula:

$$\sqrt{m\sqrt[3]{4(m-2n)} + n\sqrt[3]{4m+n}} = \pm\tfrac{1}{3}\left(\sqrt[3]{(4m+n)^2} + \sqrt[3]{4(m-2n)(4m+n)} - \sqrt[3]{2(m-2n)^2}\right).$$

Let α and β be integers and define $\gamma = \sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$. In chapter 3 we prove, using the normal closure of $\mathbb{Q}(\gamma)/\mathbb{Q}$, that γ can be denested if and only if $\sqrt[3]{\alpha} + \sqrt[3]{\beta}$ equals $\sqrt[3]{\alpha}^k \cdot \sqrt[3]{\beta}^l \cdot f \cdot e^2$ for some $f \in \mathbb{Q}$, $k, l \in \mathbb{Z}_{>0}$ and e in $\mathbb{Q}(\sqrt[3]{\alpha}, \sqrt[3]{\beta})$. We use this to show that γ can only be denested if there exist integers m and n with

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3} \tag{3}$$

or if β/α is a cube in $\mathbb{Q}$.

For example, if we take $m = n = 1$, then the quotient above equals $-\frac{5}{4}$. Hence we have the denesting

$$\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = \tfrac{1}{3}(\sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25}).$$

It can be shown that there do not exist integers m, n satisfying equation (3) if, for instance, we take $\alpha = 2$ and $\beta = 3$. Hence $\sqrt{\sqrt[3]{2} + \sqrt[3]{3}}$ cannot be denested.

Chapter 4

Let K be a field, let $\alpha_1, \ldots, \alpha_t$ be radicals over K and define $L = K(\alpha_1, \ldots, \alpha_t)$. In this chapter we give a necessary condition for a nested radical of the form $\sqrt[n]{\delta}$ with $n \in \mathbb{Z}_{>0}$ and $\delta \in L \setminus K$ to be contained in $K^{(1)}$.

We define the field $K_\infty \subset \bar{K}$ as the smallest extension over K containing all roots of unity in $\bar{K}$. At the beginning of this introduction we described the Kummer correspondence between subfields and subgroups of the multiplicative group of generating radicals. We use this correspondence to show that $\sqrt[n]{\delta} \in K^{(1)}$ implies that there exist $w \in K_\infty \cap L$, $e \in L$ and integers $s_1, \ldots, s_t$ with $\delta = w \cdot e^n \cdot \prod_i \alpha_i^{s_i}$.

If both the field L and the finite subextension of $K^{(1)}$ containing $\sqrt[n]{\delta}$ are pure then we even have $w \in K$. In general w is not contained in K. We provide an example where w is contained in $(K_\infty \cap L) \setminus K$.

Chapter 5

This chapter consists of an article co-authored with Alice Gee. It was accepted by the Ramanujan Journal in May 2001 and can also be found in [10]. We determine nested radicals for singular values of the Rogers-Ramanujan continued fraction

$$R(z) = q^{\frac{1}{5}} \prod_{n=1}^{\infty} \left(1 - q^n\right)^{\left(\frac{n}{5}\right)},$$

where z is an element of the complex upper half plane, q is $e^{2\pi i z}$ and $\left(\frac{n}{5}\right)$ denotes the Legendre symbol.

First we prove that $R(z)$ is a modular function of level 5. In fact, the field F_5 of functions of level 5 over $\mathbb{Q}(\zeta_5)$ equals $\mathbb{Q}(R, \zeta_5)$. Let τ be an element of the upper half plane with $[1, \tau]$ a $\mathbb{Z}$-basis of some imaginary quadratic order. We denote by H_5 the field of function values in τ of elements of F_5. The first main theorem of complex multiplication states that H_5 is abelian over $\mathbb{Q}(\tau)$. Therefore, all elements of H_5, and especially $R(\tau)$, are nested radicals over $\mathbb{Q}(\tau)$ and consequently over $\mathbb{Q}$ since $[\mathbb{Q}(\tau) : \mathbb{Q}]$ equals 2.

To compute the radical expression for these numbers we use Lagrange resolvents. For example, let i be a primitive 4-th root of unity and assume that K is a field containing i. If $\alpha = R(\tau)$ generates a cyclic extension of degree 4 over K, then we use the Galois group of $K(\alpha)/K$ to compute conjugates $\alpha_1 = \alpha, \alpha_2, \alpha_3$ and α_4 of α.

We define

$$\begin{aligned} l_0 &= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \\ l_1 &= \alpha_1 + i\alpha_2 - \alpha_3 - i\alpha_4, \\ l_2 &= \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4, \\ l_3 &= \alpha_1 - i\alpha_2 - \alpha_3 + i\alpha_4. \end{aligned}$$

Then we have $4 \cdot \alpha_1 = l_0 + l_1 + l_2 + l_3$ and l_0, l_2^2, l_1^4 and l_3^4 are elements of K. A radical expression for α over K is

$$\frac{1}{4}\left(l_0 + \sqrt{l_2^2} + \sqrt[4]{l_1^4} + \sqrt[4]{l_3^4}\right).$$

In general we form a chain of subextensions of $H_5/\mathbb{Q}$. A radical expression for α over $\mathbb{Q}$ is now derived by doing similar computations as above recursively in every subextension in the chain until we end up in $\mathbb{Q}$. In chapter 5 we use that, for our choice of τ, the powers are elements of $\mathbb{Z}$, the ring of integers of $\mathbb{Q}$. We compute a sufficiently precise numerical estimate for $\alpha = R(\tau)$ to find these integers. In every step the nesting depth increases by 1. We give radical expressions that can be uniquely interpreted: we only take roots of positive real numbers for which we choose the unique positive real root.

Chapter 1

Galois groups of maximal radical extensions

Kummer theory gives a description of the Galois group of a radical extension over a ground field containing the appropriate roots of unity. In this chapter we give a similar description for certain radical extensions of a ground field that is not required to contain those roots of unity.

For a field K we fix an algebraic closure $\bar{K}$. We denote by K^* the group of invertible elements in K and by $\mu(K)$ the group of roots of unity in K. For a subgroup A of $\bar{K}^*$ we denote by $\mu(A)$ the subgroup of roots of unity in A.

Let K be a field of characteristic $\mathrm{char}(K)$. Then the group of *radicals* over K is given by

$$A = \{\alpha \in \bar{K}^* : \alpha^n \in K \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } \mathrm{char}(K) \nmid n\}.$$

This set A is a multiplicative group and the radical extension $L = K(A)$ over K is a Galois extension. In this chapter we describe its Galois group $\mathrm{Gal}(L/K)$.

In sections 1.1, 1.2 and 1.3 we give the necessary definitions and recall the main results from Kummer theory. In section 1.4 we show that there exists a subgroup C of A with

$$A/\mu(K) = \mu(\bar{K})/\mu(K) \times C/\mu(K).$$

The group C is not uniquely determined. We fix a choice for C and define the fields $M = K(\mu(A))$ and $F = K(C)$. In section 1.5 we study how $\mathrm{Gal}(L/K)$ acts on elements of M and F. This gives a subgroup Z of $\hat{\mathbb{Z}}^*$ isomorphic to $\mathrm{Gal}(M/K)$ and a Kummer-like homomorphism group J. We will show that $\mathrm{Gal}(L/K)$ can be embedded in a semidirect product $\Gamma = J \rtimes Z$ of these groups.

In order to determine the image of $\mathrm{Gal}(L/K)$ in Γ we determine the intersection D of the fields M and the maximal Kummer extension inside F over K. In sections 1.6

and 1.7 we construct the following diagram.

$$\begin{array}{ccc} \Gamma = J \rtimes Z & \longrightarrow & J \\ \downarrow & & \downarrow \\ Z & \longrightarrow & \mathrm{Gal}(D/K) \end{array}$$

The image of $\mathrm{Gal}(L/K)$ in Γ consists of the elements $(f, z) \in J \rtimes Z$ for which the images of f and z in $\mathrm{Gal}(D/K)$ are equal. Finally, in section 1.8 we prove some properties of the field D and compute it in some simple examples.

Throughout the chapter we use the case $K = \mathbb{Q}$ as a standard example. The group $\mathrm{Gal}(\mathbb{Q}(A)/\mathbb{Q})$ was described before by H.W. Lenstra in the exercises of the lecture notes 'Galois Theory for Schemes' [24].

1.1 Preliminaries

In this section we give some basic definitions and results.

We start with the basics about profinite groups. For details we refer to [12]. Given a directed set I and an inverse system of finite groups $(G_i)_{i\in I}$ we obtain a profinite group $G = \varprojlim_{i\in I} G_i$. This is a topological group under the relative topology inside the product $\prod_{i\in I} G_i$, with the discrete topology on the groups G_i. We denote an element g of G by $g = (g_i)_{i\in I}$. A profinite group is compact and Hausdorff. If the groups G_i are all abelian, then G is abelian as well.

For all $n, n' \in \mathbb{Z}_{>0}$ with $n \mid n'$ we consider the reduction maps of the abelian groups $\mathbb{Z}/n'\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. We denote by $\hat{\mathbb{Z}}$ the projective limit of $\mathbb{Z}/n\mathbb{Z}$ for all $n \in \mathbb{Z}_{>0}$ with respect to these homomorphisms. Moreover, we define for a prime number p the group

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{Z}_{>0}} \mathbb{Z}/p^n\mathbb{Z}.$$

In fact $\hat{\mathbb{Z}}$ and $\mathbb{Z}_p$, for all primes p, are rings and we have a canonical isomorphism of rings $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$, where p ranges over the prime numbers. Similarly the group $\hat{\mathbb{Z}}^*$ is the projective limit $\varprojlim_{n\in\mathbb{Z}_{>0}} (\mathbb{Z}/n\mathbb{Z})^*$ with reduction maps $(\mathbb{Z}/n'\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ for all n, n' with $n \mid n'$ in $\mathbb{Z}_{>0}$.

Let $(G_i)_{i\in I}$ be an inverse system of finite abelian groups for some index set I. We show that $G = \varprojlim_{i\in I} G_i$ is a $\hat{\mathbb{Z}}$-module. Let a be an element of $\hat{\mathbb{Z}}$; we write $a = (a_n)_{n\in\mathbb{Z}_{>0}}$. For all i we define $n_i = \#G_i$. If h is an element of the group G_i for some $i \in I$, then we define $h^a = h^{a_{n_i}}$. With this action G_i is a topological $\hat{\mathbb{Z}}$-module with discrete topology. As G inherits the action on its components we have

$$g^a = \left(g_i^{a_{n_i}}\right)_{i\in I}$$

for all $(g_i)_{i\in I} \in G$. Hence G is a topological $\hat{\mathbb{Z}}$-module as well.

Definition 1. By P we denote the set of prime numbers. A *Steinitz number* is a formal expression

$$m = \prod_{p \in P} p^{m(p)},$$

where $m(p)$ is an element of $\{0, 1, 2, \ldots, \infty\}$ for all $p \in P$.

The Steinitz numbers for which we have $m(p) < \infty$ for all primes p and $m(p) = 0$ for almost all p are identified with positive integers by multiplying out the formal expression.

Let $m = \prod_{p \in P} p^{m(p)}$ and $n = \prod_{p \in P} p^{n(p)}$ be Steinitz numbers. We say that m divides n and write $m \mid n$ if $m(p) \leq n(p)$ for all $p \in P$. Moreover, we define for a set I of Steinitz numbers the greatest common divisor and the least common multiple as

$$\gcd_{m \in I}(m) = \prod_{p \in P} p^{\min_{m \in I} m(p)} \quad \text{and} \quad \operatorname{lcm}_{m \in I}(m) = \prod_{p \in P} p^{\sup_{m \in I} m(p)}.$$

Let m be a Steinitz number, then we define $m\hat{\mathbb{Z}} = \bigcap_{n|m} n\hat{\mathbb{Z}}$, where the intersection ranges over the integers n dividing m.

Proposition 2. *The map $m \mapsto m\hat{\mathbb{Z}}$ from the set of Steinitz numbers to the set of closed subgroups of $\hat{\mathbb{Z}}$ is bijective.*

Proof. For every integer n, the subgroup $n\hat{\mathbb{Z}}$ of $\hat{\mathbb{Z}}$ is closed because it is the kernel of the continuous projection map $\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. As an intersection of closed groups, also $m\hat{\mathbb{Z}}$ is a closed subgroup of $\hat{\mathbb{Z}}$ for every Steinitz number m.

Let S be a closed subgroup of $\hat{\mathbb{Z}}$ and denote, for every integer n, the projection map $\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ by π_n. Let x be an element of $\bigcap_n \pi_n^{-1}(\pi_n(S))$. As the maps $\pi_n \colon S \longrightarrow \pi_n(S)$ are surjective, there exists for every $n \in \mathbb{Z}_{>0}$ an element $s_n \in S$ with $\pi_n(x) = \pi_n(s_n)$. It is easy to see that $\hat{\mathbb{Z}}$ equals $\varprojlim_{n \in \mathbb{Z}_{>0}} \mathbb{Z}/n!\mathbb{Z}$. Since S is a closed subgroup of $\hat{\mathbb{Z}}$, the limit x of the sequence $(s_{n!})_n$ is also contained in S. It follows $S = \bigcap_n \pi_n^{-1}(\pi_n(S))$. Writing $\pi_n(S) = d_n\mathbb{Z}/n\mathbb{Z}$ for some integer $d_n \mid n$ one obtains $S = m\hat{\mathbb{Z}}$ for the Steinitz number m that equals $\operatorname{lcm}_{n \in \mathbb{Z}_{>0}}(d_n)$. □

As a profinite group G is a continuous topological $\hat{\mathbb{Z}}$-module, the annihilator $\operatorname{Ann}_{\hat{\mathbb{Z}}}(G)$ is closed. Hence, by proposition 2, it equals $m\hat{\mathbb{Z}}$ for some Steinitz number m.

Definition 3. The *exponent* of a profinite group G is the Steinitz number $\exp(G)$ for which we have

$$\exp(G) \cdot \hat{\mathbb{Z}} = \operatorname{Ann}_{\hat{\mathbb{Z}}}(G) = \{a \in \hat{\mathbb{Z}} : g^a = 1 \text{ for all } g \in G\}.$$

Proposition 4. *Let $G = \varprojlim_{i\in I} G_i$ for finite abelian groups G_i. If the projection map $G \longrightarrow G_i$ is surjective for all $i \in I$ then we have*

$$\exp(G) = \mathrm{lcm}_{i\in I}\left(\exp(G_i)\right).$$

Proof. Let $a \in \hat{\mathbb{Z}}$. By definition we have $a \in \exp(G)\cdot\hat{\mathbb{Z}}$ if and only if $g^a = 1$ holds for all $g \in G$. As G maps surjectively to the G_i this is also equivalent to

$$g^a = 1 \quad \text{for all } g \in G_i \text{ and all } i \in I.$$

So, we have the following equivalent statements:

$$\begin{aligned} a \in \exp(G)\cdot\hat{\mathbb{Z}} &\iff a \in \exp(G_i)\cdot\hat{\mathbb{Z}} \quad \text{for all } i \in I \\ &\iff a \in \bigcap_{i\in I} \exp(G_i)\cdot\hat{\mathbb{Z}} \\ &\iff a \in \mathrm{lcm}_{i\in I}(\exp(G_i))\cdot\hat{\mathbb{Z}}. \end{aligned}$$

This concludes the proof of the proposition. □

In the next section we study Kummer extensions. The field extensions that we consider do not have to be finite. We state two main theorems of infinite Galois theory ([12]).

Definition 5. Let $K \subset L$ be an algebraic field extension. For a group $G \subset \mathrm{Aut}_K(L)$ we write L^G for the field of elements of L that are invariant under G. More explicitly we have

$$L^G = \{l \in L : \sigma(l) = l \text{ for all } \sigma \in G\}.$$

We call L/K a *Galois extension* if there exists a group $G \subset \mathrm{Aut}_K(L)$ such that $K = L^G$. If L/K is a Galois extension then we define the *Galois group* $\mathrm{Gal}(L/K)$ to be $\mathrm{Aut}_K(L)$.

Theorem 6. *Let K be a field and L a subfield of $\bar{K}$ containing K. Denote by I the set of subfields E of L for which E is a finite Galois extension of K. Then I, when partially ordered by inclusion, is a directed set. Moreover, the following four assertions are equivalent:*

- *The field L is a Galois extension of K.*
- *The field L is normal and separable over K.*
- *There is a set $F \subset K[x]$ of separable non-constant polynomials such that L is the splitting field of F over K in $\bar{K}$.*
- *The composite of the fields E in I equals L.*

If L/K is a Galois extension, then there is a group isomorphism

$$\mathrm{Gal}(L/K) \simeq \varprojlim_{E \in I} \mathrm{Gal}(E/K)$$

mapping $\sigma \in \mathrm{Gal}(L/K)$ to $(\sigma_{|_E})_{E \in I}$.

For a Galois extension L/K, this gives $\mathrm{Gal}(L/K)$ the structure of a profinite group. For finite normal subextensions E/K of L/K the projection maps to the Galois groups $\mathrm{Gal}(E/K)$ are surjective.

Theorem 7. *Let L/K be a Galois extension of fields with Galois group G. The maps*

$$\{E : E \text{ is a subextension of } L/K\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{H : H \text{ is a closed subgroup of } G\},$$

defined by $\varphi(E) = \mathrm{Aut}_E(L)$ and $\psi(H) = L^H$, are bijective and inverse to each other.

1.2 Kummer theory

In this section we give the definition of a Kummer extension of exponent m, for a Steinitz number m, and give some basic results from classical Kummer theory, following [22] chapter VI.

Definition 8. Let m be a Steinitz number and let K be a field. We define the multiplicative group

$$\mu_m(K) = \{\zeta \in K^* : \zeta^n = 1 \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid m\}.$$

When we consider a fixed field K within some algebraic closure $\bar{K}$ we will also use the notation μ_m for $\mu_m(\bar{K})$.

Similarly, we define for a multiplicative group A the group $\mu_m(A)$.

Definition 9. For $n \in \mathbb{Z}_{>0}$ we write $w_n(K) = \#\mu_n(K)$. For a Steinitz number m we define the Steinitz number $w_m(K)$ as $\mathrm{lcm}_{n|m}\big(w_n(K)\big)$, where n ranges over the positive integers dividing m.

Definition 10. Let m be a Steinitz number. A field extension L over K is called a *Kummer extension of exponent m* if it is a Galois extension, $w_m(K)$ equals m, and the group $\mathrm{Gal}(L/K)$ is a profinite abelian group of exponent dividing m.

If L/K is a Kummer extension of exponent $m = \prod_{q \in P} q^{m(q)}$ and K has characteristic p for some prime p then $\mu_p(K)$ consists of one single element as $x^p - 1 = (x-1)^p \in K[x]$ holds. Therefore we have $p \nmid w_m(K)$. We conclude $m(p) = 0$.

Proposition 11. *A field extension L/K is a Kummer extension of exponent m if and only if all finite extensions M/K with $K \subset M \subset L$ are Kummer extensions of exponent m.*

Proof. Let I be the set of all finite subextensions of L over K

Assume that L/K is a Kummer extension of exponent m with Galois group G. As L/K is abelian, also M/K is a Galois extension with abelian Galois group G_M for all $M \in I$ and, by theorem 6, we have $G = \varprojlim_{M \in I} G_M$. Let M be an element of I. As G maps surjectively to G_M we have $\exp(G_M) = n$ for some $n \in \mathbb{N}$ with $n \mid m$. Using $w_m(K) = m$, we see that the extension M/K is a Kummer extension of exponent m over K.

Now assume that all finite subextensions of L/K are Kummer extensions of exponent m. Then, as L is the composite of the fields M for $M \in I$ by theorem 6, also L/K is a Galois extension. Its Galois group is $G = \varprojlim_{M \in I} \mathrm{Gal}(M/K)$ and thus L/K is abelian. By proposition 4 the group G is of exponent m and as $w_m(K) = m$ holds we conclude that L/K is a Kummer extension of exponent m. □

Corollary 12. *A field extension L/K is a Kummer extension of exponent m if and only if all extensions M/K with $K \subset M \subset L$ are Kummer extensions of exponent m.*

Definition 13. Let n be a positive integer and let K be a field containing a primitive n-th root of unity. Then within a fixed algebraic closure $\bar{K}$ of K we define $K\left(a^{1/n}\right)$ for $a \in K$ as the splitting field of $x^n - a$ over K. For a subset W of K^* we write $K(W^{1/n})$ for the composite of the fields $K(a^{1/n})$ for all $a \in W$.

For a Steinitz number m and a field K with $w_m(K) = m$ we define for all $W \subset K^*$ the field $K(W^{1/m})$ as the composite of the fields $K(W^{1/n})$ for all $n \in \mathbb{Z}_{>0}$ with $n \mid m$.

In classical Kummer theory we have the following theorem ([22], VI, 8.2).

Theorem 14. *Let n be a positive integer and K a field containing a primitive n-th root of unity. There is a bijection from the set of all subgroups W of K^* containing K^{*n} to the set of all Kummer extensions of exponent n over K inside $\bar{K}$, given by $W \mapsto K\left(W^{1/n}\right)$.*

It is not hard to check that the inverse of this map is given by sending a Kummer extension L/K of exponent n to the subgroup $L^{*n} \cap K^*$ of K^*.

Using this correspondence we can give a nice description of the Galois group of a Kummer extension of exponent $n \in \mathbb{Z}_{>0}$.

Theorem 15. *Let n be a positive integer and let L/K be a Kummer extension of exponent n. If W is the subgroup of K^* containing K^{*n} corresponding to L/K as in theorem 14, then there is an isomorphism of topological groups*

$$\varphi\colon \mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}\left(W/K^{*n}, \mu_n(K)\right),$$

such that $\varphi(\sigma)(aK^{*n}) = \sigma(\alpha)/\alpha$ *for all* $\alpha \in L$ *and all* $a \in W$ *with* $\alpha^n = a$. *Here the group* $\mathrm{Hom}\left(W/K^{*n}, \mu_n(K)\right)$ *has the relative topology in* $\prod \mu_n(K)$, *where the product ranges over the elements of* W/K^{*n}, *and* $\mu_n(K)$ *has the discrete topology.*

Proof. Write $W_L = W$ and define for all finite subextensions E/K of L/K the unique group W_E such that $K^{*n} \subset W_E \subset W_L$ and $E = K(W_E)$. Then it is shown in [22], chapter VI theorem 8.1, that for every finite subextension E/K of L/K the map φ induces an isomorphism from $\mathrm{Gal}(E/K)$ to $\mathrm{Hom}\left(W_E/K^{*n}, \mu_n(K)\right)$. As we have $W_L/K^{*n} = \varinjlim_{E \subset L} W_E/K^{*n}$ this gives the following commuting diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\varphi} & \mathrm{Hom}(W_L/K^{*n}, \mu_n(K)) \\ \| & & \| \\ \varprojlim_E \mathrm{Gal}(E/K) & \xrightarrow{\sim} & \varprojlim_E \mathrm{Hom}(W_E/K^{*n}, \mu_n(K)). \end{array}$$

It follows that φ is an isomorphism as well. As $\mathrm{Gal}(L/K) = \varprojlim_{E \subset L} \mathrm{Gal}(E/K)$ is compact and the group $\mathrm{Hom}\left(W/K^{*n}, \mu_n(K)\right)$ is Hausdorff it remains to prove that the map φ is continuous.

Define for all $a \in W$ the map $\varphi_a \colon \mathrm{Hom}\left(W/K^{*n}, \mu_n(K)\right) \longrightarrow \mu_n(K)$ by $\varphi_a(f) = f(a \cdot K^{*n})$ and the projection map $\tau_a \colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}\left(K(a^{1/n})/K\right)$. Then φ is continuous if and only if $\varphi_a \circ \varphi$ is continuous for all $a \in W$. Let a in W and let $\alpha \in \bar{K}$ with $\alpha^n = a$. We define a map $f_a \colon \mathrm{Gal}(K(a^{1/n})/K) \longrightarrow \mu_n(K)$ by $f_a(\sigma) = \sigma(\alpha)/\alpha$. Then the map $\varphi_a \circ \varphi \colon \mathrm{Gal}(L/K) \longrightarrow \mu_n(K)$ equals $f_a \circ \tau_a$.

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\varphi_a \circ \varphi} & \mu_n(K) \\ & {\scriptstyle \tau_a} \searrow \quad \nearrow {\scriptstyle f_a} & \\ & \mathrm{Gal}\left(K(a^{1/n})/K\right) & \end{array}$$

Both τ_a, by definition of a projection map, and f_a, as a map between finite groups, are continuous and thus also $\varphi_a \circ \varphi$ is continuous. □

Let K be a field and let n be a positive integer. In theorem 14 we saw that there is a one-to-one correspondence between Kummer extensions of exponent n and subgroups W of K^* containing K^{*n}. For a Steinitz number m, we can use this correspondence to show that the intersection of Kummer extensions of exponent m can be expressed in terms of the generating radicals of the extensions.

Definition 16. Let K be a field, $\bar{K}$ an algebraic closure of K and m a Steinitz number not divisible by the characteristic of K. If μ_m is contained in K we define the *multiplicative group of radicals of exponent* m *over* K as

$$(K^*)^{1/m} = \{\alpha \in \bar{K}^* \text{ with } \alpha^n \in K^* \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid m\}.$$

Proposition 17. *Let m be a Steinitz number not divisible by the characteristic of K. If $K_1 = K(W_1)$ and $K_2 = K(W_2)$ are Kummer extensions of exponent m, for subgroups W_1, W_2 of $(K^*)^{1/m}$ containing K^*, then we have*

$$K_1 \cap K_2 = K(W_1 \cap W_2).$$

Proof. Let n be a positive integer dividing m. As $\mu_n \subset K^*$ holds, there is a bijection between the set of subgroups of K^* containing K^{*n} and the set of subgroups of $(K^*)^{1/n}$ containing K^* given by sending $K^{*n} \subset W \subset K^*$ to $W^{1/n} = \{a \in \bar{K}^* : a^n \in W\}$. Hence, theorem 14 gives a bijection between the set of subgroups of $(K^*)^{1/n}$ containing K^* and the set of Kummer extensions of exponent n over K inside $\bar{K}$. As both these sets are partially ordered we have for $K^* \subset U \subset (K^*)^{1/n}$ and $K^* \subset V \subset (K^*)^{1/n}$ that $K(U) \cap K(V) = K(U \cap V)$.

Define for $i = 1, 2$ groups $W_{i,n} = W_i \cap (K^*)^{1/n}$ for all $n \in \mathbb{Z}_{>0}$ dividing m. Then we have

$$\begin{aligned} K(W_1 \cap W_2) &= \bigcup_{n|m} K(W_{1,n} \cap W_{2,n}) \\ &= \bigcup_{n|m} \Big(K(W_{1,n}) \cap K(W_{2,n}) \Big) \\ &= K(W_1) \cap K(W_2) = K_1 \cap K_2. \end{aligned}$$

□

In chapters 3 and 4 we study denestings of nested radicals. We will use the following reformulation of theorem 14.

Corollary 18. *Let $n \in \mathbb{Z}_{>0}$ and let K be a field containing a primitive n-th root of unity. Let $\alpha, \alpha_1, \ldots, \alpha_k \in \bar{K}^*$ such that we have $\alpha^n, \alpha_1^n, \ldots, \alpha_k^n \in K$. Then α is an element of $K\big(\alpha_1, \ldots, \alpha_k\big)$ if and only if there are $b \in K^*$ and $l_1, \ldots l_k \in \mathbb{N}$ such that α can be written in the form*

$$\alpha = b \prod_{i=1}^{k} \alpha_i^{l_i}.$$

Proof. We only prove the implication from left to right as the other one is clear. Let L be the field $K(\alpha_1, \ldots, \alpha_k)$ and assume that α is contained in L^*. Let W denote the subgroup $\langle \alpha_1^n, \ldots, \alpha_k^n \rangle \cdot K^{*n}$ of L^*. Then we have $K(W^{1/n}) = L$. Hence, by the remark following theorem 14, we have $\alpha^n \in L^{*n} \cap K^* = W$. Therefore we find

$$\alpha^n = d^n \prod_{i=1}^{k} \alpha_i^{nl_i},$$

for some $d \in K^*$ and $l_1, \ldots l_k \in \mathbb{N}$. As K contains a primitive n-th root of unity, taking n-th roots and multiplying d by some n-th root of unity gives the corollary. □

1.3 Maximal Kummer extensions

In this section K is a field and $\bar{K}$ is a fixed algebraic closure of K. Furthermore m is a Steinitz number not divisible by the characteristic of K such that $w_m(K) = m$ and L/K is *the maximal Kummer extension of exponent m over K*:

$$L = K((K^*)^{1/m}) = K\big(\{\alpha \in \bar{K}^* : \alpha^n \in K \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid m\}\big).$$

In this section we describe the Galois group of the field extension L/K.

For all $n \in \mathbb{Z}_{>0}$ we defined the group μ_n as the multiplicative group of n-th roots of unity in $\bar{K}$. For all $n, n' \in \mathbb{Z}_{>0}$ with $n \mid n'$ there is a reduction map $f_{n'n}\colon \mu_{n'} \longrightarrow \mu_n$ defined by $f(x) = x^{n'/n}$. For this system of groups and maps we write $\hat{\mu} = \varprojlim_{n\in\mathbb{Z}_{>0}} \mu_n$.

The group $\hat{\mu}$ is isomorphic to $\hat{\mathbb{Z}}$ as a $\hat{\mathbb{Z}}$-module if the characteristic of K is 0. It is isomorphic to $\prod_{p\in P, p\neq q} \mathbb{Z}_p$ if the characteristic of K is $q > 0$.

One checks that we have, for all Steinitz numbers m, a canonical isomorphism of $\hat{\mathbb{Z}}$-modules

$$\hat{\mu}/\hat{\mu}^m \xrightarrow{\sim} \varprojlim_{n\mid m} \mu_n,$$

where $\hat{\mu}^m = \hat{\mu}^{(m\hat{\mathbb{Z}})}$ and where n ranges over the positive integers.

Similarly, we have $\hat{\mathbb{Z}}/m\hat{\mathbb{Z}} \xrightarrow{\sim} \varprojlim_{n\mid m} \mathbb{Z}/n\mathbb{Z}$ and $(\hat{\mathbb{Z}}/m\hat{\mathbb{Z}})^* \xrightarrow{\sim} \varprojlim_{n\mid m} (\mathbb{Z}/n\mathbb{Z})^*$.

Theorem 19. *Let L/K be the maximal Kummer extension of K of exponent m. There is an isomorphism of topological groups*

$$\mathrm{Gal}(L/K) \simeq \mathrm{Hom}(K^*, \hat{\mu}/\hat{\mu}^m),$$

given by

$$\sigma \mapsto \left(a \mapsto \left(\frac{\sigma(\alpha_n)}{\alpha_n}\right)_{n\in\mathbb{Z}_{>0}, n\mid m}\right),$$

where for all $a \in K^*$ and all $n \in \mathbb{Z}_{>0}$ with $n \mid m$ we choose $\alpha_n \in L$ with $\alpha_n^n = a$.

Proof. Define for all $n \in \mathbb{Z}_{>0}$ with $n \mid m$ the field $L_n = K((K^*)^{1/n})$. As L is the composite of the L_n for all $n \in \mathbb{Z}_{>0}$ with $n \mid m$, an application of theorem 6 shows that the group $G = \mathrm{Gal}(L/K)$ is topologically isomorphic to $\varprojlim_{n\mid m} \mathrm{Gal}(L_n/K)$.

Let n be a positive integer with $n \mid m$. Using theorems 14 and 15 we see that $\mathrm{Gal}(L_n/K)$ is isomorphic to $\mathrm{Hom}\big(K^*/K^{*n}, \mu_n(K)\big)$ under the isomorphism sending $\sigma \in \mathrm{Gal}(L_n/K)$ to the map $(aK^{*n} \mapsto \sigma(\alpha)/\alpha)$, where α is an element of L with $\alpha^n = a$.

As every homomorphism from K^* to μ_n annihilates K^{*n} we have

$$\mathrm{Gal}(L_n/K) \simeq \mathrm{Hom}(K^*, \mu_n).$$

Let $n, n' \in \mathbb{Z}_{>0}$ such that $n \mid n'$ then we get the following diagram.

$$\begin{array}{ccc} \mathrm{Gal}(L_{n'}/K) & \xrightarrow{\sim} & \mathrm{Hom}(K^*, \mu_{n'}) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L_n/K) & \xrightarrow{\sim} & \mathrm{Hom}(K^*, \mu_n) \end{array}$$

The map from $\mathrm{Hom}(K^*, \mu_{n'})$ to $\mathrm{Hom}(K^*, \mu_n)$ is induced by the identity on K^* and the homomorphisms $f_{n'n}\colon \mu_{n'} \to \mu_n$ are defined by $f_{n'n}(x) = x^{n'/n}$. It is easy to check that the diagram commutes.

As the maps $f_{n'n}$ are the same as in the definition of $\hat{\mu}$, we get the following isomorphisms of topological groups:

$$\begin{aligned} \mathrm{Gal}(L/K) &\simeq \varprojlim_{n|m} \mathrm{Gal}(L_n/K) \\ &\simeq \varprojlim_{n|m} \mathrm{Hom}(K^*, \mu_n) \\ &\overset{(*)}{\simeq} \mathrm{Hom}(K^*, \varprojlim_{n|m} \mu_n) \\ &= \mathrm{Hom}(K^*, \hat{\mu}/\hat{\mu}^m). \end{aligned}$$

The canonical map $(*)$ is a homeomorphism as the product topologies on

$$\prod_{n|m} \Big(\prod_{a \in K^*} \mu_n \Big) \quad \text{and} \quad \prod_{a \in K^*} \Big(\prod_{n|m} \mu_n \Big)$$

are the same. □

Now we state a lemma that we use in section 1.7. Define $m^\infty = \prod_{p|m} p^\infty$, where the product ranges over the prime numbers dividing m and write $w = w_{m^\infty}(K)$. Then μ_w is contained in K, the field $K(\mu_{wm})$ is contained in L and $\mathrm{Gal}(L/K(\mu_{wm}))$ is a subgroup of $\mathrm{Gal}(L/K)$.

Lemma 20. *If L/K is the maximal Kummer extension of K of exponent m, then the isomorphism of theorem 19 induces an isomorphism*

$$\mathrm{Gal}\big(L/K(\mu_{wm})\big) \simeq \mathrm{Hom}\big(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\big).$$

Proof. Let φ be the isomorphism from theorem 19. We define the homomorphism

$$\varphi'\colon \mathrm{Gal}\big(L/K(\mu_{wm})\big) \longrightarrow \mathrm{Hom}\big(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\big)$$

by $\varphi'\big(\sigma(a \cdot \mu_w)\big) = \varphi(\sigma(a))$ for all $a \in K^*$. We show that φ' is well-defined. Let $a, b \in K^*$ with $a/b \in \mu_w$. Let $n \in \mathbb{Z}_{>0}$ with $n \mid m$ and let $\sigma \in \mathrm{Gal}\big(L/K(\mu_{wm})\big)$.

Then, for all $\alpha, \beta \in L$ with $\alpha^n = a$ and $\beta^n = b$ we have $\sigma(\alpha)/\alpha = \sigma(\beta)/\beta$ as $\sigma(\alpha/\beta) = \alpha/\beta \in K(\mu_{wm})$.

This gives the following commuting diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow[\varphi]{\sim} & \mathrm{Hom}(K^*, \hat{\mu}/\hat{\mu}^m) \\ \uparrow{\scriptstyle \sigma\mapsto\sigma} & & \uparrow{\scriptstyle \psi} \\ \mathrm{Gal}\left(L/K(\mu_{wm})\right) & \xrightarrow{\varphi'} & \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right), \end{array}$$

where $\psi(f)(a) = f\big(a \cdot \mu_w\big)$. The homomorphism φ' is injective as φ is injective. Let $f \in \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right)$ and define $\sigma = \varphi^{-1}(\psi(f))$. Let $a \in \mu_w$. As μ_w is contained in the kernel of f we have $f(a) = 1 \in \hat{\mu}/\hat{\mu}^m$. Therefore also $\psi(f)(a) = 1 \in \hat{\mu}/\hat{\mu}^m$ and consequently for all integer divisors n of m we have $\sigma(\alpha_n)/\alpha_n = 1$ for all $\alpha_n \in L$ with $\alpha_n^n = a$. Hence it follows $\sigma(\alpha) = \alpha$ for all $\alpha \in L$ with $\alpha^n = 1$ and $n \mid wm$. So $\sigma \in \mathrm{Gal}(L/K)$ is contained in $\mathrm{Gal}(L/K(\mu_{mw}))$. As we have $\varphi'(\sigma) = f$, we conclude that φ' is surjective. □

1.4 Separating the roots of unity

We fix the following notation for the rest of this chapter:

K	is a field;
$\bar{K}$	is an algebraic closure of K;
m	is a Steinitz number not divisible by the characteristic of K;
w	is $w_{m^\infty}(K)$;
A	is the multiplicative group of radicals of exponent m over K defined by $A = \{\alpha \in \bar{K}^* : \alpha^n \in K \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid m\}$;
L	is the field $K(A)$.

The torsion elements in the groups K^* and A are precisely the roots of unity. In particular the groups of m^∞-torsion in K^* and A are $\mu_{m^\infty}(K^*) = \mu_w$ respectively $\mu_{m^\infty}(A) = \mu_{mw}$.

We would like to write A as a direct product with its torsion subgroup as one of the factors. Unfortunately, as we will see in example 22, this is not possible for every abelian group. However, we can write A/μ_w as a direct product with its torsion subgroup as one of the factors. To show this we consider the inclusion map

$$\gamma\colon \mu_{mw}/\mu_w \longrightarrow A/K^*.$$

Theorem 21. *There exists a homomorphism $\delta\colon A/K^* \longrightarrow \mu_{mw}/\mu_w$ such that $\delta\gamma = 1$ holds.*

We will use the rest of this section to prove this theorem and to construct the desired splitting of A/μ_w. But first we show that there exist abelian groups that are not a direct product with the torsion subgroup as a factor.

Example 22. Consider the group $\prod_p \mathbb{F}_p$, where p ranges over the prime numbers. The torsion subgroup of $\prod_p \mathbb{F}_p$ is $\bigoplus_p \mathbb{F}_p$. For $H = \left(\prod_p \mathbb{F}_p\right)/\bigoplus_p \mathbb{F}_p$ the sequence

$$0 \longrightarrow \bigoplus_p \mathbb{F}_p \longrightarrow \prod_p \mathbb{F}_p \longrightarrow H \longrightarrow 0$$

is exact. First we show that H is divisible. Let $x = (x_p)_{p\in P}$ be an element of $\prod_p \mathbb{F}_p$ and let n be a positive integer. We define $y = (y_p)_{p\in P}$ by

$$y_p = \begin{cases} x_p/n & \text{if } p \nmid n \\ 0 & \text{if } p \mid n. \end{cases}$$

Then we have $ny - x \in \bigoplus_p \mathbb{F}_p$. So, for every $\bar{x} \in H$ and every $n \in \mathbb{Z}_{>0}$ there is an element $\bar{y} \in H$ with $\bar{x} = n\bar{y}$. This shows that H is a divisible group. If the sequence splits, H is isomorphic to the kernel of the splitting map $\prod_p \mathbb{F}_p \longrightarrow \bigoplus_p \mathbb{F}_p$ and consequently H is isomorphic to a subgroup of $\prod_p \mathbb{F}_p$. But this is not possible as $\prod_p \mathbb{F}_p$ has no non-zero divisible subgroups. We conclude that the sequence above does not split. It is therefore not possible to give a splitting of $\prod_p \mathbb{F}_p$ with its torsion subgroup as one of the factors.

Inspired by the previous example we also construct a Kummer extension generated by a group of radicals for which the torsion subgroup is not a direct factor. Example 23 is based on a suggestion by B. Poonen.

Example 23. Denote by ζ_p a primitive p-th root of unity. Consider the fields $K = \mathbb{Q}(\zeta_p \colon p \in P)$ and $K(\sqrt[p]{2 \cdot \zeta_p} \colon p \in P)$ and let R be the generating group of radicals $\langle K^*, \sqrt[p]{2 \cdot \zeta_p} \colon p \in P\rangle$. Below we will show that $R/\mu(R)$ is not a direct factor of R. It follows immediately that also $\mu(R)$ is not a direct factor of R.

First we determine $\mu(R)$. Suppose ζ is a root of unity contained in R. Then ζ is of the form $k \prod \sqrt[p]{2 \cdot \zeta_p}^{n_p}$ for some element k of K and integers $0 \leq n_p < p$. Let r be the product of all primes for which we have $n_p \neq 0$ and let n be the least common multiple of r^2 and the order of ζ. Then we have

$$\zeta^n = 1 = k^n \cdot \prod_{p\in P} 2^{n_p \cdot n/p} \in K.$$

Let $\mathfrak{p}$ be a prime above 2 in $\mathbb{Q}(k)$. We normalise the $\mathfrak{p}$-valuation in $\mathbb{Q}(k)/\mathbb{Q}$ by $v_\mathfrak{p}(2) = 1$ and find

$$-n \cdot v_\mathfrak{p}(k) = v_\mathfrak{p}(2) \sum_{p\in P} n_p \cdot n/p = \sum_{p\in P} n_p \cdot n/p.$$

Suppose that p is a prime with $n_p \neq 0$. Then p divides n. Let l be the largest integer with $p^l \mid n$. We have $p^l \mid n_q \cdot n/q$ for all primes $q \neq p$. As p^l is not a

divisor of $n_p \cdot n/p$, we have $p^l \nmid \sum_p n_p \cdot n/p$. But p^l is a divisor of n and we have a contradiction. We conclude that n_p equals 0 for all primes p and that $\mu(R)$ equals $\mu(K^*) = \langle \mu_p \colon p \in P \rangle$.

If $R/\mu(R)$ is a direct factor of R then there exists a splitting of the projection map π in the exact sequence

$$0 \longrightarrow \mu(R) \longrightarrow R \xrightarrow{\pi} R/\mu(R) \longrightarrow 0.$$

Clearly, the element $2 \cdot \mu(R)$ is a p-th power in $R/\mu(R)$ for all primes p. Hence, the image of $2 \cdot \mu(R)$ under the splitting homomorphism is also a p-th power for all primes p. By definition of π this image is of the form $2 \cdot \zeta$ for some root of unity ζ. Let q be a prime that does not divide the order of ζ. Then each of the elements ζ, $2 \cdot \zeta$ and $2 \cdot \zeta_q$ is contained in R^q. It follows that also ζ_q is contained in R^q. But this is impossible as $\mu(R)$ equals $\langle \mu_p \colon p \in P \rangle$. Therefore the sequence does not split and the group R is not a direct product with $\mu(R)$ as one of the factors.

To construct a splitting of the inclusion map γ from the beginning of this section, we remark that A/K^* is a torsion group. All elements are of finite order and we define

$$A_p = \{\alpha \in \bar{K}^* : \alpha^n \in K \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid \gcd(m, p^\infty)\}.$$

We have

$$A/K^* = \bigoplus_{p \in P} A_p/K^*.$$

Also μ_{mw}/μ_w is a torsion group, hence we have

$$\mu_{mw}/\mu_w = \bigoplus_{p \in P} U_p, \qquad \text{where } U_p = \mu_{\gcd(p^\infty, m)w}/\mu_w.$$

The p-part of γ is the restriction of γ to U_p, so we have $\gamma_p \colon U_p \longrightarrow A_p/K^*$. It suffices to show that there exists a splitting of γ_p for every prime p dividing m.

Definition 24. Let R be a ring. An R-module Q is called *injective*, if given any R-module N, a submodule N' and a homomorphism $N' \longrightarrow Q$, there exists an extension of this homomorphism to N.

Lemma 25. *Let p be a prime dividing m. Let R be a ring and suppose we have R-module structures on U_p and A_p/K^* such that $\gamma_p \colon U_p \longrightarrow A_p/K^*$ is an R-module homomorphism and such that the group U_p is an injective R-module. Then there exists a homomorphism $\delta_p \colon A_p/K^* \longrightarrow U_p$ with $\delta_p \gamma_p = 1$.*

Proof. When we take $Q = N' = U_p$ and $N = A_p/K^*$, in the notation of definition 24, then there exists an extension δ_p of the identity on U_p mapping A_p/K^* to U_p, as U_p is injective. For this homomorphism we have $\delta_p \gamma_p = 1$. □

First we prove that U_p is an injective $\mathbb{Z}$-module in the case that $p^\infty \mid m$.

Lemma 26. *An abelian group is injective if and only if it is divisible.*

Proof. This is proved in [22], chapter XX, lemma 4.2. □

Lemma 27. *If p is a prime with $p^\infty \mid m$ then the group U_p is an injective $\mathbb{Z}$-module.*

Proof. It suffices to prove that $U_p = \mu_{p^\infty w}/\mu_w$ is divisible; to do so, we show that for every $a \in U_p$ and for every prime q the group U_p contains an element b with $a = b^q$.

Let a be in U_p and let q be a prime. Then a is the class of a p^n-th root of unity ζ_{p^n} for some $n \in \mathbb{N}$. If p equals q there exists a primitive p^{n+1}-th root of unity ζ in U_p with $\zeta^p = \zeta_{p^n}$; we take $b = \zeta \cdot \mu_w \in U_p$. If $p \neq q$ then $\gcd(p, q) = 1$ and thus there are $x, y \in \mathbb{Z}$ with $xp^n + yq = 1$. Let $b = \zeta_{p^n}^y \cdot \mu_w \in U_p$, then we have $b^q = \zeta_{p^n} \cdot \mu_w$. □

Now we will consider the case that p is a prime dividing m such that $p^\infty \nmid m$. Again we will show that U_p is an injective module, only this time, the group is not an injective $\mathbb{Z}$-module, but it is an injective $\mathbb{Z}/p^n\mathbb{Z}$-module.

Lemma 28 (Baer's Criterion). *Let R be a ring and E an R-module. Then E is an injective R-module if and only if for all left ideals $J \subset R$, every R-module homomorphism $J \longrightarrow E$ can be extended to a homomorphism $R \longrightarrow E$.*

Proof. This is theorem 2.3.1 in [39]. □

Lemma 29. *Let p be a prime dividing m with $p^\infty \nmid m$ and let $n \in \mathbb{Z}_{>0}$ with $p^n \mid m$ and $p^{n+1} \nmid m$. Then the group U_p is an injective $\mathbb{Z}/p^n\mathbb{Z}$-module.*

Proof. If p^∞ divides w then U_p is the trivial group and hence U_p is an injective $\mathbb{Z}/p^n\mathbb{Z}$-module.

Assume $p^\infty \nmid w$. Then U_p is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. We apply Baer's criterion. Let J be an ideal of $\mathbb{Z}/p^n\mathbb{Z}$, then there exists some $k \in \mathbb{N}$ with $k \leq n$ such that $J = p^k \cdot \mathbb{Z}/p^n\mathbb{Z}$ holds. When $\tau\colon J \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ is a homomorphism then we have $\tau(J) \subset p^k \cdot \mathbb{Z}/p^n\mathbb{Z}$. As both J and $\mathbb{Z}/p^n\mathbb{Z}$ are additive cyclic groups generated by p^k respectively 1, we define an extension $\tau'\colon \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ of τ as follows. Let $\alpha \in \mathbb{Z}/p^n\mathbb{Z}$ such that $\tau(p^k) = p^k \cdot \alpha$ holds. We define $\tau'(1) = \alpha$. Then for all $\beta = p^k \cdot \beta' \in J$ we have

$$\tau(\beta) = \beta' \cdot \tau(p^k) = \beta' \cdot p^k \cdot \alpha = \beta \cdot \tau'(1) = \tau'(\beta),$$

so, τ' is an extension of τ. We conclude that $\mathbb{Z}/p^n\mathbb{Z}$, and consequently U_p, is an injective $\mathbb{Z}/p^n\mathbb{Z}$-module. □

Proof of theorem 21. Let p be a prime with $p^\infty \mid m$. Then by lemma 27 the group U_p is an injective $\mathbb{Z}$-module. As an abelian group also A_p/K^* is a $\mathbb{Z}$-module and the inclusion map γ_p is a $\mathbb{Z}$-module homomorphism.

Let p be a prime dividing m and let $n \in \mathbb{Z}_{>0}$ with $p^n \mid m$ and $p^{n+1} \nmid m$. Then by lemma 29 the group U_p is an injective $\mathbb{Z}/p^n\mathbb{Z}$-module. As an abelian group annihilated by p^n also A_p/K^* is a $\mathbb{Z}/p^n\mathbb{Z}$-module and the inclusion map γ_p is a $\mathbb{Z}/p^n\mathbb{Z}$-module homomorphism.

Therefore, by lemma 25, for every prime p dividing m there exists a homomorphism $\delta_p \colon A_p/K^* \longrightarrow U_p$ with $\delta_p\gamma_p = 1$. Since A/K^* is the direct sum of the groups A_p/K^* for $p \in P$ the maps δ_p on the p-part together give us a splitting δ of γ. □

Corollary 30. *There exists a subgroup C of A with $K^* \subset C$ such that*

$$A/\mu_w = \mu_{mw}/\mu_w \times C/\mu_w.$$

Proof. By theorem 21 there exists a homomorphism $\delta \colon A/K^* \longrightarrow \mu_{mw}/\mu_w$ such that $\delta\gamma = 1$. We define $\psi \colon A/\mu_w \longrightarrow \mu_{mw}/\mu_w$ by $\psi(a) = \delta(a \cdot K^*)$ for all $a \in A/\mu_w$. Let $\varphi \colon \mu_{mw}/\mu_w \longrightarrow A/\mu_w$ be the inclusion map. Then we have the following splitting exact sequence:

$$0 \longrightarrow \mu_{mw}/\mu_w \underset{\varphi}{\overset{\psi}{\rightleftarrows}} A/\mu_w \longrightarrow \ker(\psi) \longrightarrow 0\ .$$

We conclude

$$A/\mu_w = \mu_{mw}/\mu_w \times \ker(\psi).$$

Let C be the set of all elements c of A with $c \cdot \mu_w \in \ker(\psi)$, then C is a subgroup of A and by construction we have $K^*/\mu_w \subset \ker(\psi)$. □

Example 31. We consider $\bar{\mathbb{Q}} \subset \mathbb{C}$. We set $K = \mathbb{Q}$ and $m = \prod_{p \in P} p^\infty$. We have $L = K(A)$ with

$$A = \{\alpha \in \mathbb{C}^* \text{ with } \alpha^n \in \mathbb{Q} \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

There exists a splitting of A with $\mu_{mw}(A) = \mu(\mathbb{C})$ as a component:

$$A = \mu(\mathbb{C}) \times \{\alpha \in \mathbb{R}_{>0} \text{ with } \alpha^n \in \mathbb{Q} \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

Taking both factors modulo $\mu_w(\mathbb{Q}^*) = \{\pm 1\}$ gives a splitting of A/μ_w. The corresponding maps δ and ψ are given by $\delta(a \cdot \mathbb{Q}^*) = 1 \cdot \{\pm 1\}$ for all $a \in A \cap \mathbb{R}_{>0}$ and $\delta(\zeta \cdot \mathbb{Q}^*) = \zeta \cdot \{\pm 1\}$ for every root of unity ζ and $\psi(a \cdot \mu_w) = \delta(a \cdot \mathbb{Q}^*)$ for all $a \in A$. Note that many other splittings can be found.

1.5 Galois action on radicals

In this section we embed the group $\mathrm{Gal}(L/K)$ in a semidirect product

$$\Gamma = \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m) \rtimes Z$$

where Z is a particular subgroup of $(\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^*$.

Let from now on C be a fixed subgroup of A with $K^* \subset C$ such that

$$A/\mu_w = \mu_{wm}/\mu_w \times C/\mu_w.$$

The existence of C follows from corollary 30. We define the following two subfields of $L = K(A)$:

$$M = K(\mu_{wm}) \quad \text{and} \quad F = K(C).$$

First we will consider the action of $\mathrm{Gal}(L/K)$ on the roots of unity in μ_{wm}, then the action on C. Let σ be an element of $\mathrm{Gal}(L/K)$, then for every $n \in \mathbb{Z}_{>0}$ with $n \mid wm$ there exists a natural number $k_{\sigma,n}$ such that for every primitive n-th root of unity, ζ_n, we have $\sigma(\zeta_n) = \zeta_n^{k_{\sigma,n}}$. Define the homomorphism

$$\omega\colon \mathrm{Gal}(L/K) \longrightarrow (\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^* \simeq \varprojlim_{n \mid wm} (\mathbb{Z}/n\mathbb{Z})^*$$

by

$$\omega(\sigma) = (k_{\sigma,n})_{n \mid wm}\,.$$

We show that ω is well-defined. Let $n, n' \in \mathbb{Z}_{>0}$ with $n \mid n'$. For every primitive n'-th root of unity $\zeta_{n'}$ there exists a primitive n-th root of unity ζ_n with $\zeta_{n'}^{n'/n} = \zeta_n$. Now for all $\sigma \in \mathrm{Gal}(L/K)$ the elements $k_{\sigma,n} \in (\mathbb{Z}/n\mathbb{Z})^*$ and $k_{\sigma,n'} \in (\mathbb{Z}/n'\mathbb{Z})^*$ satisfy

$$\zeta_n^{k_{\sigma,n}} = \sigma(\zeta_n) = \sigma(\zeta_{n'}^{n'/n}) = (\zeta_{n'}^{k_{\sigma,n'}})^{n'/n} = \zeta_n^{k_{\sigma,n'}}.$$

Hence, we have $k_{\sigma,n} \equiv k_{\sigma,n'}$ modulo n for all $n \mid n'$ in $\mathbb{Z}_{>0}$ and all σ in $\mathrm{Gal}(L/K)$. It follows that $\omega(\sigma)$ is an element of $(\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^*$ for all σ.

Lemma 32. *The homomorphism ω induces an isomorphism of topological groups between the Galois group $\mathrm{Gal}(M/K)$ and a closed subgroup Z of the kernel of the projection map $\pi_w\colon (\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^* \longrightarrow (\hat{\mathbb{Z}}/w\hat{\mathbb{Z}})^*$.*

Proof. Since we have $M = K(\mu_{wm})$ the map ω is injective on $\mathrm{Gal}(M/K)$. As μ_w is contained in K^* we have $k_{\sigma,n} = 1$ for all $n \in \mathbb{Z}_{>0}$ with $n \mid w$ and all $\sigma \in \mathrm{Gal}(L/K)$. Therefore, the image $Z = \omega(\mathrm{Gal}(M/K))$ is a subgroup of the kernel of the projection map π_w.

The map ω is continuous if and only if for all $n \in \mathbb{Z}_{>0}$ with $n \mid wm$ the compositions ω_n of ω with the projection on $(\mathbb{Z}/n\mathbb{Z})^*$ are continuous. The maps ω_n factor over $\mathrm{Gal}(K(\zeta_n)/K)$:

$$\begin{array}{ccc} \mathrm{Gal}(M/K) & \xrightarrow{\quad\omega_n\quad} & (\mathbb{Z}/n\mathbb{Z})^* \\ & \searrow \quad \nearrow_{\sim} & \\ & \mathrm{Gal}\left(K(\zeta_n)/K\right). & \end{array}$$

Being the composition of a projection map and an isomorphism of finite groups, the homomorphisms ω_n are continuous.

As both $\mathrm{Gal}(M/K)$ and $(\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^*$ are profinite groups, the map induced by ω is a continuous bijection from a compact space to a Hausdorff space and therefore it is a homeomorphism. □

We fix the following notation:

$$Z = \omega\big(\mathrm{Gal}(M/K)\big) \subset (\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^*,$$

and we define

$$\Gamma = \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m) \rtimes Z,$$

where the action of Z on $\mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m)$ is induced by the action of $(\hat{\mathbb{Z}}/wm\hat{\mathbb{Z}})^*$ on $\hat{\mu}/\hat{\mu}^m$.

Now we consider the more difficult part of the action of $\mathrm{Gal}(L/K)$ on A: the action on the elements of C. The extension $F = K(C)$ over K is, in general, not a Galois extension, but $K(\mu_m)(C)/K(\mu_m)$ is. Inspired by the homomorphism from lemma 20 we define a map

$$\chi\colon\ \mathrm{Gal}(L/K) \longrightarrow \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m),$$

describing the action of $\mathrm{Gal}(L/K)$ on the elements of C.

First we define the map χ in our standard example.

Example 33. We look at the situation of example 31 again. We assume that the fixed group C for this example is the group of real radicals in $\mathbb{C}$. Let the elements of $C/\{\pm 1\}$ be represented by the radicals in the set

$$\{\alpha \in \mathbb{R}_{>0} : \alpha^n \in \mathbb{Q}^* \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

The field F is defined as

$$F = K(C) = \mathbb{Q}\big(\{\alpha \in \mathbb{R}_{>0} : \alpha^n \in \mathbb{Q}^* \text{ for some } n \in \mathbb{Z}_{>0}\}\big).$$

Define for every $a \in \mathbb{Q}_{>0}$ and for all $n \in \mathbb{Z}_{>0}$ the element $\sqrt[n]{a}$ as the positive real n-th root of a. In analogy with Kummer theory we define the map χ by

$$\chi(\sigma) = \Big(a \mapsto \big(\sigma(\sqrt[n]{a})/\sqrt[n]{a}\big)_{n\in\mathbb{Z}_{>0}}\Big) \in \mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu})$$

for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and for all $a \in \mathbb{Q}_{>0}$. We now show that χ is a well-defined map. Take $a \in \mathbb{Q}_{>0}$ and define for $n \in \mathbb{Z}_{>0}$ and $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ the root of unity $\zeta_{\sigma,n}$ by $\sigma(\sqrt[n]{a})/\sqrt[n]{a}$. Then we have for all $n, n' \in \mathbb{Z}_{>0}$ with $n \mid n'$

$$\zeta_{\sigma,n}\sqrt[n]{a} = \sigma(\sqrt[n]{a}) = \sigma(\sqrt[n']{a})^{n'/n} = \zeta_{\sigma,n'}^{n'/n}$$

and thus, by definition of $\hat{\mu}$, we have $\chi(\sigma) \in \mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu})$. As $\mathbb{Q}_{>0}$ is a system of representatives of $\mathbb{Q}^*/\{\pm 1\}$ this also defines a map from $\mathrm{Gal}(L/\mathbb{Q})$ to $\mathrm{Hom}(\mathbb{Q}^*/\{\pm 1\}, \hat{\mu})$.

To define the map χ in the general case we use the following lemma.

Lemma 34. *For every $a \in K^*$ and every $n \in \mathbb{Z}_{>0}$ with $n \mid m$ there exists a unique n-th root of $a \cdot \mu_w$ in C/μ_w.*

Proof. Let $a \in K^*$ and let $n \in \mathbb{Z}_{>0}$ with $n \mid m$. There is an element $b \in A$ such that $b^n = a$. Therefore we have

$$(b \cdot \mu_w)^n = a \cdot \mu_w = (1 \cdot \mu_w)(a \cdot \mu_w) \in \mu_{wm}/\mu_w \times C/\mu_w.$$

As $b \cdot \mu_w$ is an element of A/μ_w there exist unique $\zeta \in \mu_{wm}/\mu_w$ and $c \in C/\mu_w$ such that $b \cdot \mu_w = \zeta \cdot c$ holds. For these ζ and c we have $\zeta^n = 1 \cdot \mu_w$ and $c^n = a \cdot \mu_w$, this proves the existence of an n-th root of $a \cdot \mu_w$ in C/μ_w.

Let x, y be elements of C/μ_w with $x^n = y^n \in K^*/\mu_w$ for some $n \in \mathbb{Z}_{>0}$. The quotient x/y is contained in $C/\mu_w \cap \mu_{mw}/\mu_w = \{1\}$, hence x and y are equal. Therefore the n-th root of $a \cdot \mu_w$ in C/μ_w is unique. □

Note that $\mathrm{Gal}(L/K)$ acts on A. As μ_w is contained in K we have $\sigma(c)/c = \sigma(c')/c'$ for all $c, c' \in C$ with $c \cdot \mu_w = c' \cdot \mu_w$ and for all $\sigma \in \mathrm{Gal}(L/K)$.

Now we are ready to define the map χ. We assign to $\sigma \in \mathrm{Gal}(L/K)$ a homomorphism that for every $n \in \mathbb{Z}_{>0}$ with $n \mid m$ sends $a \in K^*/\mu_w$ to $\sigma(x_n)/x_n \in \mu_n$ where x_n is an element of C with $x_n^n \cdot \mu_w = a$. That is, we define

$$\chi\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m)$$

by

$$\chi(\sigma) = \left(a \mapsto \left(\frac{\sigma(x_n)}{x_n}\right)_{n|m}\right), \quad \text{where } x_n \in C \text{ with } x_n^n \cdot \mu_w = a.$$

By lemma 34 we see that for all $n, n' \in \mathbb{Z}_{>0}$ we have $x_{nn'}^n \cdot \mu_w = x_{n'} \cdot \mu_w$. In exactly the same way as we did in example 33 one proves that χ is a well-defined map. This map in general is not a homomorphism. Let ρ be the map given by

$$\rho\colon \mathrm{Gal}(L/K) \longrightarrow \Gamma, \quad \text{where } \rho(\sigma) = \big(\chi(\sigma), \omega(\sigma)\big).$$

Proposition 35. *The map ρ is an injective homomorphism.*

Proof. Let a be an element of K^*/μ_w and define $x = (x_n)_{n|m} \in \prod_{n|m} C$, where $x_n^n \cdot \mu_w = a$ for all $n \in \mathbb{Z}_{>0}$ dividing m and where again for all $n, n' \in \mathbb{Z}_{>0}$ we have $x_{nn'}^n \cdot \mu_w = x_{n'} \cdot \mu_w$. For all $\sigma \in \mathrm{Gal}(L/K)$ we denote by $\sigma(x)/x$ the element $\left(\frac{\sigma(x_n)}{x_n}\right)_{n|m}$ of $\hat{\mu}/\hat{\mu}^m$. For all $\sigma, \tau \in \mathrm{Gal}(L/K)$ we have

$$\begin{aligned}
\chi(\sigma\tau)(a) = \frac{\sigma\tau(x)}{x} &= \left(\frac{\sigma(x)}{x}\right) \cdot \left(\frac{\sigma\tau(x)}{\sigma(x)}\right) \\
&= \chi(\sigma)(a) \cdot \sigma\left(\frac{\tau(x)}{x}\right) \\
&= \chi(\sigma)(a) \cdot \chi(\tau)^{\omega(\sigma)}(a).
\end{aligned}$$

So, as ω is a homomorphism, ρ is a homomorphism as well. Let σ, τ be elements of $\mathrm{Gal}(L/K)$ with $\rho(\sigma) = \rho(\tau)$. We have $\omega(\sigma) = \omega(\tau)$ and $\chi(\sigma) = \chi(\tau)$. It follows that $\sigma(c) = \tau(c)$ holds for all $c \in \mu_{mw}$ and that $\sigma(c) = \tau(c)$ holds for all $c \in C$. Hence σ equals τ and ρ is injective. □

Proposition 36. *The map ρ is continuous.*

Proof. As we defined $\rho(\sigma) = \big(\chi(\sigma), \omega(\sigma)\big)$ we see that ρ is continuous if and only if both χ and ω are continuous. In lemma 32 we saw that ω is continuous.

The map χ is continuous if and only if for all $n \mid m$ the compositions χ_n of χ and the projection on μ_n are continuous. These factor over the Galois groups of the subextensions $K(\zeta_n)(a^{1/n})/K$ of L/K:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\quad\chi_n\quad} & \mu_n\ . \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}\left(K(\zeta_n)(a^{1/n})/K\right). & \end{array}$$

As the composition of a projection map and a homomorphism of finite groups the homomorphisms χ_n are continuous. □

In this section we defined the maps in the following commuting diagram.

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\ \rho\ } & \Gamma \\ \downarrow \text{ res} & & \downarrow \text{ projection} \\ \mathrm{Gal}(M/K) & \xrightarrow{\ \omega\ } & Z \end{array}$$

As ρ is injective, the group $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of Γ.

1.6 The maximal Kummer subextension in L

In the previous section we introduced fields F and M such that the composite of F and M is L. In general, if a Galois extension is the composite of two normal subextensions, one can express its Galois group in terms of the Galois groups of the subextensions. Unfortunately, the field F may not be a normal extension. In order to identify the image of $\mathrm{Gal}(L/K)$ in $\Gamma = \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m) \rtimes Z$ we introduce a normal subfield of F.

Fix the notation $v = \gcd(m, w)$. We define a Kummer subextension F_v/K of F/K by

$$F_v = K\left(\{c \in C \text{ with } c^n \in K^* \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid v\}\right).$$

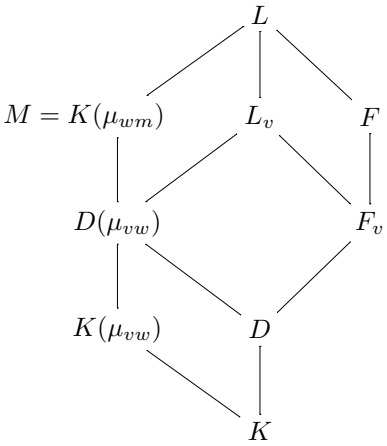
The maximal Kummer extension of exponent v inside L is

$$L_v = K\left(\{a \in A \text{ with } a^n \in K^* \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid v\}\right).$$

Below we prove

$$L_v = F_v \cdot K(\mu_{vw}) \quad \text{and} \quad K(\mu_{vw}) \cap F_v = K.$$

This enables us to extend the diagram of subextensions of L/K. Let D be the intersection field $M \cap F_v$, then we have the following diagram.



Theorem 37. *The field L_v is $F_v \cdot K(\mu_{vw})$ and we have $K(\mu_{vw}) \cap F_v = K$.*

Proof. Define groups of generating radicals for the fields $K(\mu_{vw})$ and F_v by $W_1 = \langle \mu_{vw}, K^* \rangle$ and $W_2 = \{c \in C \text{ with } c^n \in K^* \text{ for some } n \mid v\}$. As the group $(K^*)^{1/v}$ equals $\langle W_1, W_2 \rangle$ we see that L_v is the composite of $K(\mu_{vw})$ and F_v.

By proposition 17, the intersection of the fields $K(\mu_{vw})$ and F_v is the field $K(W_1 \cap W_2)$. As A/μ_w is the direct product of μ_{wm}/μ_w and C/μ_w and we have $\mu_{vw} \subset \mu_{wm}$ and $W_2 \subset C$, we see that $W_1 \cap W_2$ is K^*. It follows that $K(\mu_{vw}) \cap F_v$ is K. □

In the next section we use one more property of the field F_v. Below we will show that for all $c \in C$ with $K(c)/K$ abelian we have $c \in F_v$. To prove this we use the following result ([29], theorem 2).

Theorem 38 (Schinzel). *Let R be a field, let $n \in \mathbb{Z}_{>0}$ not divisible by $\mathrm{char}(R)$ and let u be the number of n-th roots of unity in R. Let S be the splitting field of $x^n - a$ over R for some $a \in R$. Then S/R is abelian if and only if $a^u = b^n$ for some $b \in R$.*

Proof. (cf. [35], theorem 4.1) Let a be an element of R. Suppose that $a^u = b^n$ holds for some $b \in R$. Let β be in $\bar{R}$ with $\beta^u = b$. Then we have $\beta^{un} = a^u$ and

hence $\beta^n \in a \cdot \mu_u$. It follows that S is a subfield of $R(\beta, \mu_{un})$. As $\beta^u = b \in R$ and $\mu_u \subset R$ hold, the extension $R(\beta)/R$ is cyclic. It follows that $R(\beta, \mu_{un})$ is abelian and consequently S/R is abelian.

For the converse, suppose that S/R is abelian with Galois group G. Take $\sigma \in G$ and suppose that it acts on a primitive n-th root of unity ζ_n in S as $\sigma(\zeta_n) = \zeta_n^{k_\sigma}$. If α is an element of S with $\alpha^n = a$, then for all $\tau \in G$ we have

$$\frac{\tau\sigma(\alpha)}{\sigma(\alpha)} = \sigma\left(\frac{\tau(\alpha)}{\alpha}\right) = \left(\frac{\tau(\alpha)}{\alpha}\right)^{k_\sigma} = \frac{\tau(\alpha^{k_\sigma})}{\alpha^{k_\sigma}},$$

from which we deduce that $(\alpha^{k_\sigma})/\sigma(\alpha)$ is in R as it is fixed by every $\tau \in G$. Its n-th power $a^{k_\sigma - 1}$ therefore is in R^n.

Let g denote the greatest common divisor of n and the numbers $k_\sigma - 1$ for all $\sigma \in G$. Then we have $a^g \in R^n$. If ζ is an n-th root of unity contained in S, then we have $\sigma(\zeta) = \zeta$ if and only if $\zeta^{k_\sigma - 1} = 1$ holds for all $\sigma \in G$. That is, if and only if ζ is a g-th root of unity. As the group of n-th roots of unity in R is μ_u the equality $g = u$ follows. □

Proposition 39. *Let $c \in C$. If $K(c)/K$ is abelian then c is an element of F_v.*

Proof. Let c be an element of C and assume that $K(c)/K$ is abelian. There exists a positive integer n with $n \mid m$ such that $c^n \in K^*$ holds. Denote by v_n the greatest common divisor of v and n. By theorem 38 there exists an element $b \in K^*$ with $(c^n)^{v_n} = b^n$. It follows $c^{v_n} = \zeta_n \cdot b$ for some n-th root of unity ζ_n. As we have $b \in K^*$ and $K^* \subset C$ we have $b \in C$. As also $c^{v_n} \in C$ holds, ζ_n is an element of C. We conclude that ζ_n is an element of K^* and therefore also c^{v_n} is contained in K^*. □

1.7 Determining the Galois group

Denote by D the intersection of the fields M and F_v. In this section we will prove the following theorem for K, L, m, ρ, F_v and Z as before.

Theorem 40. *The homomorphism ρ gives an isomorphism between* $\mathrm{Gal}(L/K)$ *and the subgroup H of* $\Gamma = \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right) \rtimes Z$ *defined by*

$$H = \{(f, z) \in \Gamma \text{ with } \nu_1(f) = \nu_2(z) \in \mathrm{Gal}(D/K)\},$$

where $\nu_2 \colon Z \longrightarrow \mathrm{Gal}(D/K)$ is defined by $\nu_2(z) = \omega^{-1}(z)|_D$ for all $z \in Z$ and $\nu_1 \colon \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right) \longrightarrow \mathrm{Gal}(D/K)$ is the composition of the canonical Kummer map from $\mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right)$ *to* $\mathrm{Gal}(F_v/K)$ *and the restriction map from* $\mathrm{Gal}(F_v/K)$ *to* $\mathrm{Gal}(D/K)$.

First we show that the maps ν_1 and ν_2 as defined in theorem 40 give a commuting diagram.

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\chi} & \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right) \\ \Big\downarrow{\scriptstyle \omega} & & \Big\downarrow{\scriptstyle \nu_1} \\ Z & \xrightarrow{\nu_2} & \mathrm{Gal}(D/K) \end{array}$$

Recall that χ in general is not a group homomorphism.

Proposition 41. *The map*

$$\chi' \colon \mathrm{Gal}(F_v/K) \longrightarrow \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^v)$$

defined by

$$\chi'(\sigma) = \left(a \mapsto \left(\frac{\sigma(x_n)}{x_n}\right)_{n|v}\right), \quad \textit{where } x_n \in C \textit{ with } x_n^n \cdot \mu_w = a$$

is an isomorphism of abelian groups. Moreover, if $\varphi_v \colon \hat{\mu}/\hat{\mu}^m \longrightarrow \hat{\mu}/\hat{\mu}^v$ is the projection map, then the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right) & \xleftarrow{\chi} & \mathrm{Gal}(L/K) \\ \Big\downarrow{\scriptstyle f \mapsto \varphi_v \circ f} & & \Big\downarrow{\scriptstyle res} \\ \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^v\right) & \xleftarrow{\chi'} & \mathrm{Gal}(F_v/K) \end{array}$$

Proof. From the previous section we know that $F_v \cap K(\mu_{vw})$ equals K and that L_v is $F_v(\mu_{vw})$. Hence, there is an isomorphism

$$\mathrm{Gal}\left(L_v/K(\mu_{vw})\right) \simeq \mathrm{Gal}(F_v/K)$$

given by restricting the automorphisms of $L_v/K(\mu_{vw})$ to F_v. In lemma 20 we proved for the maximal Kummer extension L_v of K that

$$\begin{aligned} \mathrm{Gal}\left(L_v/K(\mu_{vw})\right) &\simeq \mathrm{Hom}\left(K^*/\mu_{v^\infty}(K^*), \hat{\mu}/\hat{\mu}^v\right) \\ &= \mathrm{Hom}\left(K^*/\mu_w(K^*), \hat{\mu}/\hat{\mu}^v\right). \end{aligned}$$

We now define the isomorphism χ' as the composition

$$\mathrm{Gal}(F_v/K) \xrightarrow{\sim} \mathrm{Gal}\left(L_v/K(\mu_{vw})\right) \xrightarrow{\sim} \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^v).$$

Let a be an element of K^*/μ_w. We proved in lemma 34 that for every $n \mid v$ there exists a unique element $\alpha_n \in C/\mu_w$ with $\alpha_n^n = a$. We also showed that the quotient

$\sigma(x_n)/x_n$ does not depend on the choice of $x_n \in C$ with $x_n \cdot \mu_w = \alpha_n$. So, it follows from theorem 19 that the isomorphism χ' is given by

$$\chi'(\sigma) = \left(a \mapsto \left(\frac{\sigma(x_n)}{x_n} \right)_{n|v} \right), \quad \text{where } x_n \in C \text{ with } x_n^n \cdot \mu_w = a.$$

It is easy to verify that for this map χ' the diagram above commutes. □

The map ν_1 from theorem 40 is the composition of the homomorphisms in the following diagram

$$\begin{array}{ccc} \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right) & & \\ \Big\downarrow{\scriptstyle f \mapsto \varphi_v \circ f} & & \\ \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^v\right) & \xrightarrow{\chi'^{-1}} & \mathrm{Gal}(F_v/K) \\ & & \Big\downarrow{\scriptstyle \mathrm{res}} \\ & & \mathrm{Gal}(D/K). \end{array}$$

From the commuting diagram in proposition 41 we conclude that for all $\sigma \in \mathrm{Gal}(L/K)$ we have

$$\nu_1(\chi(\sigma)) = \sigma_{|D}$$

and

$$\nu_2(\omega(\sigma)) = \omega^{-1}(\omega(\sigma))_{|D} = \sigma_{|D}.$$

We get $\nu_1(\chi(\sigma)) = \nu_2(\omega(\sigma))$ for all $\sigma \in \mathrm{Gal}(L/K)$ and thus the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\chi} & \mathrm{Hom}\left(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m\right) \\ {\scriptstyle \omega}\Big\downarrow & & \Big\downarrow{\scriptstyle \nu_1} \\ Z & \xrightarrow{\nu_2} & \mathrm{Gal}(D/K) \end{array}$$

commutes.

Now we can prove theorem 40.

Proof of theorem 40. Let G be the image of $\mathrm{Gal}(L/M)$ under ρ in H. We have canonical maps $G \hookrightarrow H$ and $H \longrightarrow Z$. In lemma 32 we showed that ω induces an isomorphism of $\mathrm{Gal}(M/K)$ to Z and in section 1.5 we defined the homomorphisms χ and ρ. This gives the following commuting diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Gal}(L/M) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & 0 \\ & & {\scriptstyle \chi}\Big\downarrow{\scriptstyle \simeq} & & \Big\downarrow{\scriptstyle \rho} & & {\scriptstyle \omega}\Big\downarrow{\scriptstyle \simeq} & & \\ & & G & \xrightarrow{\gamma} & H & \xrightarrow{\vartheta} & Z & & \end{array}$$

The first row is exact because of Galois theory. The map ρ is an injective continuous homomorphism by propositions 35 and 36. The map γ is injective and because the diagram commutes and ω is an isomorphism we see that ϑ is surjective. We will prove exactness of the sequence $G \xrightarrow{\gamma} H \xrightarrow{\vartheta} Z$ in H. For all $g \in G$ we have $\vartheta(\gamma(g)) = 1$ so all there is left to prove is that for $(f,1) \in H$ we have $(f,1) \in G$.

Let $(f,1)$ be an element of H. Then we have $f \in \mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m)$ and $\nu_1(f) = \nu_2(1) = 1$. For all $n \in \mathbb{Z}_{>0}$ with $n \mid m$ we define the fields $L_n = M\big(\{\alpha \in L : \alpha^n \in K^*\}\big)$. Then, by theorem 15, we have

$$\begin{aligned}\mathrm{Gal}(L_n/M) &\simeq \mathrm{Hom}\left((K^* \cdot M^{*n})/M^{*n}, \mu_n\right)\\ &\simeq \mathrm{Hom}\left(K^*/(M^{*n} \cap K^*), \mu_n\right).\end{aligned}$$

Let $\varphi_n \colon \hat{\mu}/\hat{\mu}^m \longrightarrow \mu_n$, for all $n \in \mathbb{Z}_{>0}$ with $n \mid m$, be the projection map; we prove that $\varphi_n \circ f \in \mathrm{Hom}(K^*/(M^{*n} \cap K^*), \mu_n)$.

Let n be some positive integer and let a be an element of $K^* \cap M^{*n}$. Because K^* is contained in C^n we have $a = c^n$ for some $c \in C \cap M^*$. As c is an element of M the extension $K(c)/K$ is abelian. Moreover, as $c \in C$ we have $c \in F_v$, by proposition 39. It follows that $c \in F_v \cap M = D$. We saw that $\nu_1(f) = 1$, that is $\nu_1(f)$ acts trivial on the elements of the field D. Because c is an element of D with $c^n = a$ we have $f(a)_n = 1$. We conclude that $K^* \cap M^{*n}$ is contained in $\ker(\varphi_n \circ f)$ and thus $\varphi_n \circ f$ is an element of $\mathrm{Hom}(K^*/(M^{*n} \cap K^*), \mu_n)$.

Now, for all $n, n' \in N$ with $n \mid n'$ we get the following commuting diagram.

$$\begin{array}{ccc}\mathrm{Gal}(L_{n'}/M) & \xrightarrow{\sim} & \mathrm{Hom}(K^*/(M^{*n'} \cap K^*), \mu_{n'})\\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle g \mapsto g^{n'/n}}\\ \mathrm{Gal}(L_n/M) & \xrightarrow{\sim} & \mathrm{Hom}(K^*/(M^{*n} \cap K^*), \mu_n)\end{array}$$

The field L is the composite of the fields L_n for all positive divisors n of m and thus we have

$$G = \mathrm{Gal}(L/M) = \varprojlim_{n \mid m} \mathrm{Gal}(L_n/M).$$

For all $n \mid m$ we have $\varphi_n \circ f \in \mathrm{Hom}(K^*/(M^{*n} \cap K^*), \mu_n)$ and for all $a \in K^*/\mu_w$ we have $\big(\varphi_{n'} \circ f(a)\big)^{n'/n} = \varphi_n \circ f(a)$ for all $n, n' \in \mathbb{Z}_{>0}$ with $n \mid n'$. It follows that

$$f = (\varphi_n \circ f)_{n \mid m} \in \varprojlim_{n} \mathrm{Hom}(K^*/(M^{*n} \cap K^*), \mu_n).$$

Hence $(f,1)$ is an element of G.

We have a commuting diagram consisting of two exact sequences. As the homomorphisms $\mathrm{Gal}(L/M) \longrightarrow G$ and $\mathrm{Gal}(M/K) \longrightarrow Z$ are isomorphisms, the injection ρ also has to be an isomorphism. The group $\mathrm{Gal}(L/K)$ is compact because it is a profinite group and as H is Hausdorff the continuous isomorphism ρ is a homeomorphism and thus $\mathrm{Gal}(L/K)$ and H are isomorphic as topological groups. □

We will use this theorem to give an explicit description of $\mathrm{Gal}(L/K)$ in the case that K equals $\mathbb{Q}$ and m is $\prod_{p\in P} p^\infty$.

Lemma 42. *Let a be a positive integer and let n be an element of $\hat{\mathbb{Z}}^*$. Then there exist positive integers n_i with $\gcd(n_i, 2a) = 1$ for all $i \in \mathbb{Z}_{>0}$ such that $\lim_{i\to\infty} n_i$ equals n in $\hat{\mathbb{Z}}$.*

Proof. Let π^*, for all $k \in \mathbb{Z}_{>0}$, be the projection from $\hat{\mathbb{Z}}^*$ to $(\mathbb{Z}/k\mathbb{Z})^*$. Now define n_i for every $i \in \mathbb{Z}_{>0}$ as the integer obtained by lifting $\pi^*_{2a(i!)}$ to $\mathbb{Z}$. Then for all $i \in \mathbb{Z}_{>0}$ we have $\gcd(n_i, 2a) = 1$ and n equals $\lim_{i\to\infty} n_i$. □

Definition 43. Let p be a prime and let a be an integer. We denote the *Legendre symbol* of a and p by $\left(\frac{a}{p}\right)$.

For a positive odd integer b and an integer a with $\gcd(a, b) = 1$ the *Jacobi symbol* is defined as

$$\left(\frac{a}{b}\right) = \prod_{p|b} \left(\frac{a}{p}\right)^{v_p(b)},$$

where for a prime p and an integer b we denote by $v_p(b)$ the p-valuation of b.

Now let a be an element of $\mathbb{Q}^*$ and let n be an element of $\hat{\mathbb{Z}}^*$. Write $a = b/c$ for $b, c \in \mathbb{Z}\backslash\{0\}$ and write $n = \lim_{i\to\infty} n_i$ for a sequence $(n_i)_{i=0}^\infty$ of positive integers n_i for which $\gcd(n_i, 2bc) = 1$ for all $i > 0$. We define the *Jacobi symbol*

$$\left(\frac{a}{n}\right) = \lim_{i\to\infty} \left(\frac{b}{n_i}\right) \Big/ \left(\frac{c}{n_i}\right),$$

where $\left(\frac{b}{n_i}\right)$ and $\left(\frac{c}{n_i}\right)$ are the ordinary Jacobi symbols. Below we show that this is well-defined. Let a, b, c, n, n_i be as above and let p be an odd prime number. Then we have by quadratic reciprocity

$$\left(\frac{p}{n_i}\right) = \begin{cases} \left(\frac{n_i}{p}\right) & \text{if } p \equiv 1 \bmod 4 \\ \left(\frac{n_i}{p}\right) \cdot (-1)^{\frac{n_i-1}{2}} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

By the supplementary laws we have $\left(\frac{-1}{n_i}\right) = (-1)^{\frac{n_i-1}{2}}$ and $\left(\frac{2}{n_i}\right) = (-1)^{\frac{n_i^2-1}{8}}$. As $\left(\frac{n_i}{p}\right)$, $(-1)^{\frac{n_i-1}{2}}$ and $(-1)^{\frac{n_i^2-1}{8}}$ stabilise for large i the limits

$$\left(\frac{-1}{n}\right) = \lim_{i\to\infty} \left(\frac{-1}{n_i}\right) \quad \text{and} \quad \left(\frac{p}{n}\right) = \lim_{i\to\infty} \left(\frac{p}{n_i}\right), \text{ for } p \text{ prime},$$

exist and do not depend on the choice of the n_i. By multiplicativity this gives $\left(\frac{a}{n}\right)$.

Example 44. Let us return to the case where $K = \mathbb{Q}$ and $m = \prod_{p \in P} p^{\infty}$. We choose C as in example 33.

Remark that $\hat{\mu}/\hat{\mu}^2 \simeq \mu_2$. We have $w = 2$ and also $v = 2$. The field L_v is $\mathbb{Q}(\{\alpha \in \mathbb{C} \text{ with } \alpha^2 \in \mathbb{Q}\})$ and the field $K(\mu_{vw})$ is $\mathbb{Q}(i)$. The fields F_v and D are equal:

$$F_v = D = \mathbb{Q}(\{\alpha \in \mathbb{C} \text{ with } \alpha^2 \in \mathbb{Q}_{>0}\}).$$

Let, as before, $\varphi_2 \colon \hat{\mu}/\hat{\mu}^m = \hat{\mu} \longrightarrow \mu_2$ be the projection map. Then the isomorphism $\nu_1 \colon \mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu}) \longrightarrow \mathrm{Gal}(D/\mathbb{Q})$ satisfies

$$\nu_1(f)(\sqrt{a}\,) = \varphi_2(f(a)) \cdot \sqrt{a} \quad \text{for all } f \in \mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu}) \text{ and all } a \in \mathbb{Q}_{>0}.$$

Let p be an odd prime. Notice that $\mathbb{Q}(\sqrt{p^*}\,)$, with $p^* = (-1)^{(p-1)/2}p$, is the unique subfield of degree 2 of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. If σ is an element of $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ and we have $\sigma(\zeta_p) = \zeta_p^e$ for some $e \in \{1, 2, \ldots, p-1\}$ then

$$\sigma(\sqrt{p^*}\,) = \begin{cases} \sqrt{p^*} = \left(\frac{e}{p}\right)\sqrt{p^*} & \text{if } e \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^* \\ -\sqrt{p^*} = \left(\frac{e}{p}\right)\sqrt{p^*} & \text{if } e \text{ is not a square in } (\mathbb{Z}/p\mathbb{Z})^*. \end{cases}$$

Moreover, if σ' is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ and we have $\sigma'(\zeta_8) = \zeta_8^f$ for some $f \in \{1, 3, 5, 7\}$ then

$$\sigma'(\sqrt{-1}\,) = (-1)^{\frac{f-1}{2}}\sqrt{-1} \quad \text{and} \quad \sigma'(\sqrt{2}\,) = (-1)^{\frac{f^2-1}{8}}\sqrt{2}.$$

Let a be an element of $\mathbb{Z}_{>0}$ with prime factorisation

$$a = 2^{v_2(a)} \cdot \prod_{p \equiv 1 \bmod 4} p^{v_p(a)} \cdot \prod_{q \equiv 3 \bmod 4} q^{v_q(a)}$$

Then we have

$$\sqrt{a} = \sqrt{2}^{v_2(a)} \cdot \prod_{p \equiv 1 \bmod 4} \sqrt{p}^{v_p(a)} \cdot \prod_{q \equiv 3 \bmod 4} \sqrt{-q}^{v_q(a)} \cdot \sqrt{-1}^{x},$$

with $x = 0$ if $2 \mid \sum_q v_q(a)$ and $x = 1$ if $2 \nmid \sum_q v_q(a)$. The homomorphism $\nu_2 \colon Z \longrightarrow \mathrm{Gal}(D/K)$ maps $z \in Z$ to the restriction of $\omega^{-1}(z) \in \mathrm{Gal}(M/K)$ to $\mathrm{Gal}(D/K)$.

Hence we have, for all $z \in Z$,

$$\begin{aligned}
\nu_2(z)(\sqrt{a}) &= \nu_2(z)\left(\sqrt{2}^{v_2(a)} \cdot \prod_{p\equiv 1 \bmod 4} \sqrt{p}^{v_p(a)} \cdot \prod_{q\equiv 3 \bmod 4} \sqrt{-q}^{v_q(a)} \cdot \sqrt{-1}^{x}\right) \\
&= \left((-1)^{\frac{z^2-1}{8}}\sqrt{2}\right)^{v_2(a)} \cdot \prod_p \left(\left(\frac{z}{p}\right)\sqrt{p}\right)^{v_p(a)} \cdot \prod_q \left(\left(\frac{z}{q}\right)\sqrt{-q}\right)^{v_q(a)} \\
&\quad \cdot \left((-1)^{\frac{z-1}{2}} \cdot \sqrt{-1}\right)^{x} \\
&= \left(\frac{2}{z}\right)^{v_2(a)} \cdot \prod_p \left(\frac{p}{z}\right)^{v_p(a)} \cdot \prod_q \left(\left(\frac{q}{z}\right)\cdot(-1)^{\frac{z-1}{2}}\right)^{v_q(a)} \cdot (-1)^{\frac{z-1}{2}\cdot x} \cdot \sqrt{a} \\
&= \left(\frac{a}{z}\right)\cdot(-1)^{\frac{z-1}{2}\left(\sum_q v_q(a)+x\right)} \cdot \sqrt{a} \\
&= \left(\frac{a}{z}\right)\cdot\sqrt{a}.
\end{aligned}$$

Now let $a \in \mathbb{Q}_{>0}$ with $a = b/c$ for $b, c \in \mathbb{Z}\setminus\{0\}$. Then $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{bc})$ and $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)\left(\frac{c}{n}\right) = \left(\frac{bc}{n}\right)$, therefore $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the group

$$\left\{(f,z) \in \mathrm{Hom}(\mathbb{Q}_{>0}, \hat{\mu}) \rtimes \hat{\mathbb{Z}}^* \text{ with } \varphi_2\big(f(a)\big) = \left(\frac{a}{z}\right) \text{ for all } a \in \mathbb{Q}_{>0}\right\}.$$

1.8 Computing the field D

In this section we will show that the field $D = M \cap F_v$ equals the intersection $M \cap F$. Moreover we give a method to compute the field D in some specific cases. At the end of the section we provide some examples.

Proposition 45. *The intersection $M \cap F$ is the field D.*

Proof. As $D = M \cap F_v$ and $F_v \subset F$ we have that $D \subset M \cap F$. Now let $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma_{|_D} = 1$. We prove that also $\sigma_{|_{M\cap F}} = 1$. We have

$$\nu_1\big(\chi(\sigma)\big) = \sigma_{|_D} = 1_{|_D} = \nu_2\big(\omega(1)\big)$$

and hence $\big(\chi(\sigma), \omega(1)\big) \in H$. So, by theorem 40 there is an automorphism $\tau \in \mathrm{Gal}(L/K)$ such that

$$\rho(\tau) = \big(\chi(\tau), \omega(\tau)\big) = \big(\chi(\sigma), \omega(1)\big).$$

It follows $\chi(\sigma) = \chi(\tau)$ and therefore we have $\sigma(c) = \tau(c)$ for all $c \in C$. We conclude $\sigma_{|_F} = \tau_{|_F}$. The equality $\omega(\tau) = \omega(1)$ implies that $\tau_{|_M} = 1$ holds. So, we have

$$\sigma_{|_{M\cap F}} = \tau_{|_{M\cap F}} = 1_{|_{M\cap F}} = 1.$$

Hence $M \cap F$ is contained in D. ∎

We introduce some more notation.

Definition 46. Let p be a prime and let s be a Steinitz number. By K_p we denote the field $K(\mu_{p^\infty}(\bar{K}))$ and by $K_{p,s}$ we denote the maximal abelian subextension of K_p/K of exponent s.

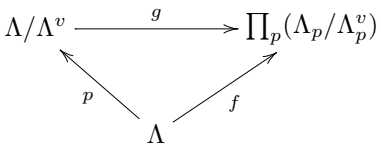
Note that if $\mathrm{char}(K) = p$ we get $K_p = K$.

Lemma 47. *Let Λ be the group $\mathrm{Gal}(M/K)$ and let Λ_p denote the Galois group $\mathrm{Gal}((M \cap K_p)/K)$, for all primes p dividing m. If the natural map*

$$g\colon \Lambda/\Lambda^v \longrightarrow \prod_{p|m} (\Lambda_p/\Lambda_p^v)$$

is injective, then the maximal abelian subextension of exponent v of M/K is the composite of the fields $M \cap K_{p,v}$.

Proof. Consider the following commuting diagram.



As we have $\Lambda_p = \mathrm{Gal}((M \cap K_p)/K)$ it follows $\mathrm{Gal}((M \cap K_{p,v})/K) = \Lambda_p/\Lambda_p^v$. Define for all primes p the map $f_p\colon \Lambda \longrightarrow \Lambda_p/\Lambda_p^v$. Then we have $M^{\ker(f_p)} = M \cap K_{p,v}$. If g is injective then $\ker(f) = \ker(p) = \Lambda^v$. The field M^{Λ^v} is the maximal abelian subextension of exponent v in M/K. □

As we will see in example 49 it is not true in general that the maximal abelian subextension of exponent v of M/K is the composite of the fields $M \cap K_{p,v}$. But if this holds, then lemma 47 gives us a method to compute the field D.

Theorem 48. *If the maximal abelian subextension of exponent v of M/K is the composite of the fields $M \cap K_{p,v}$, then the field D is the composite of the fields $\big(M \cap K_p(\mu_{vw})\big) \cap F_v$ for the primes $p \mid m$.*

Proof. We introduce two fields. Let D' be the composite of the fields $\big(M \cap K_p(\mu_{vw})\big) \cap F_v$ for all primes $p \mid m$ and let E be the composite of the fields $M \cap K_{p,v}$ for all primes $p \mid m$.

By lemma 47 we have

$$D' \subset D \subset E.$$

To prove that $D = D'$ we first show that $D(\mu_{vw}) = D'(\mu_{vw})$.

In section 1.6 we saw that the maximal Kummer extension of exponent v over K, the field L_v, is the composite of F_v and $K(\mu_{vw})$. The groups of radicals of exponent v over K, generating the fields L_v, F_v and $K(\mu_{vw})$, are

$$A_v = \{a \in A \text{ with } c^n \in K^* \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid v\},$$

$$C_v = \{c \in C \text{ with } c^n \in K^* \text{ for some } n \in \mathbb{Z}_{>0} \text{ with } n \mid v\}$$

and μ_{vw}. We have $A_v = \langle C_v, \mu_{vw} \rangle$.

Let p be a prime dividing m. The field $M \cap K_{p,v}(\mu_{vw})$ is contained in L_v, hence there exists a subgroup T of A_v such that $M \cap K_{p,v}(\mu_{vw}) = K(T)$. As T is a subgroup of $\langle C_v, \mu_{vw} \rangle$ and as μ_{vw} is contained in T we have

$$(T \cap C_v) \cdot \mu_{vw} = T.$$

Therefore, by proposition 17, also the following equality of fields holds

$$\big(K(T) \cap F_v\big)(\mu_{vw}) = K(T). \tag{1.1}$$

As $K_p(\mu_{vw}) \cap F_v$ is a field of exponent v over K we have, by corollary 18, $A_v \cap K_p(\mu_v w) \subset K_{p,v}(\mu_{vw})$. It follows

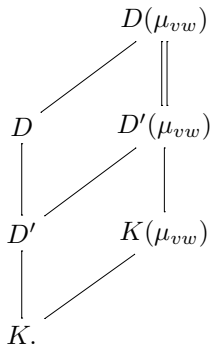
$$K_p(\mu_{vw}) \cap F_v = K_{p,v}(\mu_{vw}) \cap F_v. \tag{1.2}$$

As $K(T)$ equals $M \cap K_{p,v}(\mu_{vw})$ we can substitute equation 1.2 in the left hand side of equation 1.1. We obtain

$$\big((M \cap K_p(\mu_{vw})) \cap F_v\big)(\mu_{vw}) = M \cap K_{p,v}(\mu_{vw}).$$

Taking the composite over all primes p dividing m gives $D'(\mu_{vw}) = E(\mu_{vw})$. As we have $D' \subset D \subset E$ we derive that $D(\mu_{vw}) = D'(\mu_{vw})$.

Now look at the following diagram:

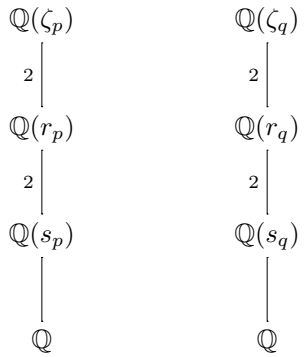


All the extensions are Galois extensions and by theorem 37 we know that the intersection $D \cap K(\mu_{vw})$ equals K. We conclude that

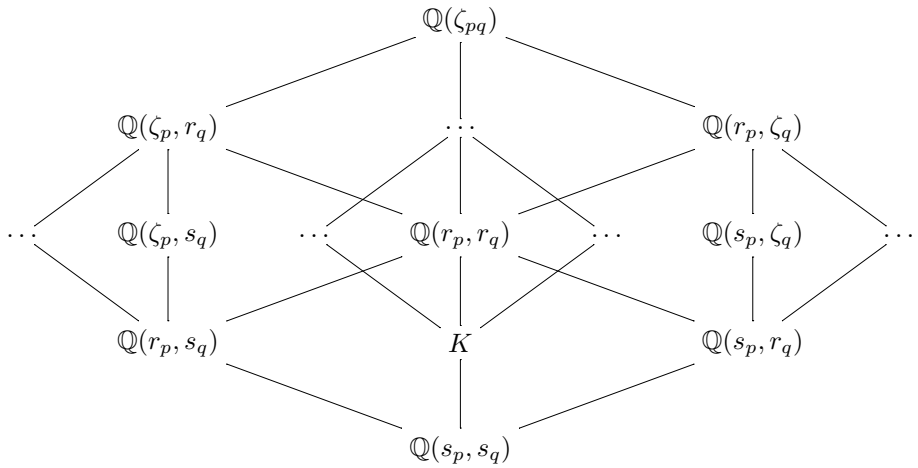
$$\mathrm{Gal}(D(\mu_{vw})/D) \simeq \mathrm{Gal}(K(\mu_{vw})/K) \simeq \mathrm{Gal}(D'(\mu_{vw})/D'),$$

hence we have $D = D'$. □

Example 49. Let p and q be distinct primes congruent to 1 modulo 4. Let m be $2pq$. We construct a field K for which the composite of the fields $K_{p,2}$ and $K_{q,2}$ is smaller than the maximal Kummer extension of exponent 2 over K in the field $M = K(\mu_{pq})$. Define elements r_p, s_p in $\mathbb{Q}(\zeta_p)$ and elements r_q, s_q in $\mathbb{Q}(\zeta_q)$ that generate subfields of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$ as indicated in the following diagrams.



As $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(s_p, s_q)$ is a Galois extension with Galois group $C_4 \times C_4$ we have the following diagram of subfields.



Let K be the quadratic subextension of $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(s_p, s_q)$ that is not equal to $\mathbb{Q}(r_p, s_q)$ or $\mathbb{Q}(s_p, r_q)$. The maximal Kummer extension of exponent 2 in $K(\zeta_{pq})/K$ is a degree 4 extension. However, the extension $K_{p,2} = K_{q,2} = \mathbb{Q}(r_p, r_q)$ is of degree 2 over K.

Below we compute the intersection field D in some special cases. We start with our standard example.

Example 50. Let, as before, $K = \mathbb{Q}$, $m = \prod_{p\in P} p^\infty$, and let F be the field generated by the real radicals in $\mathbb{C}$. In this case we have $v = 2$. As the Galois group of $\mathbb{Q}(\mu(\mathbb{C}))$ over $\mathbb{Q}$ is isomorphic to $\hat{\mathbb{Z}}^*$ which is the direct product of the $\mathbb{Z}_p^*$ for all primes p we can apply theorem 48.

Let p be an odd prime. Then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is cyclic of degree $p-1$ and the unique subfield of degree 2 of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{\pm p})$. As $vw = 4$ we have $K_p(\mu_{vw}) \cap F_v = \mathbb{Q}(\sqrt{p})$. Moreover, we have $K_2(\mu_{vw}) \cap F_v = K_2 \cap F_v = \mathbb{Q}(\sqrt{2})$. It follows that

$$D = \mathbb{Q}(\sqrt{p} \colon p \in P).$$

In the case that $K = \mathbb{Q}$ and $m = \prod_{p\in P} p^\infty$ we could also have made other choices for the subgroup C in the splitting of A (section 1.5) resulting in a non-real field F. Also in these cases it is easy to compute the field D. For every prime p precisely one of the elements $\sqrt{p}$ and $\sqrt{-p}$ is contained in F_v. When we denote this element by $\bar{p}$ then we have $D = \mathbb{Q}(\bar{p} : p \in P)$.

Example 51. Let $K = \mathbb{Q}(\sqrt{2})$ and $m = \prod_{p\in P} p^\infty$. The Galois group of $\mathbb{Q}(\mu(\mathbb{C}))$ over $\mathbb{Q}(\sqrt{2})$ is the direct product of the groups $\mathbb{Z}_p^*$ for odd primes p with

$$\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}(\sqrt{2})) \subset \mathbb{Z}_2^*.$$

Again we apply theorem 48.

As in example 50 we have $v = 2$ and for all odd primes the intersection $K_p(\mu_{vw}) \cap F_v$ equals $\mathbb{Q}(\bar{p})$, where $\bar{p} \in \{\sqrt{p}, \sqrt{-p}\}$ depending on the choice for C.

Again we have $K_2(\mu_{vw}) = K_2$. For the intersection $K_2 \cap F_v$ there are only few possibilities. The only extensions over $\mathbb{Q}(\sqrt{2})$ of exponent 2 in K_2 are $\mathbb{Q}(\zeta_8) \not\subset F_v$, $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ and $\mathbb{Q}(\zeta_{16} - \zeta_{16}^{-1})$. The following equalities hold:

$$\left(\zeta_{16} + \zeta_{16}^{-1}\right)^2 = 2 + \sqrt{2} \qquad \text{and} \qquad \left(\zeta_{16} - \zeta_{16}^{-1}\right)^2 = -2 + \sqrt{2}.$$

Moreover we have $(2+\sqrt{2})(-2+\sqrt{2}) \cdot \mu_w = -2 \cdot \mu_w$. By lemma 34 there is a unique square root of $(2+\sqrt{2}) \cdot \mu_w$ in C/μ_w. As we have $\sqrt{2} \in C$ and $i \notin F_v$ precisely one of the elements $\zeta_{16} + \zeta_{16}^{-1}$ and $\zeta_{16} - \zeta_{16}^{-1}$ is contained in F_v.

Example 52. Let K be a real number field and let m be a Steinitz number coprime to 2. Then v equals 1. Consequently, we have $F_v = K = D$.

Example 53. Let K be $\bar{\mathbb{Q}} \cap \mathbb{R}$ and let m be 2. Then $L = M = K(i)$ and the field F equals the ground field K. All square roots of the elements of $K_{\geq 0}$ are contained in K and the product of this group and the group generated by i gives all square roots of elements of K.

Example 54. If L/K is a Kummer extension of exponent m for some Steinitz number m, then we have $v = \gcd(m, w) = m$. As the field M equals $K(\mu_{wm})$ we

have $M = K(\mu_{vw})$. In section 1.6 we showed that $K(\mu_{vw}) \cap F_v = K$, so in this case we have $D = M \cap F_v = K$.

Moreover we have $L = MF = MF_v$ and thus $\mathrm{Gal}(L/K)$ is the direct product of $\mathrm{Hom}(K^*/\mu_w, \hat{\mu}/\hat{\mu}^m) \simeq \mathrm{Gal}(F_v/K)$ and $Z \simeq \mathrm{Gal}(M/K)$. As M/K is a Kummer extension, the group Z is isomorphic to $\mathrm{Hom}(\mu_w, \hat{\mu}/\hat{\mu}^m)$. We derive the result of theorem 19 again: $\mathrm{Gal}(L/K) \simeq \mathrm{Hom}(K^*, \hat{\mu}/\hat{\mu}^m)$.

Chapter 2

Subfields of radical extensions

In the main theorem in the previous chapter we computed the Galois group of a large field generated by radicals. When we are able to compute all subgroups of this Galois group we know all subfields of the extension. As we will see in chapters 4 and 5, it is useful to know the subfields of a field generated by radicals in order to denest radicals. In this chapter we study the subfields of the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, where α is an element of $\mathbb{C}$ with $\alpha^n \in \mathbb{Q}$ for some positive integer n.

Definition 55. Let L/K be a field extension. A group C is called a *radical group for* L/K if $K^* \subset C \subset L^*$, if $L = K(C)$ and if there exists a positive integer n with $C^n \subset K^*$.

The extension L/K is called a *radical extension of exponent* n if there exists a radical group C for L/K with $C^n \subset K^*$.

Let L/K be a radical extension of exponent n with radical group C. If K contains a primitive n-th root of unity then L/K is a Kummer extension of exponent n, the map

$$\psi\colon \{\text{subgroups of } C \text{ containing } K^*\} \longrightarrow \{\text{subfields of } L \text{ containing } K\}$$

given by $\psi(C') = K(C')$ is a bijection, and, if L/K is finite, we have $\#(C/K^*) = [L : K]$. Under special conditions such a correspondence also holds for other radical extensions.

In this chapter we determine for which radicals α the map

$$\psi_\alpha\colon \{\text{subgroups of } \langle \mathbb{Q}^*, \alpha\rangle \text{ containing } \mathbb{Q}^*\} \longrightarrow \{\text{subfields of } \mathbb{Q}(\alpha)\}$$

given by $\psi_\alpha(C) = \mathbb{Q}(C)$ is surjective. This results in the following theorem. By $\mu_n = \mu_n(\mathbb{C})$ we denote, as in definition 8, the group of n-th roots of unity in $\mathbb{C}$.

Theorem 56. *Let $\alpha \in \mathbb{C}$ be a radical over $\mathbb{Q}$ with $n \in \mathbb{Z}_{>0}$ minimal such that $\alpha^n \in \mathbb{Q}$. Let D_α be the subgroup $\langle \mathbb{Q}^*, \alpha\rangle$ of $\mathbb{C}^*$. Every subfield of $\mathbb{Q}(\alpha)$ is of the form*

$\mathbb{Q}(\alpha^d)$ for some positive integer $d \mid n$ if and only if one of the following conditions holds:

(i) *$D_\alpha \cap \mu_n \subset \mu_2$ and we have $6 \nmid n$ or $\sqrt{-3} \notin D_\alpha$,*

(ii) *$D_\alpha \cap \mu_n = \mu_3$,*

(iii) *$D_\alpha \cap \mu_n = \mu_4$ and $1 + i \in D_\alpha$,*

(iv) *$D_\alpha \cap \mu_n = \mu_6$ and $\sqrt{-3} \in D_\alpha$,*

(v) *$D_\alpha \cap \mu_n = \mu_{10}$ and both $4 \nmid n$ and $\sqrt{5} \in D_\alpha$.*

In section 2.1 we give the context of the results in this chapter. We state some known results for generalising Kummer theory to radical extensions over fields that do not contain the appropriate roots of unity. The proof of theorem 56 comprises the rest of the chapter.

In section 2.2 we show the first implication: if every subfield of $\mathbb{Q}(\alpha)$ is generated by a power of α then α has to satisfy one of the conditions (i), (ii), (iii), (iv) or (v). In section 2.3 we embed the Galois group of $\mathbb{Q}(\zeta_n, \alpha)$ over $\mathbb{Q}$ in $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$. We use the intersection field $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ to give an explicit description of the image G of $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q})$ in $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$. In sections 2.4 and 2.5 we show, for the radicals α satisfying one of the five conditions of theorem 56, that all subgroups of the group G are of the form $G \cap \left(d\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*\right)$ for some divisor d of n. These subgroups correspond to the fields $\mathbb{Q}(\alpha^{n/d})$. This will finish the proof of theorem 56.

As a corollary we prove the following theorem at the end of section 2.5.

Theorem 57. *Let $\alpha \in \mathbb{C}$ be a radical over $\mathbb{Q}$ with $n \in \mathbb{Z}_{>0}$ minimal such that $\alpha^n \in \mathbb{Q}$. Let D_α be the group $\langle \mathbb{Q}^*, \alpha \rangle$. The map ψ_α is bijective if and only if one of the following properties holds:*

(i) *$D_\alpha \cap \mu_n \subset \mu_2$ and we have $6 \nmid n$ or $\sqrt{-3} \notin D_\alpha$,*

(ii) *$D_\alpha \cap \mu_n = \mu_3$.*

In this chapter we fix the following notation. Always $\alpha \in \mathbb{C}$ will denote a radical over $\mathbb{Q}$ and n will be the smallest positive integer for which α^n is contained in $\mathbb{Q}$. By D_α we denote the multiplicative group $\langle \mathbb{Q}^*, \alpha \rangle \subset \mathbb{C}^*$.

If m is a natural number then we denote a primitive m-th root of unity in $\mathbb{C}$ by ζ_m, the group $\langle \zeta_m \rangle$ we denote by μ_m and the number $\varphi(m)$ is the Euler totient of m.

2.1 Known results

The first results in finding non-Kummer radical extensions for which the map ψ from the introduction is a bijection impose conditions on the group C to ensure

that the group index and the degree of the field extension are equal. In [16] Kneser generalised results of Besicovitch [3], Mordell [25] and Siegel [33]. He proved the following theorem.

Theorem 58. *Let K be a field of characteristic 0. Let L/K be a radical extension of exponent n with radical group C. If L/K is a finite extension then the degree $[L : K]$ equals the index $(C : K^*)$ if and only if R_1 and R_2 hold:*

R_1: for all odd primes p: if $\zeta_p \in C$ then $\zeta_p \in K$,

R_2: if $1 + i \in C$ then $i \in K$.

We prove one implication: the conditions R_1 and R_2 are necessary.
Assume that $[L : K] = (C : K^*)$ holds. For every element c of C we have

$$[K(c) : K] \quad \leq \quad (\langle K^*, c\rangle : K^*). \tag{2.1}$$

As $[L : K]$ is equal to $[L : K(c)][K(c) : K]$ and $(C : K^*)$ equals the product $(C : \langle K^*, c\rangle)(\langle K^*, c\rangle : K^*)$ it follows from $[L : K] = (C : K^*)$ that equality holds in 2.1. Let p be an odd prime with $\zeta_p \in C$. Then, in particular we have $[K(\zeta_p) : K] = (\langle K^*, \zeta_p\rangle : K^*)$. As the degree $[K(\zeta_p) : K]$ divides $p - 1$ and the group index $(\langle K^*, \zeta_p\rangle : K^*)$ is 1 or p it follows that ζ_p is an element of K. The same argument works if $1 + i \in C$: the field $K(1 + i) = K(i)$ is of degree 2 over K if we have $i \notin K$; in this case the group index $(\langle K^*, 1 + i\rangle : K^*)$ is 4, so i must be an element of K.

Whether or not the conditions R_1 and R_2 from theorem 58 are satisfied does not only depend on the extension L/K but also on the choice for the radical group C.

Example 59. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_8)$. If we take $C = \langle \mathbb{Q}^*, \zeta_8\rangle$, then C satisfies the conditions R_1 and R_2 from theorem 58 and we have $4 = [L : K] = (C : K^*)$. But, if we take $C = \langle \mathbb{Q}^*, \zeta_8, \sqrt{2}\rangle$ then $(C : K^*) = 8 \neq [L : K]$. And indeed, in this case $\zeta_8 \cdot \sqrt{2} = 1 + i$ is an element of C and as i is not contained in $\mathbb{Q}$ this group does not satisfy R_2.

Given a radical extension L/K it also depends on the choice for the radical group C whether or not the map ψ is bijective as we see in the following example.

Example 60. Take $K = \mathbb{Q}$ and let $\alpha \in \mathbb{C}$ be an element with $\alpha^4 = -9$. Define $L = \mathbb{Q}(\alpha)$. When we take $C = \langle \mathbb{Q}^*, \alpha\rangle$, then the conditions R_1 and R_2 hold and the degree of the extension L/K equals the group index $(C : K^*)$. But, as L equals $\mathbb{Q}(i, \sqrt{6}\,)$ and C/K^* is a cyclic group, the map ψ is not a bijection.
If we take $C = \langle \mathbb{Q}^*, i, \sqrt{6}\rangle$, then again C satisfies the conditions in Kneser's theorem. However, in this case the map ψ is a bijection.

The previous example also shows that conditions R_1 and R_2 from theorem 58 are not sufficient for ψ to be a bijection.

In [11] Greither and Harrison introduce the notion of cogalois theory. Given a radical extension L/K they fix a choice for the radical group C. They give a condition on the extension L/K for the map ψ to be a bijection. This condition implies that every radical group for L/K satisfies R_1 and R_2.

Definition 61. A field extension L/K is called *pure* if the following holds: if $p = 4$ or p is prime then every element $\zeta \in L$ satisfying $\zeta^p = 1$ is contained in K.

Let L/K be a field extension and let C be a subgroup of L^*/K^*, then we denote by $K(C)$ the subextension of L/K generated by all $b \in L$ with $b \cdot K^*$ in C.

Proposition 62 (Greither and Harrison). *Let K be a field of characteristic 0 and let L/K be a pure radical extension. Then the maps*

$$\psi\colon \{\textit{subgroups of } (L^*/K^*)_{\mathrm{tors}}\} \longrightarrow \{\textit{subfields of } L \textit{ containing } K\},$$

defined by $\psi(C/K^*) = K(C)$ and

$$\varphi\colon \{\textit{subfields of } L \textit{ containing } K\} \longrightarrow \{\textit{subgroups of } (L^*/K^*)_{\mathrm{tors}}\},$$

defined by $\varphi(M) = (M^*/K^*)_{\mathrm{tors}}$ are bijections that are inverse to each other.

Corollary 63. *Let $\alpha_1, \ldots, \alpha_t$ be real numbers for which there exist positive integers $n_1, \ldots, n_t$ with $\alpha_i^{n_i} \in \mathbb{Q}$ for all i. Define L as the subfield $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ of $\mathbb{R}$. Then every subfield of L is generated by monomials in the radicals α_i.*

Proof. As L is a real field the extension $L/\mathbb{Q}$ is pure and we can apply proposition 62. The map ψ is a bijection, hence every subfield of L is generated by a subgroup C of the multiplicative group $\langle \mathbb{Q}^*, \alpha_1, \ldots, \alpha_t \rangle$ with $\mathbb{Q}^* \subset C$. □

In [18] Halter-Koch reformulates the problem. He remarks that for certain radicals α there exist subfields of $\mathbb{Q}(\alpha)$ that are conjugate to a field of the form $\mathbb{Q}(\alpha^d)$ but that are not generated by a power of α, see example 65. Therefore he defines a new map ψ' mapping subgroups of the radical group C of L/K to classes of conjugate subfields of L/K. He gives sufficient conditions on C for ψ' to be a bijection.

Theorem 64. *Let K be a field of characteristic 0 and let L/K be a radical extension of exponent $n \in \mathbb{Z}_{>0}$ with radical group C. If the degree of the extension $[L : K]$ equals the index $(C : K^*)$ and if C satisfies the condition*

R_3*: If $4 \mid n$, $i \in L$, $y \in L$ and $(1 + i)y \in C$, then $i \in K(y)$ or $i \in K(iy)$,*

then every subfield K' of L containing K is conjugate to a field of the form $K(C')$ for some subgroup C' of C containing K^*.

Example 65. Let α be an element of $\mathbb{C}$ with $\alpha^6 = -3$. One easily checks that the group $C = \langle \mathbb{Q}^*, \alpha \rangle$ satisfies the conditions R_1, R_2 and R_3.

In the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ there are subextensions, like $\mathbb{Q}(\zeta_3 \cdot \alpha^2)$, that are not generated by a subgroup C' of C, but all subfields of $\mathbb{Q}(\alpha)$ are conjugate to a field $\mathbb{Q}(C')$ for such a subgroup C'. Namely, if we fix the notation $\sqrt[3]{-3} = \alpha^2$, then the subfields of $\mathbb{Q}(\alpha)$ are

$$\mathbb{Q}, \quad \mathbb{Q}(\sqrt{-3}\,), \quad \mathbb{Q}(\sqrt[3]{-3}\,), \quad \mathbb{Q}(\zeta_3 \cdot \sqrt[3]{-3}\,), \quad \mathbb{Q}(\zeta_3^2 \cdot \sqrt[3]{-3}\,) \quad \text{and} \quad \mathbb{Q}(\alpha).$$

These are all conjugate to $\mathbb{Q}$, $\mathbb{Q}(\alpha^3)$, $\mathbb{Q}(\alpha^2)$ or $\mathbb{Q}(\alpha)$.

We give an example that shows that condition R_3 in theorem 64 is not necessary.

Example 66 ([18]). Let K be $\mathbb{Q}(\sqrt{-2}\,)$ and let α be an element of $\mathbb{R}$ with $\alpha^8 = 5$. If we take $L = \mathbb{Q}(\zeta_8, \alpha)$ and we let C be $\langle K^*, i, \alpha \rangle$, then all subfields of L are conjugate to a field generated by a subgroup of C, although the group C does not satisfy condition R_3: let y be $(1+i) \cdot \alpha^2$, then we have $(1+i)y = 2i \cdot \alpha^2 \in C$, but i is an element of neither $K(y)$ nor $K(iy)$.

2.2 First implication

In this section we prove proposition 67, which gives one implication of theorem 56. Recall that $\alpha \in \mathbb{C}$ is a radical over $\mathbb{Q}$ with $n \in \mathbb{Z}_{>0}$ minimal such that $\alpha^n \in \mathbb{Q}$ and that D_α is the subgroup $\langle \mathbb{Q}^*, \alpha \rangle$ of $\mathbb{C}^*$.

Proposition 67. *If every subfield of $\mathbb{Q}(\alpha)$ is of the form $\mathbb{Q}(\alpha^d)$ for some positive integer $d \mid n$ then one of the following conditions holds:*

(i) *$D_\alpha \cap \mu_n \subset \mu_2$ and we have $6 \nmid n$ or $\sqrt{-3} \notin D_\alpha$,*

(ii) *$D_\alpha \cap \mu_n = \mu_3$,*

(iii) *$D_\alpha \cap \mu_n = \mu_4$ and $1 + i \in D_\alpha$,*

(iv) *$D_\alpha \cap \mu_n = \mu_6$ and $\sqrt{-3} \in D_\alpha$,*

(v) *$D_\alpha \cap \mu_n = \mu_{10}$ and both $4 \nmid n$ and $\sqrt{5} \in D_\alpha$.*

First we give two lemmas.

Lemma 68. *Let K be a field and let a be an element of K. Let f be the polynomial $x^m - a \in K[x]$ for some integer $m \geq 2$. Then f is reducible over K if and only if at least one of the following two properties holds.*

- *There exist a divisor $d > 1$ of m and an element b in K such that $a = b^d$.*
- *We have $4 \mid m$ and there exists an element $c \in K$ such that $a = -4c^4$.*

Proof. This is [22] Chapter VI, section 9, page 297, theorem 9.1. □

Lemma 69. *Let d be a divisor of n. If $\mathbb{Q}(\alpha^{n/d})/\mathbb{Q}$ is an abelian extension then we have $\mu_d \cdot \mathbb{Q}^* = \langle \mathbb{Q}^*, \alpha^{2n/d} \rangle$.*

Proof. As $\mathbb{Q}(\alpha^{n/d})/\mathbb{Q}$ is abelian and $\alpha^{n/d}$ is a root of $x^d - \alpha^n \in \mathbb{Q}[x]$, theorem 38 shows that there exists some rational number b with $\alpha^{2n} = b^d$. Taking d-th roots gives $\alpha^{2n/d} = \zeta_d^k \cdot b$ for some positive integer k.

Let $g = \gcd(k, d)$, then we have $\left(\alpha^{2n/d}\right)^{d/g} \in \mathbb{Q}^*$. Suppose that g is greater than 2, then there is an integer $t < n$ with $\alpha^t \in \mathbb{Q}^*$, which gives a contradiction with the minimality of n.

If g equals 1, then ζ_d^k is a primitive d-th root of unity and thus $\langle \mathbb{Q}^*, \alpha^{2n/d} \rangle$ is $\mu_d \cdot \mathbb{Q}^*$.

Suppose that $4 \mid d$. Then there exist $t \in \mathbb{Z}_{>1}$ and $l \in \mathbb{N}$ with $d = 2^t \cdot l$. Substituting this in the identity $\alpha^{2n/d} = \zeta_d^k \cdot b$ gives

$$\alpha^{n/(2^{t-1} \cdot l)} = b \cdot \zeta_{2^t \cdot l}^k.$$

As n is minimal with $\alpha^n \in \mathbb{Q}$ we have $\left(\zeta_{2^t \cdot l}^k\right)^{2^{t-2} \cdot l} \notin \mathbb{Q}$. Therefore ζ_4^k is not contained in $\mathbb{Q}$ and hence k is odd and so g equals 1.

If g equals 2 then $4 \nmid d$ and we have $\gcd(d/2, k/2)$ is 1. Write $\zeta = \zeta_{d/2}^{k/2}$, then

$$\alpha^{2n/d} = \zeta_d^k \cdot b = \zeta \cdot b,$$

where ζ is a primitive $d/2$-th root of unity. We saw above that $d/2$ is odd. Therefore $-\zeta$ is a primitive d-th root of unity. We conclude that, also in this case, the group $\langle \mathbb{Q}^*, \alpha^{2n/d} \rangle$ equals $\mu_d \cdot \mathbb{Q}^*$. □

Corollary 70. *Let d be a divisor of n. If $\mathbb{Q}(\alpha^{n/d})/\mathbb{Q}$ is an abelian extension then we have $\mu_d \subset \mathbb{Q}(\alpha^{n/d})$.*

For the rest of this section we assume that every subfield of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of the form $\mathbb{Q}(\alpha^d)$ for some positive integer $d \mid n$. First we show that the intersection $D_\alpha \cap \mu_n$ is contained in μ_{60}, then we prove that $D_\alpha \cap \mu_n$ equals μ_k for some k in $\{1, 2, 3, 4, 6, 10\}$. Finally we give a subfield of $\mathbb{Q}(\alpha)/\mathbb{Q}$ that is not generated by a power of α for the cases that are excluded in proposition 67.

Lemma 71. *If all subfields of $\mathbb{Q}(\alpha)$ are generated by α^d for some divisor d of n, then $\mathbb{Q}(\alpha)$ has at most one subfield of degree 2 over $\mathbb{Q}$.*

Proof. Suppose that K is a quadratic subfield of $\mathbb{Q}(\alpha)$. Then there exists an integer t with $K = \mathbb{Q}(\alpha^{n/t})$. All extensions of degree 2 over $\mathbb{Q}$ are abelian. So, by corollary 70, we have $\mu_t \subset K$. Hence $\varphi(t) \leq 2$. We conclude that t is one of the numbers $1, 2, 3, 4, 6$. For $t = 1$ we have $\mathbb{Q}(\alpha^{n/t}) = \mathbb{Q}$. Moreover we know that $\mathbb{Q}(\alpha^{n/3}) \subset \mathbb{Q}(\alpha^{n/6})$ and $\mathbb{Q}(\alpha^{n/2}) \subset \mathbb{Q}(\alpha^{n/4})$, so there are at most two different subfields of $\mathbb{Q}(\alpha)$

of degree 2 over $\mathbb{Q}$. If both $\mathbb{Q}(\alpha^{n/3}) = \mathbb{Q}(\mu_3)$ and $\mathbb{Q}(\alpha^{n/4}) = \mathbb{Q}(\mu_4)$ are quadratic subfields of $\mathbb{Q}(\alpha)$, then $\mathbb{Q}(\sqrt{3})$ is another subfield of $\mathbb{Q}(\alpha)$ of degree 2 over $\mathbb{Q}$. This field cannot be generated by a power of α, so, $\mathbb{Q}(\alpha)$ has at most one subfield of degree 2. □

Proposition 72. *If all subfields of $\mathbb{Q}(\alpha)$ are generated by α^d for some divisor d of n, then we have $D_\alpha \cap \mu_n \subset \mu_{60}$.*

Proof. Let k be the positive integer with $D_\alpha \cap \mu_n = \mu_k$. If p is a prime dividing k, then $\mathbb{Q}(\zeta_p)$ is a subfield of $\mathbb{Q}(\alpha)$. Let K be $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) \subset \mathbb{Q}(\zeta_p)$. The extension $K/\mathbb{Q}$ is abelian and $\mu_n \cap K$ is contained in $\langle -1 \rangle$. As a subfield of $\mathbb{Q}(\alpha)$ the field K is generated by a power of α. Let $r \in \mathbb{Z}_{>0}$ be the largest integer with $K = \mathbb{Q}(\alpha^{n/r})$. As K is abelian we have by corollary 70 that $\mu_r \subset K$ and thus $r \mid 2$. So, K is a subfield of degree 1 or 2 over $\mathbb{Q}$. We conclude that the only primes dividing k are in the set $\{2, 3, 5\}$.

Suppose that p is an element of $\{3, 5\}$ such that p^2 divides k. Then the field $\mathbb{Q}(\zeta_{p^2})$ is abelian and it is of degree $p(p-1)$ over $\mathbb{Q}$. Therefore $\mathbb{Q}(\alpha)$ contains an abelian subfield K of degree p with $\mu_n \cap K \subset \langle -1 \rangle$, generated by a power of α. This gives a contradiction with corollary 70 and thus $\gcd(9 \cdot 25, k)$ is a divisor of 15.

Suppose that 8 divides k. Then ζ_8 is contained in $\mathbb{Q}(\alpha)$. Therefore $\mathbb{Q}(\alpha)$ has three different subfields of degree 2 over $\mathbb{Q}$, which gives a contradiction with lemma 71. We conclude that k divides $15 \cdot 4 = 60$. □

Corollary 73. *If all subfields of $\mathbb{Q}(\alpha)$ are generated by α^d for some divisor d of n, then we have $D_\alpha \cap \mu_n = \mu_k$ for some k in $\{1, 2, 3, 4, 6, 10\}$.*

Proof. By proposition 72 we have $k \mid 60$ and by lemma 71 there is at most one subfield of degree 2 over $\mathbb{Q}$ in $\mathbb{Q}(\alpha)$. If 3 divides k then this unique quadratic field is $\mathbb{Q}(\zeta_3)$. If 4 divides k it is $\mathbb{Q}(i)$ and if 5 divides k it is the subfield $\mathbb{Q}(\sqrt{5})$ of $\mathbb{Q}(\zeta_5)$. Hence k cannot be $12, 15, 20, 30$ or 60. In the case that 5 divides k the field $\mathbb{Q}(\sqrt{5})$ is generated by a power of α. As $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is an abelian extension we see by corollary 70 that the field $\mathbb{Q}(\sqrt{5})$ equals $\mathbb{Q}(\alpha^{n/t})$ for some $t \in \{1, 2\}$. As $\mathbb{Q}(\alpha^n)$ is $\mathbb{Q}$ we have $t = 2$ and $2 \mid n$. We conclude that also k is even; this excludes $k = 5$. Hence, k is an element of the set $\{1, 2, 3, 4, 6, 10\}$. □

We have shown that the assumption that all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α implies that $D_\alpha \cap \mu_n$ equals μ_k for some k in $\{1, 2, 3, 4, 6, 10\}$. Proposition 67 states that this assumption leads to some additional restrictions on n and D_α. In the following lemmas we prove, for each of the possible values for k, that the extra conditions are necessary.

Lemma 74. *If $D_\alpha \cap \mu_n$ is contained in μ_2 and all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α then we have $6 \nmid n$ or $\sqrt{-3} \notin D_\alpha$.*

Proof. We use lemma 68 to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ equals n. Suppose that the polynomial $x^n - \alpha^n$ is reducible over $\mathbb{Q}$.

We do not have $4 \mid n$ and $\alpha^n = -4c^4$ for some $c \in \mathbb{Q}$, as in that case $\alpha^{n/2} = 2ic^2$ and $i \in D_\alpha \cap \mu_n$. Therefore there exists a divisor $d > 1$ of n and an element $b \in \mathbb{Q}$ with $\alpha^n = b^d$. If d is even, then also n is even and we find the equality $(x^n - \alpha^n) = (x^{n/2} - b^{d/2})(x^{n/2} + b^{d/2}) \in \mathbb{Q}[x]$, which gives a contradiction with the minimality of n. So, d is odd and hence we have $\alpha^{n/d} = \zeta_d^k \cdot b$ for some $k \in \mathbb{N}$ with $\gcd(k, d) = 1$. Therefore $\zeta_d^k \in D_\alpha \cap \mu_n \subset \mu_2$. It follows that d equals 1 and thus $x^n - \alpha^n$ is irreducible over $\mathbb{Q}$.

Suppose that we have $6 \mid n$ and $\sqrt{-3} \in D_\alpha$. As $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ equals n, the degree of $\mathbb{Q}(\alpha^{n/d})$ over $\mathbb{Q}$ is d for all divisors d of n, thus $\mathbb{Q}(\alpha^{n/3})$ is the unique subextension of $\mathbb{Q}(\alpha)/\mathbb{Q}$ of degree 3 generated by a power of α. As $\sqrt{-3} \in D_\alpha$, we have $\zeta_3 \in \mathbb{Q}(\alpha)$ and therefore also $\mathbb{Q}(\zeta_3 \cdot \alpha^{n/3})$ is a subfield of $\mathbb{Q}(\alpha)$ of degree 3 over $\mathbb{Q}$. As $\zeta_3 \in \mathbb{Q}(\alpha^{n/3}, \zeta_3 \cdot \alpha^{n/3})$ and $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$, the field $\mathbb{Q}(\zeta_3 \cdot \alpha^{n/3})$ cannot be generated by a power of α. □

Lemma 75. *Suppose that 4 divides n. If α^n is an element of $-\mathbb{Q}^{*2} \setminus -4 \cdot \mathbb{Q}^{*4}$ then $\mathbb{Q}(\alpha^{n/4})$ has three different subfields of degree 2 over $\mathbb{Q}$.*

Proof. By lemma 68 the minimal polynomial of $\alpha^{n/4}$ is $x^4 - \alpha^n = x^4 + t^2 \in \mathbb{Q}[x]$ for some $t \in \mathbb{Q}^*$. Let β be a root of $x^4 + t^2$. The elements β^2, $\frac{1}{t}\beta^3 + \beta$ and $\frac{1}{t}\beta^3 - \beta$ are roots of the polynomials

$$x^2 + t^2, \quad x^2 + 2t \quad \text{and} \quad x^2 - 2t.$$

These are, again by lemma 68, all irreducible as we have $-t^2 \notin -4 \cdot \mathbb{Q}^4$, so there are three different subfields of $\mathbb{Q}(\alpha)$ of degree 2 over $\mathbb{Q}$. □

Lemma 76. *If $D_\alpha \cap \mu_n$ is μ_4 and all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α then we have $1 + i \in D_\alpha$.*

Proof. As we have $D_\alpha \cap \mu_n = \mu_4$ we know that 4 divides n and that $\alpha^{n/2}$ is an element of $i \cdot \mathbb{Q}^*$. Suppose that α^n is not an element of $-4 \cdot \mathbb{Q}^{*4}$. By the previous lemma we know that $\mathbb{Q}(\alpha)$ had three different subfields of degree 2 over $\mathbb{Q}$. This gives a contradiction with lemma 71. Therefore we conclude $\alpha^n \in -4 \cdot \mathbb{Q}^{*4}$ and hence we have $\alpha^{n/4} \in (1+i) \cdot \mathbb{Q}^* \cup (1-i) \cdot \mathbb{Q}^*$. If $\alpha^{n/4} \in (1+i) \cdot \mathbb{Q}^*$, then clearly we have $1 + i \in D_\alpha$. If $\alpha^{n/4} \in (1-i) \cdot \mathbb{Q}^*$, then $(1+i) = -(1-i)^3/2$ is an element of D_α as well. □

Lemma 77. *If d is a divisor of n with $\mu_d \subset D_\alpha$ then we have $\langle \mathbb{Q}^*, \alpha^{2n/d} \rangle = \mu_d \cdot \mathbb{Q}^*$.*

Proof. As μ_d is contained in D_α, the group $\langle \mathbb{Q}^*, \zeta_d \rangle / \mathbb{Q}^*$ is the unique subgroup of order $d/\gcd(d, 2)$ of the cyclic group $D_\alpha/\mathbb{Q}^*$. As also $\langle \mathbb{Q}^*, \alpha^{2n/d} \rangle / \mathbb{Q}^*$ has order $d/\gcd(d, 2)$ the subgroups $\langle \mathbb{Q}^*, \alpha^{2n/d} \rangle$ and $\langle \mathbb{Q}^*, \zeta_d \rangle = \mu_d \cdot \mathbb{Q}^*$ of D_α containing $\mathbb{Q}^*$ must be equal. □

Lemma 78. *If $D_\alpha \cap \mu_n$ is μ_6 and all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α then we have $\sqrt{-3} \in D_\alpha$.*

Proof. As we have $D_\alpha \cap \mu_n = \mu_6$ the integer n is divisible by 6. By lemma 77 we have $\mathbb{Q}(\alpha^{n/3}) = \mathbb{Q}(\zeta_3)$. In lemma 71 we saw that there can only be one subfield of $\mathbb{Q}(\alpha)$ of degree 2 over $\mathbb{Q}$. So, the unique quadratic subfield of $\mathbb{Q}(\alpha)$ is $\mathbb{Q}(\alpha^{n/2}) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}\,)$. Thus, by corollary 18, we have $\alpha^{n/2} \in \sqrt{-3} \cdot \mathbb{Q}^*$. □

Lemma 79. *If $D_\alpha \cap \mu_n$ is μ_{10} and all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α then we have $2 \mid n$, $4 \nmid n$ and $\sqrt{5} \in D_\alpha$.*

Proof. In lemma 71 we showed that there can be at most one subfield of degree 2 over $\mathbb{Q}$ in $\mathbb{Q}(\alpha)$. As we have $\mathbb{Q}(\sqrt{5}\,) \subset \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\alpha)$ this subfield is $\mathbb{Q}(\sqrt{5}\,)$. We therefore have $2 \mid n$ and $\alpha^{n/2} \in \sqrt{5} \cdot \mathbb{Q}^*$.

We have $\mathbb{Q}(\alpha^{n/5}) = \mathbb{Q}(\zeta_5)$ by lemma 77. Hence, if 4 is a divisor of n then the fields $\mathbb{Q}(\alpha^{n/4})$ and $\mathbb{Q}(\alpha^{n/5})$ are subfields of $\mathbb{Q}(\alpha)$ of degree 4. Both of these fields contain $\mathbb{Q}(\alpha^{n/2}) = \mathbb{Q}(\sqrt{5}\,)$. The field $\mathbb{Q}(\alpha^{n/4})$ is isomorphic to $\mathbb{Q}(\sqrt[4]{5c^2}\,)$ for some $c \in \mathbb{Q}$ as $\alpha^{n/2}$ is an element of $\sqrt{5} \cdot \mathbb{Q}^*$. As D_α does not contain i, the extension $\mathbb{Q}(\alpha^{n/4})/\mathbb{Q}$ is not abelian and thus $\mathbb{Q}(\alpha^{n/5})$ is not equal to $\mathbb{Q}(\alpha^{n/4})$. Hence, there also exists some third subfield of $\mathbb{Q}(\alpha)$ of degree 2 over $\mathbb{Q}(\sqrt{5}\,)$.

We show that there exist at most two subfields of degree 4 of $\mathbb{Q}(\alpha)$ generated by a power of α. Let t be a divisor of n such that $[\mathbb{Q}(\alpha^{n/t}) : \mathbb{Q}]$ is equal to 4. For divisors $r \mid r'$ of n we have $\mathbb{Q}(\alpha^{n/r'}) \subset \mathbb{Q}(\alpha^{n/r})$. So, for all prime divisors p of t we have $[\mathbb{Q}(\alpha^{n/p}) : \mathbb{Q}]$ divides 4. As, lemma 68, $x^p - \alpha^n$ is reducible if and only if there exists some integer b with $\alpha^n = b^p$ and n is minimal, we have $[\mathbb{Q}(\alpha^{n/p}) : \mathbb{Q}] \in \{p, p-1\}$ and hence $p \in \{2, 3, 5\}$. Suppose $3 \mid t$, then, as $x^3 - \alpha^n$ is reducible, we have $\mathbb{Q}(\alpha^{n/3}) = \mathbb{Q}(\zeta_3)$. But, this is impossible as $\mathbb{Q}(\sqrt{5}\,)$ is the unique subfield of degree 2 of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Therefore t is the product of a power of 2 and a power of 5. If $5 \mid t$ then $\mathbb{Q}(\alpha^{n/t})$ contains the field $\mathbb{Q}(\alpha^{n/5})$, if $5 \nmid t$, then $4 \mid t$ and $\mathbb{Q}(\alpha^{n/t})$ contains the field $\mathbb{Q}(\alpha^{n/4})$. Thus $\mathbb{Q}(\alpha^{n/t})$ equals one of these two fields. □

2.3 The Galois group

In the previous section we showed one implication in theorem 56. In this section we start the proof of the other implication. First we show that $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q})$ can be viewed as a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$. Then we prove that the intersection field $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ is of the form $\mathbb{Q}(\alpha^{n/r})$ for some integer r. For the radicals that satisfy one of the conditions (i), (ii), (iii), (iv) or (v) of theorem 56 we explicitly determine this intersection field. We compute its Galois group and use this to give an explicit description of $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q})$ as a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$.

For computing the subfields of $\mathbb{Q}(\alpha)$ we use the Galois correspondence between subfields of $\mathbb{Q}(\zeta_n, \alpha)$ and subgroups of its Galois group over $\mathbb{Q}$. To show that

$\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q})$ can be viewed as a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$ we define the map

$$\rho\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q}) \longrightarrow \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

by $\rho(\sigma) = (k,l)$ where $\sigma(\alpha) = \zeta_n^k \cdot \alpha$ and $\sigma(\zeta_n) = \zeta_n^l$.

Before we prove that ρ is an injective group homomorphism we recall the group-operation in the semidirect product $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$. Let t, t' be positive integers such that $t' \mid t$. The action of $(\mathbb{Z}/t\mathbb{Z})^*$ on $\mathbb{Z}/t'\mathbb{Z}$ is given by multiplication:

$$\mathbb{Z}/t'\mathbb{Z} \times (\mathbb{Z}/t\mathbb{Z})^* \longrightarrow \mathbb{Z}/t'\mathbb{Z}$$

$$(k,l) \mapsto kl.$$

This action induces the following group operation in $\mathbb{Z}/t'\mathbb{Z} \rtimes (\mathbb{Z}/t\mathbb{Z})^*$: for elements (k,l) and $(k',l') \in \mathbb{Z}/t'\mathbb{Z} \rtimes (\mathbb{Z}/t\mathbb{Z})^*$ we have

$$(k,l)(k',l') = (k + lk', ll');$$

the inverse of the element (k,l) is $(k,l)^{-1} = (-l^{-1}k, l^{-1})$.

Proposition 80. *The map ρ is an injective group homomorphism.*

Proof. The map ρ clearly is well-defined. It is injective because an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q})$ is determined by the images of ζ_n and α. Let σ and τ be elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q})$ with $\rho(\sigma) = (k_\sigma, l_\sigma)$ and $\rho(\tau) = (k_\tau, l_\tau)$. Then we have

$$\sigma\tau(\zeta_n) = (\zeta_n^{l_\tau})^{l_\sigma} = \zeta_n^{l_\tau l_\sigma} \quad \text{and} \quad \sigma\tau(\alpha) = \sigma(\zeta_n^{k_\tau} \cdot \alpha) = \zeta_n^{l_\sigma k_\tau + k_\sigma} \cdot \alpha.$$

Therefore we have

$$\rho(\sigma\tau) = (k_\sigma + l_\sigma k_\tau, l_\tau l_\sigma) = (k_\sigma, l_\sigma)(k_\tau, l_\tau) \in \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*,$$

hence ρ is a homomorphism. □

The following lemma shows that the intersection field $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ is of the form $\mathbb{Q}(\alpha^{n/r})$ for some $r \in \mathbb{N}$. In corollary 82 we compute the degree of some of the subextensions of $\mathbb{Q}(\zeta_n,\alpha)$ that we use later.

Lemma 81. *Let m be a positive integer and let $K \subset \mathbb{C}$ be a field containing a primitive m-th root of unity. Let γ be an element of $\mathbb{C}$ with $\gamma^m \in K$. Then $K(\gamma)$ over K is a cyclic Galois extension of degree r for some r dividing m, and we have $\gamma^r \in K$.*

Proof. This follows directly from theorem 14, the main theorem of Kummer theory (cf. [22], Chapter VIII, section 6, theorem 10). □

Corollary 82. *Let $d \in \mathbb{Z}_{>0}$ be minimal such that $\alpha^d \in \mathbb{Q}(\zeta_n)$; then we have*

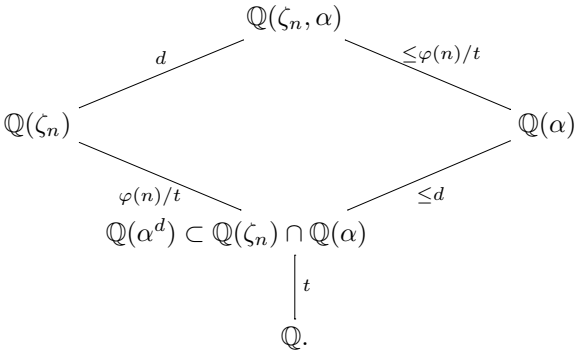
- $[\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q})] = \varphi(n) \cdot d$ *and*
- $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^d)$.

Proof. By lemma 81 we have $[\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}(\zeta_n)] = d$. As the degree of ζ_n over $\mathbb{Q}$ is $\varphi(n)$ we have $[\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}] = \varphi(n) \cdot d$.

Because α^d is an element of $\mathbb{Q}(\zeta_n)$ the degree of α over $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ is at most d. Denote the degree of $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ over $\mathbb{Q}$ by t. Then we have

$$[\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)] = \frac{\varphi(n)}{t}.$$

We get the following diagram



It follows that all inequalities in the diagram have to be equalities. As the degree of α over $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ is d we conclude that $\mathbb{Q}(\alpha^d)$ equals the intersection field $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$. □

For the rest of this section we fix the following notation. Let r denote the largest divisor of n with $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^{n/r})$; for the number d in corollary 82 we have $r = n/d$. Let X denote the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ for which the image under ρ of $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\alpha)\right)$ is $\{0\} \rtimes X$ and let G denote the image of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q})$ in $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$ under the map ρ.

Now the Galois group of $\mathbb{Q}(\alpha^{n/r})$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*/X$. The action of X on $\mathbb{Z}/n\mathbb{Z}$ induces an action on the subgroup $(n/r)\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/r\mathbb{Z}$. By corollary 70 we have $\mu_r \subset \mathbb{Q}(\alpha^{n/r}) \subset \mathbb{Q}(\alpha)$. So $k \in X$ implies that r divides $k - 1$. Therefore the action of X on $\mathbb{Z}/r\mathbb{Z}$ is trivial. Restricting $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}\right)$ to $\mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})$ gives an embedding ρ' of the group $\mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})$ in $\mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*/X$ such that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Gal}\left(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q}) \\ \downarrow \rho & & \downarrow \rho' \\ \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* & \xrightarrow{\text{proj}} & \mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*/X. \end{array}$$

Proposition 83. *Let G' be the image of* $\mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})$ *under ρ' in $\mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*/X$. Then G is the pre-image of G' under the projection map* proj.

Proof. This simply follows from the degrees of the subextensions of $\mathbb{Q}(\alpha)/\mathbb{Q}$. The number of elements in the kernel of the map proj is $\#(r\mathbb{Z}/n\mathbb{Z} \rtimes X) = n/r \cdot \#X$. By corollary 82 we have

$$\begin{aligned} n/r \cdot \#X &= [\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}(\zeta_n)] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha^{n/r})] \\ &= [\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}(\alpha^{n/r})] \\ &= \frac{\#G}{\#G'}. \end{aligned}$$

The number of elements of the pre-image of G' equals the number of elements in G, consequently these groups are equal. □

Proposition 84. *Let α be a radical satisfying one of the conditions* (i), (ii), (iii), (iv) *or* (v) *of theorem 56. Let k be defined by $D_\alpha \cap \mu_n = \mu_k$.*

- *If α satisfies condition* (i) *then r is* 1 *or* 2,
- *If α satisfies one of the conditions* (ii), (iii), (iv) *or* (v) *then $r = k$ and $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha) = \mathbb{Q}(\mu_r)$.*

Proof. The extension $\mathbb{Q}(\alpha^{n/r})/\mathbb{Q}$ is abelian as $\mathbb{Q}(\alpha^{n/r})$ is contained in $\mathbb{Q}(\zeta_n)$. Therefore, by lemma 69, we have $\mu_r \cdot \mathbb{Q}^* = \langle \mathbb{Q}^*, \alpha^{2n/r} \rangle$. As $\mu_r \cdot \mathbb{Q}^* \subset D_\alpha$, we have $\mu_r \subset \mu_k$ and hence $r \mid k$. Lemma 77 gives $\mu_k \cdot \mathbb{Q}^* = \langle \mathbb{Q}^*, \alpha^{2n/k} \rangle \subset \mathbb{Q}(\alpha^{n/r})$, as $\mu_k \subset D_\alpha$. This results in the following chain of field extensions.

$$\begin{array}{c} \mathbb{Q}(\alpha^{n/r}) \\ | \\ \mathbb{Q}(\alpha^{2n/k}) = \mathbb{Q}(\mu_k) \\ | \\ \mathbb{Q}(\alpha^{2n/r}) = \mathbb{Q}(\mu_r) \end{array}$$

By definition of r every odd divisor of k is also a divisor of r. Thus $r \mid k$ and $k \mid 2r$.

If k is 1 or 2, then clearly $r \in \{1, 2\}$. If α satisfies condition (ii) then n is odd and hence $\mathbb{Q}(\alpha^{n/r}) = \mathbb{Q}(\alpha^{2n/r}) = \mathbb{Q}(\mu_r)$ and r equals k. If α satisfies condition (iii) then $k = 4$, so $r \in \{2, 4\}$. As $1 + i \in D_\alpha$ we have $\mathbb{Q}(\alpha^{n/4}) = \mathbb{Q}(\alpha^{n/2}) = \mathbb{Q}(i)$. Hence r equals $k = 4$ and $\mathbb{Q}(\alpha^{n/r})$ is $\mathbb{Q}(\mu_r)$. If α satisfies condition (iv) then $k = 6$, so $r \in \{3, 6\}$. As $\zeta_3 \in \mathbb{Q}(\alpha^{n/3}) \setminus \mathbb{Q}$, we have $\mathbb{Q}(\alpha^{n/6}) = \mathbb{Q}(\alpha^{n/3}, \alpha^{n/2}) = \mathbb{Q}(\zeta_3, \sqrt{-3}\,) = \mathbb{Q}(\zeta_3)$. Hence r equals $k = 6$ and $\mathbb{Q}(\alpha^{n/r})$ is $\mathbb{Q}(\mu_r)$. Similarly, if α satisfies condition (v) then $\mathbb{Q}(\alpha^{n/10}) = \mathbb{Q}(\alpha^{n/5}, \alpha^{n/2}) = \mathbb{Q}(\zeta_5)$. We therefore have $r = k = 10$ and $\mathbb{Q}(\alpha^{n/r}) = \mathbb{Q}(\mu_r)$. □

Theorem 85. *Let α be a radical satisfying one of the conditions* (i), (ii), (iii), (iv) *or* (v) *of theorem 56. With notation as in proposition 83 and for a particular choice for ζ_4, ζ_6 and ζ_{10}, we have*

$$G' = \begin{cases} \text{the trivial group} & \text{if } r = 1, \\ \{(0,1),(1,\varepsilon)\} \subset \mathbb{Z}/2\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*/X & \text{if } r = 2, \\ \{(0,1),(1,-1)\} \subset \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/3\mathbb{Z})^* & \text{if } r = 3, \\ \{(0,1),(-1,-1)\} \subset \mathbb{Z}/4\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z})^* & \text{if } r = 4, \\ \{(0,1),(-1,-1)\} \subset \mathbb{Z}/6\mathbb{Z} \rtimes (\mathbb{Z}/6\mathbb{Z})^* & \text{if } r = 6, \\ \{(0,1),(6,-1),(7,7),(9,3)\} \subset \mathbb{Z}/10\mathbb{Z} \rtimes (\mathbb{Z}/10\mathbb{Z})^* & \text{if } r = 10, \end{cases}$$

where, for $r = 2$, the element ε is the non-trivial element of the group $(\mathbb{Z}/n\mathbb{Z})^*/X$.

Proof. If r is 1, then the field $\mathbb{Q}(\alpha^{n/r})$ is $\mathbb{Q}$ and its Galois group over $\mathbb{Q}$ is trivial, hence also G' is trivial.

If $r = 2$ then the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})$ has two elements. The non-trivial element acts non-trivially on $\alpha^{n/r}$ and it is the restriction to $\mathbb{Q}(\alpha^{n/r})$ of an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ that acts non-trivially on ζ_n. This gives us $G' = \{(0,1),(1,\varepsilon)\} \subset \mathbb{Z}/2\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*/X$, where ε denotes the non-trivial element of $(\mathbb{Z}/n\mathbb{Z})^*/X$.

If $r > 2$ then by proposition 84, we see that $\mathbb{Q}(\alpha^{n/r})$ equals $\mathbb{Q}(\mu_r)$. In these cases the group $(\mathbb{Z}/n\mathbb{Z})^*/X$ is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^*$. Calculating the action of $\mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})$ on $\alpha^{n/r}$ and on ζ_r gives the groups listed in the theorem. For example if r equals 10 then it follows from the fact $\sqrt{5} \in D_\alpha$ that $\alpha^{n/2} \in \sqrt{5} \cdot \mathbb{Q}^*$. As $\mathbb{Q}(\alpha^{n/10})$ is abelian corollary 70 gives $\mu_{10} \subset \mathbb{Q}(\alpha^{n/5})$ and thus $\alpha^{n/5} \in \zeta_5^k \cdot \mathbb{Q}^*$ for some $k \in \{1,2,3,4\}$. We therefore know that $\alpha^{n/10}$ is of the form $\zeta_5^l\sqrt{5} \cdot c$ for some $c \in \mathbb{Q}^*$ and for $l = 3k \bmod 5$. If, for example, σ is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ with $\sigma(\zeta_5) = \zeta_5^2$, then $\sigma(\zeta_{10}) = \zeta_{10}^7$ (as 7 is the unique element t of $(\mathbb{Z}/10\mathbb{Z})^*$ for which t is 2 modulo 5) and $\sigma(\sqrt{5}) = 2(\zeta_5 + \zeta_5^{-1}) + 1 = 2\sigma(\zeta_5^2 + \zeta_5^{-2}) + 1 = -\sqrt{5}$. The element automorphism σ corresponds under ρ to the element $(2l+5, 7) \in \mathbb{Z}/10\mathbb{Z} \rtimes (\mathbb{Z}/10\mathbb{Z})^*$ as we have

$$\sigma(\alpha^{n/10}) = \sigma(\zeta_5^l\sqrt{5})c = -\zeta_5^{2l}\sqrt{5}c = \zeta_{10}^5 \cdot \zeta_5^l \cdot \zeta_5^l\sqrt{5}c = \zeta_{10}^{2l+5} \cdot \zeta_5^l\sqrt{5}c = \zeta_{10}^{2l+5}\alpha^{n/10}.$$

If we compute the action of each element of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ on $\alpha^{n/10}$ and on ζ_{10}, then we find the group $\{(0,1),(2l+5,7),(4l+5,3),(6l,9)\}$. For the choice $l = 1$, this gives the group listed in the theorem. □

In the next two sections we finish the proof of theorem 56. We determine the subgroups of $\rho(G)$ that correspond to the subfields of $\mathbb{Q}(\alpha)$. The next lemma gives the subgroups of $\rho(G)$ that correspond to subfields of $\mathbb{Q}(\alpha)$ generated by a power of α.

Lemma 86. *Let d be a divisor of n. Then the ρ-image of the Galois group $F = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\alpha^{n/d})\right)$ equals $(d\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*) \cap G$.*

Proof. An element σ of $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}\right)$ corresponds under ρ to a pair

$$(k, l) \in \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*,$$

with $\sigma(\alpha) = \zeta_n^k \alpha$ and $\sigma(\zeta_n) = \zeta_n^l$. We have $\sigma(\alpha^{n/d}) = \zeta_n^{nk/d} \alpha^{n/d}$ and thus $\sigma \in F$ holds if and only if d is a divisor of k. That is, the image of F is the intersection of G and $d\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$. □

2.4 Subgroups

In this section we give a group theoretical theorem that we will use in the next section to finish the proof of theorem 56.

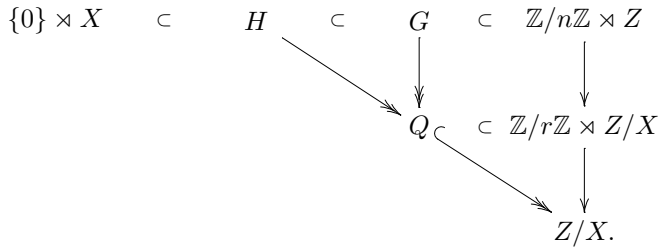
Lemma 87. *Let N be a group and let G be a group acting on N by group homomorphisms. For every subgroup H of $N \rtimes G$ containing $\{1\} \rtimes G$ we have $H = (H \cap N) \rtimes G$.*

Proof. Because we have $\{1\} \rtimes G \subset H$ it is clear that $(H \cap N) \rtimes G$ is contained in H. Let h be an element of H. Then we have $h = n \cdot g$ for some $n \in N$ and some $g \in G$. As g is an element of H we have $n \in H \cap N$, so H is contained in $(H \cap N) \rtimes G$. □

Theorem 88. *Let $r, n \in \mathbb{Z}_{>0}$ with $r \mid n$. Consider the following groups:*

- Z: *a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$,*
- X: *a subgroup of Z contained in the kernel of the projection map $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/r\mathbb{Z})^*$,*
- Q: *a subgroup of $\mathbb{Z}/r\mathbb{Z} \rtimes Z/X$ isomorphic to Z/X under projection on the second coordinate,*
- G: *the pre-image of Q under the projection map $\pi\colon \mathbb{Z}/n\mathbb{Z} \rtimes Z \longrightarrow \mathbb{Z}/r\mathbb{Z} \rtimes Z/X$,*
- H: *a subgroup of G containing $\{0\} \rtimes X$ that maps surjectively to Z/X under π.*

These groups give the following commuting diagram



If for all divisors s of r with $s \neq 1$ we have $Q \not\subset s\mathbb{Z}/r\mathbb{Z} \rtimes Z/X$ and if for all $f \in \mathbb{Z}/n\mathbb{Z}$ and all $g \in Z$ the condition $(f, g) \in H$ implies that $(rf, 1)$ is an element of H, then we have

$$H = (d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G$$

for some divisor d of n.

Proof. Let H_0 be the kernel of the projection map $H \longrightarrow Z/X$. Then clearly we have $\{0\} \rtimes X \subset H_0 \subset r\mathbb{Z}/n\mathbb{Z} \rtimes X$. By lemma 87 we therefore see that

$$H_0 = d_0\mathbb{Z}/n\mathbb{Z} \rtimes X,$$

for some divisor d_0 of n with $r \mid d_0$. Let a be an element of $\mathbb{Z}/n\mathbb{Z}$ such that there exists some $b \in Z$ with $(a, b) \in H$. Then we have by the second condition in the theorem $(ra, 1) \in H_0$ and thus ra is an element of $d_0\mathbb{Z}/n\mathbb{Z}$. It follows that a is contained in $\frac{d_0}{r}\mathbb{Z}/n\mathbb{Z}$. Let d be the integer d_0/r. We showed that H is contained in $(d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G$. Below we prove that these groups are equal. We consider the chain of groups

$$H_0 = d_0\mathbb{Z}/n\mathbb{Z} \rtimes X \subset H \subset (d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G \subset d\mathbb{Z}/n\mathbb{Z} \rtimes Z.$$

As we have $(d\mathbb{Z}/n\mathbb{Z} \rtimes Z : d_0\mathbb{Z}/n\mathbb{Z} \rtimes Z) = d_0/d = r$ we see that the index $\big(d\mathbb{Z}/n\mathbb{Z} \rtimes Z : H_0\big)$ equals $r \cdot (Z : X) = r \cdot \#(Z/X)$. By definition of H_0 we have $(H : H_0) = \#(Z/X)$.

To determine the index of $(d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G$ in $d\mathbb{Z}/n\mathbb{Z} \rtimes Z$ we consider the projection map $\mathbb{Z}/n\mathbb{Z} \rtimes Z \longrightarrow \mathbb{Z}/r\mathbb{Z} \rtimes Z/X$. As $H \subset d\mathbb{Z}/n\mathbb{Z} \rtimes Z$ maps surjectively to Z/X via Q we have $Q \subset \gcd(r, d)\mathbb{Z}/r\mathbb{Z} \rtimes Z/X$. By assumption we therefore have $\gcd(r, d) = 1$.

$$\begin{array}{ccc} G & \subset & \mathbb{Z}/n\mathbb{Z} \rtimes Z \\ \cup & & \cup \\ (d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G & \subset & d\mathbb{Z}/n\mathbb{Z} \rtimes Z \\ \big\downarrow & & \big\downarrow \\ Q & \subset & \mathbb{Z}/r\mathbb{Z} \rtimes Z/X \end{array}$$

As G is the pre-image of Q also $(d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G$ is the pre-image of Q under the surjective projection map $d\mathbb{Z}/n\mathbb{Z} \rtimes Z \longrightarrow \mathbb{Z}/r\mathbb{Z} \rtimes Z/X$. We conclude that

$$(d\mathbb{Z}/n\mathbb{Z} \rtimes Z : (d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G) = (\mathbb{Z}/r\mathbb{Z} \rtimes Z/X : Q) = r.$$

Summarising, we showed

$$\big(d\mathbb{Z}/n\mathbb{Z} \rtimes Z : (d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G\big)\big(H : H_0\big) = r \cdot \#(Z/X) = \big(d\mathbb{Z}/n\mathbb{Z} \rtimes Z : H_0\big).$$

We conclude that H is equal to $(d\mathbb{Z}/n\mathbb{Z} \rtimes Z) \cap G$. □

2.5 Conclusion of the proof

In this section we finish the proof of theorem 56 and prove theorem 57. We apply theorem 88 to show that all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α if α satisfies one of the conditions (i), (ii), (iii), (iv) or (v) of theorem 56. We first give a proposition and some lemmas. In proposition 94 we will use these results to show that the conditions of theorem 88 are satisfied for the groups that we are interested in.

Proposition 89. *Let Z be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and let G be a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes Z$ consisting of the elements in $(A \times X) \cup (B \times Y)$ for subsets A, B of $\mathbb{Z}/n\mathbb{Z}$ and subsets X, Y of Z with*

X: *a subgroup of Z of index 2,*
Y: *the complement of X in Z,*
A: *a subgroup of $\mathbb{Z}/n\mathbb{Z}$,*
B: *some coset of A in $\mathbb{Z}/n\mathbb{Z}$.*

Let f be an element of $\mathbb{Z}/n\mathbb{Z}$ and let g be an element of Z. For subgroups H of G with $\{0\} \rtimes X \subset H$ we have the following implication

$$(f, g) \in H \Rightarrow (kf, 1) \in H$$

for all k in the ideal $\langle y + 1 \colon y \in Y \rangle \subset \mathbb{Z}/n\mathbb{Z}$.

Proof. We use the group action in $\mathbb{Z}/n\mathbb{Z} \rtimes Z$, as described in section 2.3.

First assume that f is an element of $\mathbb{Z}/n\mathbb{Z}$ and that g is an element of Z with (f, g) in $H \cap A \times X$. As X is a subgroup of Z we have $x^{-1} \in X$ for all $x \in X$. Therefore we have for all $k \in \mathbb{N}$

$$(kf, 1) = \big((f, g)(0, g^{-1})\big)^k \in H.$$

Now assume that f is an element of $\mathbb{Z}/n\mathbb{Z}$ and that g is an element of Z with (f, g) in $H \cap B \times Y$. As X is a subgroup of Z of index 2 and $X \cup Y$ equals Z the element $z^{-1}y$ is contained in X for all $y, z \in Y$. Therefore we see that

$$(f, y) = (f, g)(0, g^{-1}y) \in H \quad \text{for all } y \in Y.$$

Squaring this element shows that $\big((1 + y)f, y^2\big) \in H$ for all $y \in Y$. As y^2 is an element of X we see that

$$\big((1 + y)f, 1\big) = \big((1 + y)f, y^2\big)(0, y^{-2}) \in H \quad \text{for all } y \in Y.$$

Let k be an element of $\langle y + 1 \colon y \in Y \rangle$. Then there are elements $y_i \in Y$ and integers c_i with $k = \sum_i c_i(y_i + 1)$. As $\big((1 + y)f, 1\big)$ is contained in $A \times X$ for all y in Y, we have

$$(kf, 1) = \sum_i \big((1 + y_i)f, 1\big)^{c_i} \in H,$$

also in this case. □

Lemma 90. *Let p be a prime number and let t be a positive integer. Let X be a subgroup of $(\mathbb{Z}/p^t\mathbb{Z})^*$ of index 2 and let Y be its complement. Then the ideal $\langle y+1\colon y \in Y\rangle$ in $\mathbb{Z}/p^t\mathbb{Z}$ is the ideal generated by 2 if and only if one of the following conditions holds:*

- *p is greater than 3,*
- *p is 2 or 3 and X is not equal to the kernel of the projection map $(\mathbb{Z}/p^t\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$, where $m = 4$ if p is 2 and $m = 3$ if p is 3.*

Proof. The ideal $\langle y + 1\colon y \in Y\rangle$ is of the form $p^s\mathbb{Z}/p^t\mathbb{Z}$ for some $0 \leq s \leq t$. The number of elements of Y is $\varphi(p^t)/2$. The number of elements of $p^s\mathbb{Z}/p^t\mathbb{Z}$ is p^t/p^s. Therefore, for all primes $p > 3$, we see that

$$\#\langle y + 1\colon y \in Y\rangle \geq \#Y > \#(p\mathbb{Z}/p^t\mathbb{Z})$$

and hence in these cases the ideal $\langle y + 1\colon y \in Y\rangle$ must equal the full ring $\mathbb{Z}/p^t\mathbb{Z} = 2\mathbb{Z}/p^t\mathbb{Z}$.

If p is 3 we have $\#Y = \varphi(p^t)/2 = 2p^{t-1}/2 = p^{t-1} = \#(p\mathbb{Z}/p^t\mathbb{Z})$. We conclude that $\langle y+1\colon y \in Y\rangle$ is $3\mathbb{Z}/3^t\mathbb{Z}$ if Y equals $\{y \in (\mathbb{Z}/3^t\mathbb{Z})^*$ with $y = 2 \bmod 3\}$ and that $\langle y + 1\colon y \in Y\rangle$ equals $\mathbb{Z}/3^t\mathbb{Z} = 2\mathbb{Z}/3^t\mathbb{Z}$ if there is some $y \in Y$ with $y = 1 \bmod 3$.

If p is 2 clearly we have $\langle y + 1\colon y \in Y\rangle \subset 2\mathbb{Z}/2^t\mathbb{Z}$. In this case it holds that $\#Y = \varphi(p^t)/2 = 2^{t-1}/2 = \#(4\mathbb{Z}/2^t\mathbb{Z})$. The ideal $\langle y + 1\colon y \in Y\rangle$ is $4\mathbb{Z}/2^t\mathbb{Z}$ if Y equals $\{y \in (\mathbb{Z}/2^t\mathbb{Z})^*$ with $y = 3 \bmod 4\}$ and $\langle y + 1\colon y \in Y\rangle$ equals $2\mathbb{Z}/2^t\mathbb{Z}$ if there is some $y \in Y$ with $y = 1 \bmod 4$. □

Lemma 91. *Let $n \in \mathbb{Z}_{>0}$ and let X be a subgroup of index 2 of $(\mathbb{Z}/n\mathbb{Z})^*$ such that the group X is not equal to the kernel of the projection map $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ for any element $m \in \{3, 4\}$ dividing n. Let Y be the complement of X in $(\mathbb{Z}/n\mathbb{Z})^*$. Then the ideal $\langle y + 1\colon y \in Y\rangle$ in $\mathbb{Z}/n\mathbb{Z}$ is the ideal generated by 2.*

Proof. For all divisors d of n we define the projection map $\varphi_d\colon (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/d\mathbb{Z})^*$. As X is a subgroup of index 2 of $(\mathbb{Z}/n\mathbb{Z})^*$ the group $\varphi_d(X)$ is a subgroup of index at most 2 in $(\mathbb{Z}/d\mathbb{Z})^*$ and $\#\varphi_d(X) = \#\varphi_d(Y)$ for all divisors d of n. Let $n = p_1^{r_1} \cdots p_s^{r_s}$ be the prime factorisation of n. By lemma 90 the element 2 is in the image of $\langle y + 1\colon y \in Y\rangle$ under the map $\varphi_{p_i^{r_i}}$ for all i. The Chinese remainder theorem now tells us that 2 is contained in $\langle y + 1\colon y \in Y\rangle$. If n is odd, it follows that $\langle y + 1\colon y \in Y\rangle$ is $\mathbb{Z}/n\mathbb{Z} = 2\mathbb{Z}/n\mathbb{Z}$. If n is even all elements of Y are odd, hence we have $2 \in \langle y + 1\colon y \in Y\rangle \subset 2\mathbb{Z}/n\mathbb{Z}$. We conclude that also in this case $\langle y + 1\colon y \in Y\rangle$ is $2\mathbb{Z}/n\mathbb{Z}$. □

Lemma 92. *Let r be a divisor of n and suppose that r is even if n is even. Let Y be the pre-image of -1 under the projection map $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/r\mathbb{Z})^*$. Then the ideal $\langle y + 1\colon y \in Y\rangle \subset \mathbb{Z}/n\mathbb{Z}$ equals $r\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let p be a prime and assume that $n = p^k$ and $r = p^l$ for integers k, l with $l \leq k$.

If $l \neq 0$ then Y is the set $-1+\langle p^l \rangle \subset (\mathbb{Z}/n\mathbb{Z})^*$, so p^l is an element of $\langle y+1 \colon y \in Y \rangle$ and it follows $\langle y+1 \colon y \in Y \rangle = r\mathbb{Z}/n\mathbb{Z}$.

Now consider the case that l is 0. By assumption p is odd and as the pre-image of -1 is the group $(\mathbb{Z}/n\mathbb{Z})^*$ we have $1 \in Y$. Therefore 2 is an element of $\langle y+1 \colon y \in Y \rangle$ and as $\gcd(2,p) = 1$ the ideal $\langle y+1 \colon y \in Y \rangle$ equals $r\mathbb{Z}/n\mathbb{Z}$.

So the lemma holds for n a prime power. For general n, we first determine the prime factorisation of $n = p_1^{r_1} \cdots p_k^{r_k}$. As the projection of $\langle y+1 \colon y \in Y \rangle$ in $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$ is $r\mathbb{Z}/p_i^{r_i}\mathbb{Z}$ for all i we have $\langle y+1 \colon y \in Y \rangle = r\mathbb{Z}/n\mathbb{Z}$ by the Chinese remainder theorem. □

Lemma 93. *Let n be a positive integer with $10 \mid n$ and $4 \nmid n$. Let G be the pre-image of the group $\{(0,1),(6,-1),(7,7),(9,3)\} \subset \mathbb{Z}/10\mathbb{Z} \rtimes (\mathbb{Z}/10\mathbb{Z})^*$ under the projection*

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{Z}/10\mathbb{Z} \rtimes (\mathbb{Z}/10\mathbb{Z})^*.$$

Let π be the projection map $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/10\mathbb{Z})^*$ and define $X = \pi^{-1}(1)$.

Let f be an element of $\mathbb{Z}/10\mathbb{Z}$ and let g be an element of $(\mathbb{Z}/n\mathbb{Z})^*$. Then for all subgroups H of G containing $\{0\} \rtimes X$ we have the implication

$$(f,g) \in H \Rightarrow (10f, 1) \in H.$$

Proof. Define one more projection map $p \colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/10\mathbb{Z}$ and define subsets of $(\mathbb{Z}/n\mathbb{Z})^*$ by $Y = \pi^{-1}(-1)$, $U = \pi^{-1}(7)$ and $V = \pi^{-1}(3)$ and subsets of $\mathbb{Z}/n\mathbb{Z}$ by $A = p^{-1}(0)$, $B = p^{-1}(6)$, $C = p^{-1}(7)$ and $D = p^{-1}(9)$. Then G is the group given by the elements

$$(A \times X) \cup (B \times Y) \cup (C \times U) \cup (D \times V) \quad \text{in} \quad \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*.$$

Let H be a subgroup of G with $\{0\} \rtimes X \subset H$. Let f be an element of $\mathbb{Z}/10\mathbb{Z}$ and let g be an element of $(\mathbb{Z}/10\mathbb{Z})^*$ such that (f,g) is contained in H. As before (proposition 89) one shows that (f,g) in $(A \times X)$ implies

$$(kf, 1) = \big((f,g)(0,g^{-1})\big)^k \in H$$

for all integers k, and (f,g) in $(B \times Y)$ implies

$$((1+y)f, 1) = \big((f,g)(0,yg^{-1})\big)^2 (0, y^{-2}) \in H$$

for all $y \in Y$ and thus $(kf,1)$ in H for all $k \in \langle y+1 \colon y \in Y \rangle$.

Now assume that (f,g) is contained in $H \cap (C \times U)$. First we remark that for all $u \in U$ we have $g^{-1}u \in X$. Therefore we have

$$(f,u) = (f,g)(0,g^{-1}u) \in H \quad \text{for all } u \in U.$$

Then also $(f,u)^2 = \big((1+u)f, u^2\big)$ is an element of $H \cap (B \times Y)$ and by multiplying by $(0, yu^{-2}) \in A \times X$ we have $\big((1+u)f, y\big) \in H$ for all $y \in Y$ and for all $u \in U$. Squaring this element gives

$$\big((1+u)(1+y)f, 1\big) = \big((1+u)f, y\big)^2(0, y^{-2}) \in H \quad \text{for all } u \in U \text{ and for all } y \in Y,$$

hence $(kf, 1)$ is an element of H for all k in $\langle (1+u)(1+y) \colon u \in U, y \in Y \rangle$. In lemma 92 we saw that $\langle y+1 \colon y \in Y \rangle$ equals $10\mathbb{Z}/n\mathbb{Z}$. Similarly one shows that U equals the set $\{u \in (\mathbb{Z}/n\mathbb{Z})^* \text{ with } u = 7 \bmod 10\}$ and therefore $\langle u+1 \colon u \in U \rangle$ is $2\mathbb{Z}/n\mathbb{Z}$. Because 4 is not a divisor of n we have

$$\langle (1+u)(1+y) \colon u \in U, y \in Y \rangle = 20\mathbb{Z}/n\mathbb{Z} = 10\mathbb{Z}/n\mathbb{Z}.$$

The implication

$$(f,g) \in H \cap (C \times U) \Rightarrow (kf, 1) \in H,$$

for all k in $\langle y+1 \colon y \in Y \rangle = 10\mathbb{Z}/n\mathbb{Z}$ follows. The proof for elements (f,g) of $H \cap (D \times V)$ is exactly the same as the proof for (f,g) in $H \cap (C \times U)$. We conclude that for all $f \in \mathbb{Z}/n\mathbb{Z}$ and all $g \in (\mathbb{Z}/n\mathbb{Z})^*$ with $(f,g) \in H$ we have $(kf, 1) \in H$ for all k in $\langle y+1 \colon y \in Y \rangle$. □

Before we conclude the proof of theorem 56 in the following proposition we fix three homomorphisms. Let $\rho \colon \mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}) \longrightarrow \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$ be the map that we introduced in section 2.3. Denote by π be the composition of the map ρ and the projection $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ and let, as in section 2.3,

$$\rho' \colon \mathrm{Gal}(\mathbb{Q}(\alpha^{n/r}) : \mathbb{Q}) \longrightarrow \mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* / \pi\big(\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\alpha))\big)$$

be the composite of ρ and the projection

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* / \pi\big(\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\alpha))\big).$$

Proposition 94. *Let $\alpha \in \mathbb{C}$ be a radical over $\mathbb{Q}$ with $n \in \mathbb{Z}_{>0}$ minimal such that $\alpha^n \in \mathbb{Q}$. Let D_α be the group $\langle \mathbb{Q}^*, \alpha \rangle$.*

If α satisfies one of the following conditions

(i) *$D_\alpha \cap \mu_n \subset \mu_2$ and we have $6 \nmid n$ or $\sqrt{-3} \notin D_\alpha$,*

(ii) *$D_\alpha \cap \mu_n = \mu_3$,*

(iii) *$D_\alpha \cap \mu_n = \mu_4$ and $1 + i \in D_\alpha$,*

(iv) *$D_\alpha \cap \mu_n = \mu_6$ and $\sqrt{-3} \in D_\alpha$,*

(v) *$D_\alpha \cap \mu_n = \mu_{10}$ and both $4 \nmid n$ and $\sqrt{5} \in D_\alpha$,*

then every subfield of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of the form $\mathbb{Q}(\alpha^d)$ for some positive divisor d of n.

Proof. Let α be a radical satisfying one of the conditions (i), (ii), (iii), (iv) or (v). Let K be a subfield of $\mathbb{Q}(\alpha)$ and let H_K be the image of the group $\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/K)$ under ρ. Let r, as before, denote the maximal positive divisor of n with $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha^{n/r})$.

We consider three cases: first we suppose that K contains the field $\mathbb{Q}(\alpha^{n/r})$. Then we consider the case that the intersection $K\cap\mathbb{Q}(\alpha^{n/r})$ is $\mathbb{Q}$. Finally we suppose that $K\cap\mathbb{Q}(\alpha^{n/r})$ is a field not equal to $\mathbb{Q}(\alpha^{n/r})$ or $\mathbb{Q}$. In each of these cases we prove that H_K is a group of the form

$$\big(d\mathbb{Z}/n\mathbb{Z}\rtimes(\mathbb{Z}/n\mathbb{Z})^*\big)\cap\rho\big(\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q})\big),$$

for some divisor d of n. It follows by lemma 86 that all subfields of $\mathbb{Q}(\alpha)$ are generated by a power of α.

Suppose that K is a subfield of $\mathbb{Q}(\alpha)$ containing $\mathbb{Q}(\alpha^{n/r})$. Let X be the group $\pi\big(\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q}(\alpha))\big)$. As $\mathbb{Q}(\alpha^{n/r})$ is a subfield of K we have

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n,\alpha)/K\right)\subset\mathrm{Gal}\left(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q}(\alpha^{n/r})\right).$$

By Galois theory the group $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha^{n/r})\right)$ is isomorphic to a subgroup X of $(\mathbb{Z}/n\mathbb{Z})^*$. As $\mathbb{Q}(\zeta_n)\cap K$ equals $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha^{n/r})$ the inclusion

$$\rho\big(\mathrm{Gal}\left(\mathbb{Q}(\zeta_n,\alpha)/K\right)\big)\subset\mathbb{Z}/n\mathbb{Z}\rtimes X$$

holds; suppose $(a,y)\in\rho\big(\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/K)\big)$ with $y\in(\mathbb{Z}/n\mathbb{Z})^*\setminus X$ then (a,y) does not fix $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\alpha)$ and we have a contradiction with $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\alpha)\subset K$. As K is a subfield of $\mathbb{Q}(\alpha)$ it follows

$$\{0\}\rtimes X\subset H_K\subset\mathbb{Z}/n\mathbb{Z}\rtimes X.$$

By lemma 87 we see that H_K is of the form $d\mathbb{Z}/n\mathbb{Z}\rtimes X$ for some divisor d of n. As the group $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q}(\alpha^{n/r})\right)$ fixes the field $\mathbb{Q}(\alpha^{n/r})=\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\alpha)$ and as $n/r\in d\mathbb{Z}/n\mathbb{Z}$ since $\mathbb{Q}(\alpha^{n/r})$ is contained in K, we see that for this particular choice of d we have

$$\big(d\mathbb{Z}/n\mathbb{Z}\rtimes(\mathbb{Z}/n\mathbb{Z})^*\big)\cap G=d\mathbb{Z}/n\mathbb{Z}\rtimes X.$$

By lemma 86 we conclude that K equals $\mathbb{Q}(\alpha^{n/d})$ for some divisor d of n. This completes the proof for subfields K of $\mathbb{Q}(\alpha)$ containing $\mathbb{Q}(\alpha^{n/r})$.

If r equals 1, then for every subfield K of $\mathbb{Q}(\alpha)$ we have $\mathbb{Q}(\alpha^{n/r})\subset K$. For the rest of the proof we assume that $r>1$ holds.

Suppose that K is a subfield of $\mathbb{Q}(\alpha)$ with $K\cap\mathbb{Q}(\alpha^{n/r})=\mathbb{Q}$. We apply theorem 88 with the groups

$$\begin{aligned}
Z &= (\mathbb{Z}/n\mathbb{Z})^*\simeq\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}),\\
X &= \pi\big(\mathrm{Gal}\left(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q}(\alpha)\right)\big)\subset Z,\\
Q &= \rho'\big(\mathrm{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})\big)\subset\mathbb{Z}/r\mathbb{Z}\rtimes Z/X,\\
G &= \rho\big(\mathrm{Gal}(\mathbb{Q}(\zeta_n,\alpha)/\mathbb{Q})\big)\subset\mathbb{Z}/n\mathbb{Z}\rtimes(\mathbb{Z}/n\mathbb{Z})^*.
\end{aligned}$$

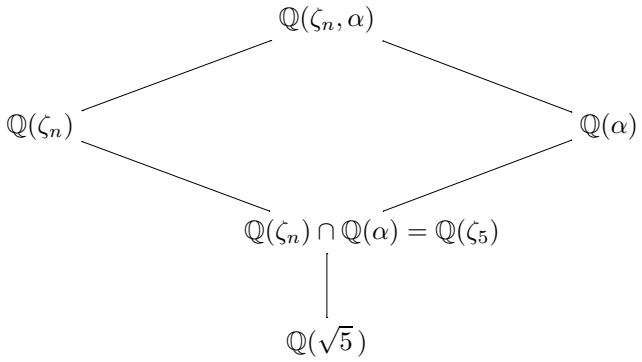
First we check that the groups above satisfy the conditions of theorem 88. By definition of the map ρ' we see that Q is isomorphic to Z/X and that G is the preimage of Q under the projection map $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{Z}/r\mathbb{Z} \rtimes Z/X$. theorem 85 shows that there does not exist a divisor $s > 1$ of r such that Q is contained in $s\mathbb{Z}/r\mathbb{Z} \rtimes Z/X$. As $K \cap \mathbb{Q}(\alpha^{n/r})$ equals $\mathbb{Q}$ the group H_K maps surjectively to $Z/X = \pi\big(\operatorname{Gal}(\mathbb{Q}(\alpha^{n/r})/\mathbb{Q})\big)$.

Now let f be an element of $\mathbb{Z}/n\mathbb{Z}$ and let g be an element of $(\mathbb{Z}/n\mathbb{Z})^*$ with $(f, g) \in H_K$. Assume that α satisfies condition (i). As $r > 1$ holds, the intersection $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha)$ is of degree 2 over $\mathbb{Q}$. By proposition 83 the group G is of the form $(A \times X) \cup (B \times Y)$, with A, B, X, Y as in proposition 89. The group X is not the kernel of the projection map $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/3\mathbb{Z})^*$ as otherwise we would have $\mu_3 \subset \mathbb{Q}(\zeta_n, \alpha)^X = \mathbb{Q}(\alpha)$, which implies that μ_3 is contained in $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^{n/r})$ and thus by lemma 69 we would have $\mu_3 \subset D_\alpha \cap \mu_n$. As μ_4 is not contained in $D_\alpha \cap \mu_n$, also X is not the kernel of the projection map $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/4\mathbb{Z})^*$. Therefore we can apply lemma 91 and we see that $\langle y + 1 \colon y \in Y \rangle$ is $2\mathbb{Z}/n\mathbb{Z}$ and proposition 89 proves that $(rf, 1) \in H_K$. Assume that α satisfies one of the conditions (ii), (iii) or (iv). By proposition 84 we have $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_r)$. Also in this case G is of the form $(A \times X) \cup (B \times Y)$, with A, B, X, Y as in proposition 89, where X is isomorphic to $\operatorname{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\alpha))$. The group X is isomorphic to $r\mathbb{Z}/n\mathbb{Z}$ and the set Y, by theorem 84, is $\{y \in (\mathbb{Z}/n\mathbb{Z})^* \text{ with } y = -1 \bmod r\}$. By lemma 92 we have $(rf, 1) \in H_K$ as r is even if n is even. If α satisfies condition (v), then lemma 93 shows $(rf, 1) \in H_K$.

We conclude that all conditions in theorem 88 are satisfied and thus H_K is of the form $(d\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*) \cap G$ for some divisor d of n. By lemma 86, we see that K is of the form $\mathbb{Q}(\alpha^d)$ for some divisor d of n. This completes the proof for subfields K of $\mathbb{Q}(\alpha)$ with $K \cap \mathbb{Q}(\alpha^{n/r}) = \mathbb{Q}$.

If α satisfies one of the conditions (i), (ii), (iii) or (iv) we have either $\mathbb{Q}(\alpha^{n/r}) \subset K$ or $K \cap \mathbb{Q}(\alpha^{n/r}) = \mathbb{Q}$ because $[\mathbb{Q}(\alpha^{n/r}) : \mathbb{Q}] = 2$. It remains to show that $K \cap \mathbb{Q}(\alpha^{n/r})$ is unequal to both $\mathbb{Q}$ and $\mathbb{Q}(\alpha^{n/r})$ which can only happen if α satisfies condition (v).

Assume that α satisfies condition (v) and let K be a subfield of $\mathbb{Q}(\alpha)$ with $K \cap \mathbb{Q}(\alpha^{n/r})$ not equal to both $\mathbb{Q}$ or $\mathbb{Q}(\alpha^{n/r}) = \mathbb{Q}(\zeta_5)$. Then we have $K \cap \mathbb{Q}(\alpha^{n/r}) = \mathbb{Q}(\sqrt{5}\,)$. Consider the following diagram.



We apply theorem 88 with

$$\begin{aligned} Z &\simeq \mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt{5}\,)\big), \\ X &= \pi(\mathrm{Gal}\big(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\alpha)\big) \subset Z \\ Q &= \rho'\big(\,\mathrm{Gal}(\mathbb{Q}(\alpha^{n/10})/\mathbb{Q}(\sqrt{5}\,))\big), \\ G &= \rho\big(\,\mathrm{Gal}(\mathbb{Q}(\zeta_n, \alpha)/\mathbb{Q}(\sqrt{5}\,))\big) \subset \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^* \end{aligned}$$

By definition of ρ' the group Q is a subgroup of $\mathbb{Z}/10\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*/X$. One easily checks that the ρ'-image of $\mathrm{Gal}(\mathbb{Q}(\alpha^{n/10})/\mathbb{Q}(\sqrt{5}\,))$ is contained in $\mathbb{Z}/10\mathbb{Z} \rtimes Z/X$. We will consider Q as a subgroup of $\mathbb{Z}/10\mathbb{Z} \rtimes Z/X$.

Similarly as before Z, X, Q and G satisfy the definitions in theorem 88 and H_K is a subgroup of G containing $\{0\} \rtimes X$ that surjects to Z/X. By lemma 93 we see that $(f, g) \in H_K$ implies that $(10f, 1) \in H_K$ for all $f \in \mathbb{Z}/n\mathbb{Z}$ and all $g \in Z$. It follows from theorem 88 that H_K equals $(d\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*) \cap G$ for some divisor d of n in this last case as well. We can literally copy the proof of lemma 86 to show that this group corresponds to the field $\mathbb{Q}(\alpha^{n/d})$. So, also all subfields K of $\mathbb{Q}(\alpha)/\mathbb{Q}$ with $K \cap \mathbb{Q}(\alpha^{n/r})$ not equal to both $\mathbb{Q}$ or $\mathbb{Q}(\alpha^{n/r})$ are generated by a power of α. □

Theorem 57 now easily follows:

Proof. The map ψ_α is surjective if and only if α satisfies one of the conditions (i), (ii), (iii), (iv) or (v) of theorem 56. In each of these cases we decide whether or not ψ_α is also injective.

Suppose that α satisfies condition (i). As $D_\alpha \cap \mu_n$ is contained in μ_2 it follows by minimality of n from lemma 68 that we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. For all divisors d of n we have $[\mathbb{Q}(\alpha^{n/d}) : \mathbb{Q}] = d$, therefore ψ_α is injective.

Suppose that α satisfies condition (ii). By corollary 82 the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is $2n/3$. We easily derive that $[\mathbb{Q}(\alpha^d) : \mathbb{Q}]$ is n/d if ζ_3 is not contained in $\mathbb{Q}(\alpha^d)$ and that $[\mathbb{Q}(\alpha^d) : \mathbb{Q}]$ is $2n/(3d)$ if ζ_3 is an element of $\mathbb{Q}(\alpha^d)$. Let $d, t \in \mathbb{Z}_{>0}$ such that $\mathbb{Q}(\alpha^d) = \mathbb{Q}(\alpha^t)$. If ζ_3 is an element of $\mathbb{Q}(\alpha^d)$ then we have $2n/3d = 2n/3t$ and thus d equals t. If ζ_3 is not contained in $\mathbb{Q}(\alpha^d)$ then $n/t = n/d$ and also in this case we have $d = t$. Hence the map ψ_α is injective.

Suppose that α satisfies condition (iii). Then we have the equality $\mathbb{Q}(\alpha^{n/4}) = \mathbb{Q}(\alpha^{n/2}) = \mathbb{Q}(i)$, hence ψ_α is not injective.

Suppose that α satisfies condition (iv). Then the fields $\mathbb{Q}(\alpha^{n/2})$ and $\mathbb{Q}(\alpha^{n/3})$ both equal $\mathbb{Q}(\zeta_3)$. We conclude that ψ_α is not injective.

Suppose that α satisfies condition (v). Then the elements $\alpha^{n/5}$ and $\alpha^{n/10}$ both generate the field $\mathbb{Q}(\zeta_5)$, and also in this case ψ_α is not injective. □

Chapter 3

Ramanujan's nested radicals

An application of the theory from the previous chapters can be found in denesting radicals. Let K be a field of characteristic 0 and let $\bar{K}$ be the algebraic closure of K. An element $\alpha \in \bar{K}$ can be represented by a radical expression if and only if the Galois group of the normal closure of $K(\alpha)$ over K is solvable ([22], chapter VI, theorem 7.2).

First we give some definitions.

Definition 95. Let K be a field and $\bar{K}$ some fixed algebraic closure of K. We denote by $K^{(0)}$ the field K itself and inductively define the fields $K^{(k)}$ for $k \geq 1$ as

$$K(\{\alpha \in \bar{K} \text{ with } \alpha^n \in K^{(k-1)} \text{ for some } n \in \mathbb{Z}_{>0}\}).$$

Definition 96. Let K be a field and let $\bar{K}$ be some fixed algebraic closure of K. We call $\alpha \in \bar{K}$ a *nested radical* if there exists some $t \in \mathbb{N}$ with $\alpha \in K^{(t)}$.

Definition 97. A nested radical is of *nesting depth* $n \in \mathbb{N}$ over a field K if n is the smallest integer for which this nested radical is contained in $K^{(n)}$.

Let K be a number field. The nesting depth of α in $\bar{K}$ is computable [7], although computing it is not easy in general. Susan Landau [20] gave an algorithm that constructs, for an element $\alpha \in \bar{K}$ with finite nesting depth, a representation of α in $K^{(r)}$ with $r \leq 1 + \text{nesting depth}(\alpha)$.

In this chapter we study nested radicals of the special form

$$\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}} \in \mathbb{Q}^{(2)}$$

for rationals α and β and give a necessary and sufficient condition for $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ to be *denestable*; that is, we show under what conditions $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ has nesting depth smaller than 2.

We prove the following theorem.

Theorem 98. *Let α, β be elements of $\mathbb{Q}^*$ such that β/α is not a cube in $\mathbb{Q}$. Then the following three statements are equivalent.*

(1) The nested radical $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ is contained in $\mathbb{Q}^{(1)}$.

(2) The polynomial $t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha} \in \mathbb{Q}[t]$ has a rational root.

(3) There exist integers m, n such that $\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}$ holds.

Radicals are often not unambiguously defined; the expression $\sqrt[3]{2}$, for example, can denote three different elements of $\mathbb{C}$. In this chapter we will consider nested radicals defined over $\mathbb{Q}$ and only take square roots and cube roots of real numbers. We fix the values for these expressions in $\mathbb{C}$ according to the following rules. Given a real number α, the expression $\sqrt[3]{\alpha}$ will represent the unique *real* cube root of α. When α is a positive real number then $\sqrt{\alpha}$ represents the *positive* square root of α. By i we denote a fixed primitive fourth root of unity in $\mathbb{C}$. If α is a negative real number then $\sqrt{\alpha}$ represents $i \cdot \sqrt{-\alpha}$.

3.1 The problem and its history

As for many subjects in number theory the history of denesting nested radicals leads us to Srinivasa Ramanujan (1887-1920). One of the questions he sent to the *Journal of the Indian Mathematical Society* was *Question 525* [28]:

> *Shew how to find the square roots of surds of the form $\sqrt[3]{A} + \sqrt[3]{B}$ and hence prove that*
>
> (i) $\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = \frac{1}{3}\left(\sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25}\right)$,
>
> (ii) $\sqrt{\sqrt[3]{28} - \sqrt[3]{27}} = \frac{1}{3}\left(\sqrt[3]{98} - \sqrt[3]{28} - 1\right)$.

In one of his notebooks [1], chapter 22, entry 23, we can find the theorem this question must have been based upon.

Theorem 99. *If m, n are arbitrary, then*

$$\sqrt{m\sqrt[3]{4(m-2n)} + n\sqrt[3]{4m+n}} = \pm\tfrac{1}{3}\left(\sqrt[3]{(4m+n)^2} + \sqrt[3]{4(m-2n)(4m+n)} - \sqrt[3]{2(m-2n)^2}\right). \quad (3.1)$$

Remark: In the examples in Ramanujan's notebook the theorem is only applied for integers m and n. We will consider rationals m, n, as we study denestability over the field $\mathbb{Q}$.

It is easy to verify that equation (3.1) holds for real numbers m and n by squaring both sides, but it is much harder to understand why it holds. However, for integers α and β with $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ contained in $\mathbb{Q}^{(1)}$ it is not clear at all whether or not there exist integers m and n as given in the theorem.

In section 3.3 we show that radicals of the form $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$, for rational numbers α and β with $\beta/\alpha \notin \mathbb{Q}^3$, are contained in $\mathbb{Q}^{(1)}$ if and only if the polynomial

$$F_{\beta/\alpha} = t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha}$$

has a rational root. Given α and β such that $F_{\beta/\alpha}$ has a rational root we express $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ in terms of this root. At the beginning of section 3.4 we prove that $F_{\beta/\alpha}$ has a rational root if and only if there exist integers m, n such that

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}.$$

Note that for rational numbers α and β with β/α a cube in $\mathbb{Q}$ the nested radical $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ is always contained in $\mathbb{Q}^{(1)}$: there exist $c \in \mathbb{Q}$ with $c^3 = \beta/\alpha$ and $d \in \mathbb{C}$ with $d^6 = \alpha$ such that we have $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}} = \pm d\sqrt{1+c}$. Theorem 98 therefore shows the generality of Ramanujan's formula.

Example 100. If the quotient β/α is a cube, then the statements (2) and (3) in theorem 98 are still equivalent, but the statements (1) and (2) are not equivalent. As remarked above for $\beta/\alpha \in \mathbb{Q}^{*3}$ statement (1) holds. However, if we have $\beta/\alpha = 1$, then the polynomial $t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha} = (t^2+2)(t^2+4t-2)$ has no rational roots.

There also exist α and β with $\beta/\alpha \in \mathbb{Q}^{*3}$ for which statement (2) does hold. For example if

$$\frac{\beta}{\alpha} = \frac{-7^3}{2^9} = \frac{(4\cdot -2+7)7^3}{4(-2-2\cdot 7)(-2)^3}$$

the polynomial $t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha}$ has two rational roots: $-7/4$ and $-7/2$.

At the end of section 3.4 we work out some examples and show, for integers α and β, that it is not possible in general to find integers m and n such that

$$\alpha = 4(m-2n)m^3 \text{ and } \beta = (4m+n)n^3$$

although there do exist m and n such that β/α equals $(4m+n)n^3/(4(m-2n)m^3)$.

3.2 Denesting condition

In this section we show that a nested radical of the form $\sqrt{\delta}$ for some δ in $\mathbb{Q}(\sqrt[3]{\gamma})$ with $\gamma \in \mathbb{Q}\setminus\mathbb{Q}^{*3}$ is contained in $\mathbb{Q}^{(1)}$ if and only if there exist $f \in \mathbb{Q}^*$ and $e \in \mathbb{Q}(\sqrt[3]{\gamma})$ such that δ equals $f \cdot e^2$.

We use the following notation. If $K/\mathbb{Q}$ is a field extension then K^{norm} denotes the normal closure of K over $\mathbb{Q}$. If G is a group then G' denotes the commutator subgroup of G and G'' denotes the group $(G')'$ and, as in chapter 2, we denote a primitive n-th root of unity by ζ_n.

Lemma 101. *Let γ be an element of $\mathbb{Q} \setminus \mathbb{Q}^3$, let δ be an element of $\mathbb{Q}(\sqrt[3]{\gamma}) \setminus \mathbb{Q}$ and let K be the field $\mathbb{Q}(\delta)^{\text{norm}} = \mathbb{Q}(\delta, \zeta_3)$. Let G be the group $\text{Gal}(\mathbb{Q}(\sqrt{\delta})^{\text{norm}}/\mathbb{Q})$ and let $\delta_1 = \delta, \delta_2, \delta_3$ be the conjugates of δ in $K/\mathbb{Q}$. Then the following implication holds*

$$G'' = \{1\} \implies \delta_2 \cdot \delta_3 \in K^{*2}.$$

Proof. Suppose that $\delta_2 \cdot \delta_3$ is not a square in K. Then $K(\sqrt{\delta_2 \cdot \delta_3})$ is an extension of degree 2 over K. As δ_1, δ_2 and δ_3 are conjugates, also $\delta_1 \cdot \delta_2$ and $\delta_1 \cdot \delta_3$ are non-squares in K. It follows that $\sqrt{\delta_1 \cdot \delta_2}$ is not contained in $K(\sqrt{\delta_2 \cdot \delta_3})$ as otherwise, by corollary 18, we have $\delta_1 \cdot \delta_3 \in K^2$.

Define L as the field $K(\sqrt{\delta_2 \cdot \delta_3}, \sqrt{\delta_1 \cdot \delta_2})$. We saw above that $[L : K]$ equals 4 and we get the following chain of field extensions

$$\begin{array}{c} L \\ \Big| {\scriptstyle V_4} \\ K \\ \Big| {\scriptstyle S_3} \\ \mathbb{Q}. \end{array}$$

This gives a contradiction with $G'' = \{1\}$ as we will see below.

Suppose that G'' equals $\{1\}$. First we remark that L is contained in $\mathbb{Q}(\sqrt{\delta})^{\text{norm}}$. Therefore we have $\text{Gal}(L/\mathbb{Q})'' \subset G'' = \{1\}$. There is an exact sequence

$$0 \longrightarrow \text{Gal}(L/K) \longrightarrow \text{Gal}(L/\mathbb{Q}) \longrightarrow \text{Gal}(K/\mathbb{Q}) \longrightarrow 0\ .$$

As $\text{Gal}(L/K) \simeq V_4$ is abelian, this gives an action of $\text{Gal}(K/\mathbb{Q}) \simeq S_3$ on $\text{Gal}(L/K)$ defined by the map

$$\text{Gal}(L/K) \times \text{Gal}(K/\mathbb{Q}) \longrightarrow \text{Gal}(L/K)$$

sending (v, σ) to $\tau v \tau^{-1} \in \text{Gal}(L/K)$ where τ is an element of $\text{Gal}(L/\mathbb{Q})$ with $\tau_{|_K} = \sigma$.

We remark that $\text{Gal}(L/K)$ is the group $\{1, \rho_1, \rho_2, \rho_1\rho_2\}$, where ρ_1 and ρ_2 are defined by

$$\begin{aligned} \rho_1 \colon \sqrt{\delta_2 \cdot \delta_3} &\mapsto -\sqrt{\delta_2 \cdot \delta_3} \\ \sqrt{\delta_1 \cdot \delta_2} &\mapsto \sqrt{\delta_1 \cdot \delta_2} \\ \sqrt{\delta_1 \cdot \delta_3} &\mapsto -\sqrt{\delta_1 \cdot \delta_3}, \end{aligned} \qquad \begin{aligned} \rho_2 \colon \sqrt{\delta_2 \cdot \delta_3} &\mapsto \sqrt{\delta_2 \cdot \delta_3} \\ \sqrt{\delta_1 \cdot \delta_2} &\mapsto -\sqrt{\delta_1 \cdot \delta_2} \\ \sqrt{\delta_1 \cdot \delta_3} &\mapsto -\sqrt{\delta_1 \cdot \delta_3}. \end{aligned}$$

The isomorphism from $\mathrm{Gal}(K/\mathbb{Q})$ to S_3 is given by the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the set of points $\delta_1, \delta_2, \delta_3$. Denote by π the map from $\mathrm{Gal}(L/\mathbb{Q})$ to $\mathrm{Gal}(K/\mathbb{Q})$ in the exact sequence above. When a, b and c in $\mathrm{Gal}(L/\mathbb{Q})$ are lifts under π of the maps corresponding to the elements $(12), (23)$ and (13) in S_3 then we have

$$\begin{aligned} a\rho_2 a^{-1}\rho_2^{-1} &= \rho_1 \\ b(\rho_1\rho_2)b^{-1}(\rho_1\rho_2)^{-1} &= \rho_2 \\ c\rho_1 c^{-1}\rho_1^{-1} &= \rho_1\rho_2 \end{aligned}$$

and thus $\mathrm{Gal}(L/K)$ is contained in $\mathrm{Gal}(L/\mathbb{Q})'$. As (123) equals $(13)(23)(13)(23)$ we see that the element $d = cbc^{-1}b^{-1} \in \mathrm{Gal}(L/\mathbb{Q})'$ is a lift under π of (123). As $\mathrm{Gal}(L/\mathbb{Q})'$ is abelian and $\mathrm{Gal}(L/K)$ is contained in $\mathrm{Gal}(L/\mathbb{Q})'$ we have $dvd^{-1}v^{-1} = 1$ for all $v \in \mathrm{Gal}(L/K)$. This gives a contradiction as $d\rho_1 d^{-1}(\sqrt{\delta_2 \cdot \delta_3}\,)$ equals $\sqrt{\delta_2 \cdot \delta_3}$. We conclude that $\delta_2 \cdot \delta_3$ is a square in K. □

Theorem 102. *Let γ be an element of $\mathbb{Q} \setminus \mathbb{Q}^3$ and let δ be an element of $\mathbb{Q}(\sqrt[3]{\gamma}\,)$. Denote by G the Galois group of the normal closure of $\mathbb{Q}(\sqrt{\delta}\,)$ over $\mathbb{Q}$. Then the following are equivalent:*

(1) The element $\sqrt{\delta}$ is contained in $\mathbb{Q}^{(1)}$.

(2) The group G'' is $\{1\}$.

(3) There exist $f \in \mathbb{Q}^*$ and $e \in \mathbb{Q}(\delta)$ such that $\delta = f \cdot e^2$.

Proof. Implication (3) ⇒ (1) is trivial.

If $\sqrt{\delta}$ is an element of $\mathbb{Q}^{(1)}$ then there exist $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ and a positive integer n with $\alpha_i^n \in \mathbb{Q}$ for all i such that $\sqrt{\delta}$ is contained in $\mathbb{Q}(\zeta_n, \alpha_1, \ldots, \alpha_k)$. Let L denote the field $\mathbb{Q}(\zeta_n, \alpha_1, \ldots, \alpha_k)$. As both $L/\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ are abelian extensions, the second derived subgroup $\mathrm{Gal}(L/\mathbb{Q})''$ of $\mathrm{Gal}(L/\mathbb{Q})$ is trivial. Now the normal closure of $\mathbb{Q}(\sqrt{\delta}\,)$ over $\mathbb{Q}$ is contained in L and hence also the second derived subgroup of its Galois group is trivial.

If δ is a rational number then implication (2) ⇒ (3) is trivial. Assume that δ is not contained in $\mathbb{Q}$ and let K be $\mathbb{Q}(\delta, \zeta_3)$. Assume that G'' is $\{1\}$. Let $\delta_1 = \delta, \delta_2, \delta_3$ be the conjugates of δ in K. In the previous lemma we showed that $\delta_2 \cdot \delta_3 \in K^2$. Now let η be an element of K with $\eta^2 = \delta_2 \cdot \delta_3$.

Suppose that η is not contained in $\mathbb{Q}(\delta)$. As $\delta_2 \cdot \delta_3$ is an element of $\mathbb{Q}(\delta)$ and K is $\mathbb{Q}(\delta, \sqrt{-3}\,)$ we see by corollary 18 that $\delta_2 \cdot \delta_3$ equals $-3 \cdot \theta^2$ for some θ in $\mathbb{Q}(\delta)$. It follows

$$N_{\mathbb{Q}}^{\mathbb{Q}(\delta)}(\eta)^2 = N_{\mathbb{Q}}^{\mathbb{Q}(\delta)}(\delta_2) \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\delta)}(\delta_3) = -27 \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\delta)}(\theta)^2.$$

As we have $-27 \notin \mathbb{Q}^2$ this gives a contradiction, so η is an element of $\mathbb{Q}(\delta)$. We have

$$\delta = \frac{\delta_1 \cdot \delta_2 \cdot \delta_3}{\delta_2 \cdot \delta_3} = N_{\mathbb{Q}}^{\mathbb{Q}(\delta)}(\delta) \cdot \eta^{-2}$$

and take $f = N_{\mathbb{Q}}^{\mathbb{Q}(\delta)}(\delta)$ and $e = \eta^{-1}$. □

3.3 A special polynomial

Given the nested radical $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ we define a polynomial $F_{\beta/\alpha}$ depending on α and β.

Definition 103. Let α, β be elements of $\mathbb{Q}^*$. The polynomial $F_{\beta/\alpha} \in \mathbb{Q}[t]$ is defined by

$$F_{\beta/\alpha} = t^4 + 4t^3 + 8\frac{\beta}{\alpha}t - 4\frac{\beta}{\alpha}.$$

In this section we show that $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ is contained in $\mathbb{Q}^{(1)}$ if and only if the polynomial $F_{\beta/\alpha}$ has a rational root. In the previous section we saw that the radical

$$\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}} = \pm\sqrt{\sqrt[3]{\alpha}}\cdot\sqrt{1+\sqrt[3]{\beta/\alpha}}$$

is contained in $\mathbb{Q}^{(1)}$ if and only if there exist $f \in \mathbb{Q}^*$ and $e \in \mathbb{Q}(\sqrt[3]{\beta/\alpha})$ such that $1+\sqrt[3]{\beta/\alpha} = f\cdot e^2$. In theorem 104 we write e on the basis $1, \sqrt[3]{\beta/\alpha}, \sqrt[3]{\beta/\alpha}^2$ of $\mathbb{Q}(\sqrt[3]{\beta/\alpha})$ as a vector space over $\mathbb{Q}$ and compare the coefficients in the resulting equation to obtain $F_{\beta/\alpha}$. At the end of the section we provide some examples.

Theorem 104. *Let α, β be elements of $\mathbb{Q}^*$ such that β/α is not a cube in $\mathbb{Q}$. The nested radical*

$$\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$$

is contained in $\mathbb{Q}^{(1)}$ if and only if the polynomial $F_{\beta/\alpha}$ has a root in $\mathbb{Q}$.

Proof. The radical $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ is contained in $\mathbb{Q}^{(1)}$ if and only if $\sqrt{1+\sqrt[3]{\beta/\alpha}}$ is contained in $\mathbb{Q}^{(1)}$. By theorem 102, this holds if and only if there exist $f \in \mathbb{Q}$ and $x, y, z \in \mathbb{Q}$ with

$$1+\sqrt[3]{\beta/\alpha} = f\left(x + y\sqrt[3]{\beta/\alpha} + z\sqrt[3]{(\beta/\alpha)^2}\right)^2.$$

The elements $1, \sqrt[3]{\beta/\alpha}$ and $\sqrt[3]{(\beta/\alpha)^2}$ are linearly independent over $\mathbb{Q}$. Therefore coefficients of like powers on both sides must be equal. This leads to the following equations:

$$\frac{1}{f} = x^2 + 2yz\frac{\beta}{\alpha}, \tag{3.2}$$

$$0 = y^2 + 2xz, \tag{3.3}$$

$$\frac{1}{f} = \frac{\beta}{\alpha}z^2 + 2xy. \tag{3.4}$$

We may assume that $z \neq 0$ (since $z = 0$ implies $y = 0$ and this gives a contradiction in (3.4)). Substitution of

$$\frac{x}{z} = -\frac{1}{2}\left(\frac{y}{z}\right)^2,$$

in (3.2) and (3.4) yields

$$\left(\frac{y}{z}\right)^4 + 8\frac{\beta}{\alpha}\frac{y}{z} = \frac{4}{f \cdot z^2},$$

$$\left(\frac{y}{z}\right)^3 = \frac{\beta}{\alpha} - \frac{1}{f \cdot z^2}.$$

The combination of the above two equalities leads to the following quartic equation in y/z

$$\left(\frac{y}{z}\right)^4 + 4\left(\frac{y}{z}\right)^3 + 8\frac{\beta}{\alpha}\left(\frac{y}{z}\right) - 4\frac{\beta}{\alpha} = 0.$$

So, if $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ is contained in $\mathbb{Q}^{(1)}$ then $F_{\beta/\alpha}$ has a rational root.

For the other implication we assume that a rational root s of $F_{\beta/\alpha}$ is given. We use the relations

$$s = \frac{y}{z}, \quad \frac{x}{z} = -\frac{1}{2}\left(\frac{y}{z}\right)^2 \quad \text{and} \quad \left(\frac{y}{z}\right)^3 = \frac{\beta}{\alpha} - \frac{1}{f \cdot z^2}$$

that we derived above and find

$$\begin{aligned}
\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}} &= \pm\sqrt{z^2 \cdot f \cdot \sqrt[3]{\alpha}}\left(-\tfrac{1}{2}\left(\tfrac{y}{z}\right)^2 + \tfrac{y}{z}\sqrt[3]{\beta/\alpha} + \sqrt[3]{(\beta/\alpha)^2}\right) \\
&= \pm\sqrt{z^2 \cdot f \cdot \sqrt[3]{\alpha}}\left(-\tfrac{1}{2}s^2 + s\sqrt[3]{\beta/\alpha} + \sqrt[3]{(\beta/\alpha)^2}\right) \\
&= \pm\frac{1}{\sqrt{\beta - s^3\alpha}}\left(-\tfrac{1}{2}s^2\sqrt[3]{\alpha^2} + s\sqrt[3]{\alpha\beta} + \sqrt[3]{\beta^2}\right). \qquad (3.5)
\end{aligned}$$

So $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$ is an element of $\mathbb{Q}^{(1)}$ if and only if $F_{\beta/\alpha}$ has a rational root. □

Corollary 105. *Let α, β be elements of $\mathbb{Q}^*$, such that β/α is not a cube in $\mathbb{Q}$. Then the nested radical*

$$\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}}$$

is contained in $\mathbb{Q}^{(1)}$ if and only if there exists an element $s \in \mathbb{Q}$ such that

$$\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}} = \pm\frac{1}{\sqrt{t}}\left(-\tfrac{1}{2}s^2\sqrt[3]{\alpha^2} + s\sqrt[3]{\alpha\beta} + \sqrt[3]{\beta^2}\right),$$

where $t = \beta - s^3\alpha$.

We give some examples.

Example 106. We compute the rational roots of $F_{-4/5}$ and $F_{-27/28}$ to derive the equalities (i) and (ii) from section 3.1. As we have

$$F_{-4/5}(-2) = F_{-27/28}(-3) = 0,$$

we find the equalities

$$\begin{aligned}\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} &= \frac{1}{\sqrt{36}}\left(-2\sqrt[3]{25} + 2\sqrt[3]{20} + 2\sqrt[3]{2}\right) \\ &= \tfrac{1}{3}\left(-\sqrt[3]{25} + \sqrt[3]{20} + \sqrt[3]{2}\right)\end{aligned}$$

and

$$\begin{aligned}\sqrt{\sqrt[3]{28} - \sqrt[3]{27}} &= -\frac{1}{\sqrt{27^2}}\left(-\tfrac{9}{2}\sqrt[3]{28^2} - 3\sqrt[3]{-27\cdot 28} + \sqrt[3]{27^2}\right) \\ &= -\tfrac{1}{3}\left(-\sqrt[3]{98} + \sqrt[3]{28} + 1\right).\end{aligned}$$

Example 107. The nested radicals do not have to be real. For example, when we take $\alpha = -2^7$ and $\beta = 7$ we get

$$\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}} = \sqrt{-4\sqrt[3]{2} + \sqrt[3]{7}}.$$

For these α and β we have the polynomial

$$F_{-7/2^7} = t^4 + 4t^3 - \frac{56}{2^7}t + \frac{28}{2^7},$$

with rational root $-1/2$. Substituting this in equation (3.5) gives

$$\begin{aligned}\sqrt{-4\sqrt[3]{2} + \sqrt[3]{7}} &= \pm\frac{1}{\sqrt{7-16}}\left(-\tfrac{1}{8}\sqrt[3]{2^{14}} - \tfrac{1}{2}\sqrt[3]{-7\cdot 2^7} + \sqrt[3]{49}\right) \\ &= \pm i\cdot\tfrac{1}{3}\left(-2\sqrt[3]{4} + 2\sqrt[3]{14} + \sqrt[3]{49}\right).\end{aligned}$$

Example 108. Until now, we only considered nested radicals for which both α and β were integers. Now let $\alpha = 2$ and $\beta = -1/2$, then $\beta/\alpha = -1/4$. The rational root of $F_{-1/4}$ is -1. This leads to the equality

$$\sqrt{\sqrt[3]{2} - \sqrt[3]{1/2}} = \frac{1}{\sqrt{3/2}}\left(-\tfrac{1}{2}\sqrt[3]{4} - \sqrt[3]{-1} + \sqrt[3]{1/4}\right),$$

which we simplify to

$$\sqrt{\sqrt[3]{2} - \sqrt[3]{1/2}} = \frac{\sqrt{2}}{\sqrt{3}}\left(1 + \tfrac{1}{2}\sqrt[3]{2} - \tfrac{1}{2}\sqrt[3]{4}\right).$$

3.4 Comparison to Ramanujan's method

In this section we derive equation (3.1) from equation (3.5). We show in theorem 109 that integers m and n that satisfy

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}$$

give a rational root n/m of $F_{\beta/\alpha}$. Conversely, if s is a rational root of $F_{\beta/\alpha}$ and $s = r/t$ for integers r and t, then we can take $n = r$ and $m = t$ and the equality above holds. Theorem 98 follows directly from it. Moreover we show that there are $\alpha, \beta \in \mathbb{Q}$ with $\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}} \in \mathbb{Q}^{(1)}$ for which there do not exist rational numbers m and n with $\alpha = 4(m-2n)m^3$ and $\beta = (4m+n)n^3$.

Theorem 109. *Let α, β be elements of $\mathbb{Q}^*$ such that β/α is not a cube in $\mathbb{Q}$. Let s be a rational number. Then s is a root of the polynomial $F_{\beta/\alpha}$ if and only if there exist integers m, n such that $s = n/m$ with*

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}.$$

Proof. Let s be a rational root of $F_{\beta/\alpha}$. Then we have

$$s^4 + 4s^3 + 8\frac{\beta}{\alpha}s - 4\frac{\beta}{\alpha} = 0,$$

so $s^3(s+4)$ equals $4(1-2s)\beta/\alpha$. Remark that $s \neq 1/2$ as $F_{\beta/\alpha}(1/2) = 9/16$. We see that s is a rational root of $F_{\beta/\alpha}$ if and only if the equality

$$\frac{\beta}{\alpha} = \frac{s^3(s+4)}{4(1-2s)}$$

holds. Writing $s = n/m$ for integers n, m gives

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}$$

which proves the theorem. □

Suppose that there exist integers m and n with $F_{\beta/\alpha}(n/m) = 0$ and

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}.$$

Then there exists some $c \in \mathbb{Q}^*$ with $\alpha = c \cdot 4(m-2n) \cdot m^3$ and $\beta = c \cdot (4m+n) \cdot n^3$. We use equation (3.5) to derive equation (3.1); by theorem 109 we have $s = n/m$.

$$\begin{aligned}
\sqrt{\sqrt[3]{\alpha} + \sqrt[3]{\beta}} &= \pm\frac{1}{\sqrt{\beta - s^3\alpha}} \left(-\tfrac{1}{2}s^2\sqrt[3]{\alpha^2} + s\sqrt[3]{\alpha\beta} + \sqrt[3]{\beta^2}\right) \\
&= \pm\frac{1}{\sqrt{9 \cdot c \cdot n^4}} \left(-\tfrac{1}{2} \cdot \tfrac{n^2}{m^2} \cdot m^2 \sqrt[3]{(4(m-2n))^2 \cdot c^2}\right. \\
&\quad \left. + \tfrac{n}{m} \cdot nm \sqrt[3]{4(m-2n)(4m+n) \cdot c^2} + n^2 \sqrt[3]{(4m+n)^2 \cdot c^2}\right) \\
&= \pm\frac{\sqrt[3]{c^2}}{3\sqrt{c}} \left(-\sqrt[3]{2(m-2n)^2} + \sqrt[3]{4(m-2n)(4m+n)}\right. \\
&\quad \left. + \sqrt[3]{(4m+n)^2}\right) \qquad (3.6)
\end{aligned}$$

If we take $c = 1$ in equation 3.6, this gives equation 3.1 again.

In the case that both α and β are integers the question arises if there always exist integers m, n such that

$$\beta = (4m+n)n^3 \quad \text{and} \quad \alpha = 4(m-2n)m^3.$$

Unfortunately, this is not the case as the examples 111 and 112 show.

Lemma 110. *Let α and β be elements of $\mathbb{Q}^*$ and let m and n be integers with*

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}.$$

Let a and b be coprime integers with $\beta/\alpha = b/a$. Then we have both

$$\left(\frac{n}{\gcd(m,n)}\right)^3 \Big| 4b \qquad \text{and} \qquad \left(\frac{m}{\gcd(m,n)}\right)^3 \Big| a.$$

Proof. Let a and b be coprime integers with $\beta/\alpha = b/a$. If we take $d = \gcd(m,n)$ then also the quotient of $(4m/d+n/d)(n/d)^3$ and $4(m/d-2n/d)(m/d)^3$ equals β/α. Now replace m by m/d and replace n by n/d. Then $\gcd(m,n) = 1$ and we have

$$(4m+n)n^3 \cdot a = 4(m-2n)m^3 \cdot b,$$

where also $\gcd(a,b) = 1$. If p is a prime diving m, then p does not divide $(4m+n)n^3$. Similarly, if p is a prime dividing n, then p does not divide $(m-2n)m^3$. Hence m^3 is a divisor of a and n^3 is a divisor of $4b$. □

Example 111. Let us look at the nested radical $\sqrt{\sqrt[3]{5} - \sqrt[3]{4}}$ from example 106 again. When we take $\alpha = -4$ and $\beta = 5$, we see that for $m = n = 1$ we have $\alpha = 4(m-2n)m^3$ and $\beta = (4m+n)n^3$. So, again we find the equality

$$\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = -\tfrac{1}{3}\left(\sqrt[3]{25} - \sqrt[3]{20} - \sqrt[3]{2}\right).$$

However, when we take $\alpha = 5$ and $\beta = -4$, which is a more obvious thing to do, there do not exist integers, or even rational numbers, m and n with $\alpha = 4(m-2n)m^3$ and $\beta = (4m+n)n^3$, although we have

$$\frac{\beta}{\alpha} = \frac{(-4+2)2^3}{4(-1-4)(-1)^3}.$$

Example 112. Now look at

$$\sqrt{5\sqrt[3]{7}-8}.$$

For this nested radical, for each of the choices $\alpha = \pm 7 \cdot 5^3$ and $\alpha = \pm 8^3$, we are not able to find integers m, n such that $\alpha = (4m+n)n^3$ and $\beta = 4(m-2n)m^3$, although we have

$$-\frac{7 \cdot 5^3}{8^3} = \frac{(16+5)5^3}{4(4-10)4^3} \qquad \text{and} \qquad -\frac{8^3}{7 \cdot 5^3} = \frac{(-20+8)8^3}{4(-5-16)(-5)^3}.$$

To give $\sqrt{5\sqrt[3]{7}-8}$ as an element of $\mathbb{Q}^{(1)}$, we take $\alpha = -8^3$ and $\beta = 7 \cdot 5^3$ and use the equality

$$\frac{\beta}{\alpha} = \frac{7 \cdot 5^3}{-8^3} = \frac{(16+5)5^3}{4(4-10)4^3}.$$

As the quotient of α and $4(4-10)4^3$ is 3, we see that

$$\sqrt{\sqrt[3]{3}}\,\sqrt{-8+5\sqrt[3]{7}} = \sqrt{4\sqrt[3]{4(4-10)}+5\sqrt[3]{16+5}}.$$

Using equation (3.6) with $c = \frac{1}{3}$ we find

$$\sqrt{8-5\sqrt[3]{7}} = \frac{\sqrt[3]{3}}{3\sqrt{3}}\left(-\sqrt[3]{21^2}+2\sqrt[3]{63}+2\sqrt[3]{9}\right).$$

Finally, one could wonder, as Ramanujan's formula (3.1) lacks obvious symmetry, what happens if the roles of α and β interchange. The answer is that we find the same simplification, putting $p = -n/\sqrt{2}$ and $q = m\sqrt{2}$. (This explains why in example 111 we were not able to find integers m and n such that $\alpha = 4(m-2n)m^3$ and $\beta = (4m+n)n^3$ for the choice $\alpha = 5$ and $\beta = -4$.) If we define $p = -n/\sqrt{2}$ and $q = m\sqrt{2}$, it holds that

$$\begin{aligned} \alpha &= 4(m-2n)m^3 = (4p+q)q^3 \\ \beta &= (4m+n)n^3 = 4(p-2q)p^3. \end{aligned}$$

Since we have

$$\begin{aligned} (4m+n)^2 &= \left(2\sqrt{2}q-\sqrt{2}p\right)^2 = 2(p-2q)^2 \\ 2(m-2n)^2 &= 2\left(\tfrac{1}{2}q^2+4pq+8p^2\right) = (4p+q)^2 \\ 4(m-2n)(4m+n) &= 4\left(2q^2+7pq-4p^2\right) = -4(p-2q)(4p+q), \end{aligned}$$

we may replace m and n simply by p and q in the right hand side of Ramanujan's formula:

$$\sqrt{\sqrt[3]{\beta}+\sqrt[3]{\alpha}}=\pm\tfrac{1}{3}\left(-\sqrt[3]{(4p+q)^2}-\sqrt[3]{4(p-2q)(4p+q)}+\sqrt[3]{2(p-2q)^2}\right).$$

Chapter 4

Nested radicals of depth one

Borodin, Fagin, Hopcroft and Tompa [5] gave conditions for the nested radical $\sqrt{a+b\sqrt{r}} \in F^{(2)}$ to be an element of $F^{(1)}$, for a real field F and a, b, r elements of F. In the previous chapter we gave conditions for $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$, with α and β in $\mathbb{Q}$, to be an element of $\mathbb{Q}^{(1)}$ and more generally we proved theorem 102. We would like to have a general condition for elements of $K^{(2)}$ to be contained in $K^{(1)}$, where K is a field of characteristic 0.

Richard Zippel [40] formulated the following conjecture for denesting radicals of nesting depth 2 that consist of one term.

Definition 113. Let K be a field and let L/K be a radical extension. We say that L/K is a *simple radical extension* if there is an element γ in L with minimal polynomial $x^r - \gamma^r$ for some $r \in \mathbb{Z}_{>0}$ such that $L = K(\gamma)$.

Conjecture 114 (Zippel). *Let K be a field of characteristic 0 and let $\bar{K}$ be a fixed algebraic closure of K. Let $\alpha_1, \ldots, \alpha_k$ in $\bar{K}^*$ be such that there exist positive integers $d_1, \ldots, d_k$ with $\alpha_1^{d_1}, \ldots, \alpha_k^{d_k} \in K$. Define L as the field $K(\alpha_1, \ldots, \alpha_k)$.*

Let F be a composite of simple radical extensions over K. Let δ be an element of L and let n be a positive integer. If $\sqrt[n]{\delta}$ is an element of the composite LF, then there exist integers $s_1, \ldots, s_k$ and an element w of K such that the product $\alpha_1^{s_1} \cdots \alpha_k^{s_k} \cdot w \cdot \delta$ is an element of L^{*n}.

In example 117, section 4.1, we show that the conjecture is false. In proving denesting conditions, most of the difficulties are caused by adjoining roots of unity in a field extension. In example 117 we consider a field extension generated by a root of unity in which we find a nested radical of depth 2 over $\mathbb{Q}$ that violates conjecture 114.

So, it is not sufficient that our field extension is a composite of simple radical extensions; we need something stronger. In this chapter we denote for positive integers n a primitive n-th root of unity by ζ_n. Let K be a field of characteristic 0

and let $\alpha \in \bar{K}$ be such that $\alpha^t \in K$ for some integer t. If the minimal polynomial of α over K is not of the form $x^n - \alpha^n$ for some $n \in \mathbb{Z}_{>0}$, then $K(\alpha) \setminus K$ contains roots of unity. In the reformulation of conjecture 114 we therefore give a condition on the roots of unity in the extension F/K instead of demanding that F is a composite of simple radical extensions.

If for some odd prime p the root of unity ζ_p is contained in K, then for all $r \in \mathbb{Z}_{>0}$ the extension $K(\zeta_{p^r})/K$ is cyclic and the minimal polynomial of ζ_{p^r} is of the form $x^n - a$ for some $n \in \mathbb{Z}_{>0}$ and some $a \in K$. So, adjoining a p^r-th root of unity to a field K with $\zeta_p \in K$ gives a simple radical extension. The same holds for adjoining ζ_{2^r} for some integer r if i is contained in K. So, if a radical extension is simple, it is pure (definition 61) as well. For a composite of radical extensions this is not necessarily true. In section 4.2 we prove Zippel's conjecture for pure extensions.

Theorem 115. *Let K, L and $\alpha_1, \ldots, \alpha_k$ be defined as in conjecture 114.*

Assume that L/K is pure. Let n be a positive integer, let δ be an element of L and let F be a pure radical extension of K with $F \subset K^{(1)}$. If we have $\beta \in F$ with $\beta^n = \delta$, then there exist elements $w \in K$ and $e \in L$ and integers $s_1, \ldots, s_k$ such that δ is equal to $w \cdot e^n \cdot \prod_i \alpha_i^{s_i}$.

Another way to make sure that the minimal polynomials of the generating radicals α are of the form $x^n - \alpha^n$ for some positive integer n is to adjoin all roots of unity to the ground field. We define $K_\infty = K(\mu(\bar{K}))$ for a fixed algebraic closure $\bar{K}$ of K.

Inspired by Zippel's idea we formulate for a field K a condition for elements of $K^{(2)}$ to be contained in $K^{(1)}$.

Theorem 116. *Let K, L and $\alpha_1, \ldots, \alpha_k$ be defined as in conjecture 114.*

Let δ be an element of L and let n be a positive integer. If there exists a field $F \subset K^{(1)}$ and an element $\beta \in F$ such that $\beta^n = \delta$, then there exist elements $w \in K_\infty \cap L$ and $e \in L$ and integers $s_1, \ldots, s_k$ such that δ is equal to $w \cdot e^n \cdot \prod_i \alpha_i^{s_i}$.

This theorem we will prove in section 4.3.

4.1 Counterexample to Zippel's conjecture

In the introduction of this chapter we gave a conjecture due to Richard Zippel. He gives a condition for the existence of a special kind of denesting of radical expressions of the form $\sqrt[n]{\delta}$ for some $n \in \mathbb{Z}_{>0}$ and some δ in $K^{(1)}$. This denesting is required to be an element of some composite of simple radical extensions.

To construct a counterexample to conjecture 114 we first forget about the condition on the field F. A well known radical equation is

$$\sqrt{1 + \sqrt{-1}} = \sqrt[8]{-4}.$$

If we take, in conjecture 114, ground field $\mathbb{Q}$, $L = \mathbb{Q}(i)$, $\delta = 1 + i$ and $n = 2$ then we see that there exists a denesting $\sqrt[8]{-4}$ in $\mathbb{Q}(i) \cdot \mathbb{Q}(\sqrt[8]{-4})$. But there do not exist $s \in \mathbb{Z}$ and $w \in \mathbb{Q}$ such that

$$w \cdot i^s \cdot (1 + i)$$

is a square in $\mathbb{Q}(\sqrt{-1})$; the norm of $w \cdot i^s \cdot (1 + i)$ is $2 \cdot w^2$ and this is not a square in $\mathbb{Q}$. So, without the extra condition on F the conjecture does not hold. However, we can embed $\mathbb{Q}(\sqrt[8]{-4})$ in a composite of simple radical extensions as we will see in example 117. This directly gives a counterexample to the conjecture itself.

Example 117. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\delta = 1+i$, $n = 2$ and define $F = \mathbb{Q}(\sqrt[8]{2}, \sqrt[8]{-2})$. As both $\mathbb{Q}(\sqrt[8]{2})$ and $\mathbb{Q}(\sqrt[8]{-2})$ are simple radical extensions, F is of the form required in conjecture 114. But similarly as before, there do not exist $s \in \mathbb{Z}$ and $w \in \mathbb{Q}$ such that $w \cdot i^s \cdot (1 + i)$ is a square in $\mathbb{Q}(\sqrt{-1})$.

In my opinion, the field F in this example clearly is not of the form that Zippel had in mind for the conjecture. Probably he wanted his conjecture to give a condition for denesting nested radicals of depth two consisting of one term without using roots of unity in the denesting. That is, without using any other roots of unity than those already contained in the ground field.

4.2 Denesting without roots of unity

In this section we give some condition for denesting without roots of unity. First we have to define what we mean by this. Assume that K is a field of characteristic zero and let L be a subfield of $K^{(1)}$ with $[L : K]$ finite. Let δ be some element of L. A denesting of $\sqrt[n]{\delta}$ is a denesting without roots of unity if we can find an element β in some pure subextension F of $K^{(1)}/K$ with $\beta^n = \delta$.

Below we use theorem 58 to prove a statement for non-Kummer extensions similar to corollary 18. The only extra condition is that the extension is pure.

Proposition 118. *Let K be a field of characteristic 0 and let $\bar{K}$ be a fixed algebraic closure of K. Let $\alpha, \alpha_1, \ldots \alpha_k \in \bar{K}^*$ be such that there exist natural numbers $n, d_1, \ldots, d_k$ with $\alpha^n, \alpha_1^{d_1}, \ldots \alpha_k^{d_k} \in K$. Let L be the field $K(\alpha, \alpha_1, \ldots \alpha_k)$. If L/K is a pure extension then α is an element of $K\big(\alpha_1, \ldots, \alpha_k\big)$ if and only if there exist $b \in K^*$ and $l_1, \ldots l_k \in \mathbb{N}$ such that α can be written in the form*

$$\alpha = b \cdot \prod_{i=1}^{k} \alpha_i^{l_i}.$$

Proof. Take groups $C_1 = \langle K^*, \alpha_i (i \in I) \rangle$ and $C_2 = \langle K^*, \alpha, \alpha_i (i \in I) \rangle$. Then we have $L = K(C_1) = K(C_2)$. As the extension L/K is pure, both C_1 and C_2 satisfy the conditions R_1 and R_2 from theorem 58. We conclude that the index $(C_1 : K^*)$

equals the index $(C_2 : K^*)$. As C_1 is contained in C_2 the groups are equal. The element α therefore is contained in C_1, hence we have

$$\alpha = b \cdot \prod_{i=1}^{k} \alpha_i^{l_i},$$

for an element b of K^* and integers $l_1, \ldots, l_k$.

If α is of the above form, then clearly α is an element of $K(\alpha_1, \ldots, \alpha_k)$. □

We apply this proposition and the theory of cogalois extensions described in section 2.1 to prove theorem 115.

Proof. Let β be an element of F with $\beta^n = \delta$. We consider the following diagram

$$\begin{array}{c} F \\ | \\ L \cap F \\ | \\ K. \end{array}$$

As F/K is a pure extension, both the extensions $F/(L \cap F)$ and $(L \cap F)/K$ are pure as well. As F is a radical extension contained in $K^{(1)}$ there are radicals $\gamma_1, \ldots, \gamma_t$ in F and integers $n_1, \ldots, n_t$ with $\gamma_i^{n_i} \in K$ for all i in $\{1, \ldots, t\}$, such that the γ_i generate F over $L \cap F$. We apply proposition 118 with ground field $L \cap F$ and α equal to β. This gives us an element $b \in (L \cap F)^*$ and integers $l_1, \ldots, l_t$ with

$$\beta = b \cdot \prod_{i=1}^{t} \gamma_i^{l_i}.$$

So, there exists some γ in F with $\gamma^m \in K$ for some positive integer m, such that β equals $b \cdot \gamma$. Raising both sides of the equation to the power n gives $\delta = b^n \cdot \gamma^n$. As both δ and b are elements of $L \cap F$, also γ^n is an element of $L \cap F$. As a subextension of the pure extension $L = K(\alpha_1, \ldots, \alpha_k)/K$, by proposition 62, also $(L \cap F)/K$ is a radical extension generated by monomials in $\alpha_1, \ldots, \alpha_k$. We apply proposition 118 again, this time with ground field K and α equal to γ^n. We find an element c in K^* and integers $s_1, \ldots, s_k$ with

$$\gamma^n = c \cdot \prod_{i=1}^{k} \alpha_i^{s_i}.$$

Hence we have

$$\delta = b^n \cdot \gamma^n = b^n \cdot c \cdot \prod_{i=1}^{k} \alpha_i^{s_i},$$

for some b in $(L \cap F)^* \subset L^*$, some $c \in K^*$ and integers $s_1, \ldots, s_k$. □

4.3 Denesting allowing roots of unity

Let K be a field of characteristic 0. Let n be a positive integer and let δ be an element of $K^{(1)}$. In theorem 116 we give a necessary condition for the nested radical $\sqrt[n]{\delta}$ to be of depth at most one. We first prove this theorem, next we derive some results in special cases, and finally we give an example that shows that the condition in this theorem in general is not sufficient.

Proof of theorem 116. Let δ be an element of L and let n be a positive integer. Assume that there exist some field $F \subset K^{(1)}$ and some β in F with $\beta^n = \delta$. Then, there exists a field $L_\infty \subset L' \subset LK^{(1)}$ of finite degree over L_∞ with β in L' that is generated by radicals of depth 1 over K; that is L' equals $L_\infty(\gamma_1, \ldots, \gamma_l)$ for elements $\gamma_i \in \bar{K}^*$ for which there exist positive integers $m_1, \ldots, m_l$ with $\gamma_i^{m_i} \in K^*$ for all i. Applying corollary 18 with ground field L_∞ and α equal to β gives

$$\beta \in \gamma \cdot L_\infty,$$

for an element γ of $\bar{K}^*$ satisfying $\gamma^m \in K^*$ for some m in $\mathbb{Z}_{>0}$.

We now study the action of elements of $\mathrm{Gal}\left(L_\infty(\gamma)/L\right)$ on β. A basis of L_∞ over K_∞ is given by a subset $c_1, \ldots, c_s$ of the basis of the extension L/K. There are unique $a_1, \ldots, a_s$ in K_∞ such that we have

$$\beta = \gamma(a_1c_1 + \cdots + a_sc_s).$$

Let σ be an element of $\mathrm{Gal}(L_\infty(\gamma)/L)$, then we have

$$\frac{\sigma(\beta)}{\sigma(\gamma)} = \sigma(a_1)c_1 + \cdots \sigma(a_s)c_s.$$

Because $\sigma(\beta)$ equals $\zeta \cdot \beta$ and $\sigma(\gamma)$ is $\xi \cdot \gamma$ for roots of unity ζ and ξ there exists some root of unity ζ_σ with

$$\sigma(a_1)c_1 + \cdots + \sigma(a_s)c_s = \zeta_\sigma(a_1c_1 + \cdots + a_sc_s).$$

As the c_i form a basis of L_∞ over K_∞ we have $\sigma(a_i) = \zeta_\sigma \cdot a_i$ for all $i \in \{1, 2, \ldots, s\}$. It follows that the quotient a_i/a_1 is contained in L for all i. Therefore we have

$$\beta \in \gamma \cdot a \cdot L,$$

where a is contained in K_∞ and γ is an element of $\bar{K}^*$ with $\gamma^m \in K^*$ for some $m \in \mathbb{Z}_{>0}$.

Raising to the powers m respectively n shows that $(\gamma \cdot a)^m$ is an element of K_∞^* and that $(\gamma \cdot a)^n$ is contained in L^*. We apply corollary 18 again, this time with ground field K_∞ and α equal to $(\gamma \cdot a)^n$. As α^m is an element of K_∞^* we see that

$$\alpha = w \cdot \prod_i \alpha_i^{s_i},$$

holds for certain $w \in K_\infty^*$ and $s_1, \dots s_k \in \mathbb{N}$. This gives the following equation

$$\delta = w \cdot e^n \cdot \prod_i \alpha_i^{s_i},$$

where we have $e \in L$, $w \in K_\infty^*$ and $s_i \in \mathbb{N}$ for all i. Because all the other terms are elements of L it follows that w is contained in L as well. □

We now have the following result similar to theorem 102.

Corollary 119. *Let K be a field of characteristic 0 and let $\bar{K}$ be a fixed algebraic closure of K. Let $\alpha_1, \dots, \alpha_k \in \bar{K}$ be such that there exist d_i in $\mathbb{Z}_{>0}$ with $\alpha_i^{d_i} \in K$ for all i and let L be $K(\alpha_1, \cdots, \alpha_k)$. Let δ be an element of L and let n be a positive integer with $\gcd(n, d_i) = 1$ for all $i \in \{1, \dots, k\}$. If there exists a field $F \subset K^{(1)}$ and an element β in F with $\beta^n = \delta$, then there exist $w \in K_\infty \cap L$ and $e \in L$ such that δ equals $w \cdot e^n$.*

Proof. Let δ be an element of L and let n be a positive integer. Assume that there exist some field $F \subset K^{(1)}$ and an element β of F with $\beta^n = \delta$. From the theorem 116 it follows

$$\delta = w \cdot e^n \cdot \prod_i \alpha_i^{l_i},$$

for $e \in L$, $w \in K_\infty$ and $l_i \in \mathbb{N}$ for all i. As we have $\gcd(n, d_i) = 1$ for all i, there are $l_i' \in \mathbb{N}$ with $nl_i' = l_i \bmod d_i$. We conclude that there is some $w' \in w \cdot K$ with

$$\delta = w' \cdot \left(e \cdot \prod_i \alpha_i^{l_i'} \right)^n.$$

As δ is an element of L and also $\alpha_1, \dots, \alpha_k$ and e are elements of L, we see that w' is contained in L as well. We therefore have $w' \in K_\infty \cap L$. □

Let K be a real field of characteristic 0 and let a, b, r be elements of K with $\sqrt{r} \notin K$ such that the nested radical $\sqrt{a + b\sqrt{r}}$ is real. Borodin et al [5] showed that the following are equivalent.

- The expression $\sqrt{a + b\sqrt{r}}$ is an element of $K^{(1)}$.
- We have $\sqrt[4]{r}\sqrt{s}\sqrt{a + b\sqrt{r}} \in K(\sqrt{r})$ or $\sqrt{s}\sqrt{a + b\sqrt{r}} \in K(\sqrt{r})$ for some s in K.
- Either $\sqrt{a^2 - b^2 r}$ or $\sqrt{r(b^2 r - a^2)}$ is an element of K.

Example 120. The radical $\sqrt{12 + 5\sqrt{6}}$ is contained in $\mathbb{Q}^{(1)}$ because the number $6(5^2 \cdot 6 - 12^2) = 36$ is a square in $\mathbb{Q}$. To determine w in $\mathbb{Q}_\infty$ and e in $\mathbb{Q}(\sqrt{6})$ such that $12 + 5\sqrt{6} = w \cdot e^2 \cdot \sqrt{6}^l$ for some $l \in \{0, 1\}$ we remark

$$12 + 5\sqrt{6} = \sqrt{6}(5 + 2\sqrt{6}).$$

If there exist a, b, c in $\mathbb{Q}$ with $c(a + b\sqrt{6})^2 = 5 + 2\sqrt{6}$ then a and b satisfy $10ab = 2(a^2 + 6b^2)$. For $a = 2$ and $b = 1$ this equality holds and indeed we have

$$12 + 5\sqrt{6} = \frac{1}{2} \cdot \sqrt{6} \cdot (2 + \sqrt{6})^2.$$

This gives

$$\sqrt{12 + 5\sqrt{6}} = \sqrt[4]{6} \cdot (\sqrt{2} + \sqrt{3}),$$

where $\sqrt[4]{6}$ is the positive real fourth root of 6.

We see that both in this case and in theorem 102 it holds that not only we have $w \in K_\infty \cap L$ but we even have $w \in K$. However, we will not be able to prove that w is contained in K in general as we saw in example 117.

In some special cases theorem 116 gives a both necessary and sufficient condition for a nested radical to be of depth one as the following corollary shows.

Lemma 121. *Let $\alpha_1, \ldots, \alpha_k$ be elements of $\mathbb{R}$ with $\alpha_i^{d_i} \in \mathbb{Q}$ for odd positive integers $d_1, \ldots, d_k$ and define $L = \mathbb{Q}(\alpha_1, \cdots, \alpha_k)$. Then the intersection $L \cap \mathbb{Q}_\infty$ equals $\mathbb{Q}$.*

Proof. When we apply the theory of chapter 1 we see

$$\mathbb{Q}_\infty \cap L \subset \mathbb{Q}(\sqrt{a} : a \in \mathbb{Q}).$$

From proposition 84 we derive that 2 does not divide $[L : \mathbb{Q}]$ and thus we have $L \cap \mathbb{Q}_\infty = \mathbb{Q}$. □

Corollary 122. *Let $\alpha_1, \ldots, \alpha_k$ be elements of $\mathbb{R}$ with $\alpha_i^{d_i} \in \mathbb{Q}$ for odd positive integers $d_1, \ldots, d_k$. We define $L = \mathbb{Q}(\alpha_1, \cdots, \alpha_k)$. Let δ be an element of L and let n be a positive integer, then $\sqrt[n]{\delta}$ is contained in $\mathbb{Q}^{(1)}$ if and only if there exist $w \in \mathbb{Q}$, $e \in L$ and $l_1, \ldots, l_k \in \mathbb{N}$ such that δ equals $w \cdot e^n \cdot \prod_i \alpha_i^{l_i}$.*

That the condition in theorem 116 is not always sufficient we see in the following example.

Example 123. With notations as in theorem 116, we take $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $\delta = 1 + \sqrt{2}$ and $n = 3$. Let α be an element of $\mathbb{R}$ with $\alpha^3 = 1 + \sqrt{2}$. We show that α is not contained in $\mathbb{Q}^{(1)}$, although we have $\alpha^3 = w \cdot e^n$ with $w = 1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}_\infty$ and $e = 1$.

First we remark that we cannot use the same strategy we followed in theorem 102. As $1 + \sqrt{2}$ is the fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{2})$ we see that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is an extension of degree 6. We have $(-1/\alpha)^3 = 1 - \sqrt{2}$ and the normal closure of

$\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \zeta_3)$. This gives the following chain of field extensions

$$\begin{array}{c} \mathbb{Q}(\alpha, \zeta_3) \\ \Big| \, C_3 \\ \mathbb{Q}(\sqrt{2}, \zeta_3) \\ \Big| \, V_4 \\ \mathbb{Q}. \end{array}$$

It immediately follows that $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q})''$ is $\{1\}$.

Suppose that α is contained in $\mathbb{Q}^{(1)}$. Applying corollary 18 with ground field $\mathbb{Q}_\infty = \mathbb{Q}(\sqrt{2})_\infty$ gives

$$\alpha \in \beta \cdot \mathbb{Q}_\infty,$$

for some $\beta \in \bar{\mathbb{Q}}$ with $\beta^m \in \mathbb{Q}$ for some positive integer m and $\beta^d \notin \mathbb{Q}$ for all divisors d of m. We assume without loss of generality that $\beta \in \mathbb{R}$ and that $b = \beta^m > 0$.

First we show that m equals 3 or 6. Because α is not an element of $\mathbb{Q}_\infty$ and α^3 is contained in $\mathbb{Q}_\infty$ we have $\beta \notin \mathbb{Q}_\infty$ and $\beta^3 \in \mathbb{Q}_\infty$. By lemma 68 we have $[\mathbb{Q}_\infty(\beta) : \mathbb{Q}_\infty] = 3$ and therefore $[\mathbb{Q}(\beta) : \mathbb{Q}(\beta^3)] = 3$. As β^3 is contained in $\mathbb{Q}_\infty$ the extension $\mathbb{Q}(\beta^3)/\mathbb{Q}$ is abelian and as $\beta^3 \in \mathbb{R}$ the degree $[\mathbb{Q}(\beta^3) : \mathbb{Q}]$ is 1 or 2. As b is positive, it follows from lemma 68 that $x^m - b$ is the minimal polynomial of β over $\mathbb{Q}$. Hence m equals 3 or 6.

We saw above that there exists some $w \in \mathbb{Q}_\infty$ with $w^3 = (1+\sqrt{2})/\beta^3$. As $\mathbb{Q}(w)/\mathbb{Q}$ is an abelian extension, the polynomial $x^3 - w^3$ is reducible over $K = \mathbb{Q}(\sqrt{2}, \beta^3)$. So, there exists some y in K such that y^3 equals w^3. For this element y^3 the norm in the extension $K/\mathbb{Q}$ is a third power in $\mathbb{Q}$. We have

$$\begin{aligned} \mathrm{N}_{\mathbb{Q}}^{K}\left(y^3\right) &= \mathrm{N}_{\mathbb{Q}}^{K}\left(\frac{1+\sqrt{2}}{\beta^3}\right) = \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\beta^3)}\left(\mathrm{N}_{\mathbb{Q}(\beta^3)}^{K}\left(\frac{1+\sqrt{2}}{\beta^3}\right)\right) \\ &= \begin{cases} \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}}\left(\frac{-1}{b^2}\right) = \frac{-1}{b^2} & \text{if } m = 3 \\ \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{2})}\left(\frac{1+\sqrt{2}}{\beta^3}\right) = \frac{1}{b} & \text{if } m = 6 \text{ and } \mathbb{Q}(\beta^3) = \mathbb{Q}(\sqrt{2}) \\ \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\beta^3)}\left(\frac{-1}{b}\right) = \frac{1}{b^2} & \text{if } m = 6 \text{ and } \mathbb{Q}(\beta^3) \neq \mathbb{Q}(\sqrt{2}). \end{cases} \end{aligned}$$

We conclude $b \in \mathbb{Q}^3$, but this is a contradiction with the definition of b, so $\sqrt[3]{1+\sqrt{2}}$ is not an element of $\mathbb{Q}^{(1)}$.

Chapter 5

Rogers-Ramanujan continued fraction

This chapter consists of a paper co-authored with Alice Gee. It was accepted by the Ramanujan Journal in May 2001 and can also be found in [10]. *The paper, with some minor corrections, follows after a brief introduction.*

In this chapter we determine the class fields generated by singular values of the famous Rogers-Ramanujan continued fraction and give a method for writing these values as nested radicals. Where, in chapters 3 and 4, our goal was to construct a radical expression of minimal nesting depth for a given nested radical, in this chapter we are satisfied if we can give a radical expression. The elements that we consider are given by values of analytic functions and we first have to prove that these elements are nested radicals. It is well known that, for a perfect field K, the element α is a nested radical over K if the Galois group of $K(\alpha)/K$ is solvable.

In section 5.1 we introduce the Rogers-Ramanujan continued fraction, R, which is a function on the complex upper half plane. Moreover, we give some history in constructing nested radicals for special values of this function. In the second section we give two formulas due to Watson [37] that relate $R(z)$, for some z in the upper half plane, to the Dedekind η-function

$$\eta(z) = e^{2\pi iz/24} \prod_{m=1}^{\infty} \left(1 - e^{2\pi izn}\right).$$

This relation we use to prove that R is a modular function of level 5. Moreover, we show that R generates the field of modular functions of level 5 over $\mathbb{Q}(\zeta_5)$. Let τ be an element of the upper half plane with $[1, \tau]$ a $\mathbb{Z}$-basis of some imaginary quadratic order. In section 5.3 we explain, for a modular function h of level $N \in \mathbb{Z}_{>0}$, how to use the structure of the Galois groups in the following chain of fields

$$\mathbb{Q} \subset K = \mathbb{Q}(\tau) \subset H \subset H(h(\tau)),$$

with H the Hilbert class field of K, to determine a nested radical for $h(\tau) \in \mathbb{R}$. In this computation we again use the Dedekind η-function. As all elements that we compute have minimal polynomial in $\mathbb{Z}[x]$ we compute sufficiently accurate real approximations of its coefficients and round these.

In section 5.4 we restrict to modular functions of level 5 again. We introduce functions v, w and $\tilde{w}$ with

$$w(z) = \frac{1}{R(z)} - R(z), \quad \tilde{w}(z) = \frac{w(z)}{\sqrt{5}} \quad \text{and} \quad v(z) = \tilde{w}(z) + \left(\frac{n}{5}\right)\tilde{w}(z)^{-1},$$

where $\left(\frac{n}{5}\right)$ denotes the Jacobi symbol (definition 43).

Another way to represent a nested radical is to give its minimal polynomial. It is clear from the relations above that given a representation for $v(z)$ a representation for $R(z)$ can easily be derived. As the representations for $v(z)$ are more compact we provide in section 5.4 a way to calculate the minimal polynomials for the algebraic integers $\tilde{w}(\tau_n)$ and $v(\tau_n)$ where τ_n is defined by

$$\tau_n = \begin{cases} \sqrt{-n} & \text{if } n \not\equiv 3 \bmod 4 \\ \frac{5+\sqrt{-n}}{2} & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

In the last section we compute nested radicals for the elements $v(\tau_n)$ for $1 \leq n \leq 16$. In section 5.3, example 128, we give an extensive explanation how we use Lagrange resolvents and the Galois action in each of the field extensions in the chain of fields

$$\mathbb{Q} \subset \mathbb{Q}(\tau) \subset H \subset H(h(\tau))$$

to calculate these expressions.

Singular values of the Rogers-Ramanujan continued fraction

Abstract Let $z \in \mathbb{C}$ be imaginary quadratic in the upper half plane. Then the Rogers-Ramanujan continued fraction evaluated at $q = e^{2\pi iz}$ is contained in a class field of $\mathbb{Q}(z)$. Ramanujan showed that for certain values of z, one can write these continued fractions as nested radicals. We use the Shimura reciprocity law to obtain such nested radicals whenever z is imaginary quadratic.

5.1 Introduction

The Rogers-Ramanujan continued fraction is a holomorphic function on the complex upper half plane $\mathbb{H}$, given by

$$R(z) = q^{\frac{1}{5}} \prod_{n=1}^{\infty} \left(1-q^n\right)^{\left(\frac{n}{5}\right)}, \quad \text{with } q = e^{2\pi iz} \text{ and } z \in \mathbb{H}. \tag{5.1}$$

Here $\left(\frac{n}{5}\right)$ denotes the Legendre symbol. The function R owes part of its name to the expansion

$$R(z) = \cfrac{q^{\frac{1}{5}}}{1+\cfrac{q}{1+\cfrac{q^2}{1+q^3\ldots}}} \tag{5.2}$$

as a continued fraction. In their first correspondence of 1913, Ramanujan astonished Hardy with the assertion

$$\cfrac{e^{-\frac{2\pi}{5}}}{1+\cfrac{e^{-2\pi}}{1+\cfrac{e^{-4\pi}}{1+e^{-6\pi}\ldots}}} = \sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}. \tag{5.3}$$

Hardy was unaware of the product expansion 5.1 that Ramanujan had used to compute identity 5.3, which is none other than the evaluation of R at i. In the same correspondence, Ramanujan expressed the equality

$$-R\left(\frac{5+i}{2}\right) = \sqrt{\frac{5-\sqrt{5}}{2}} - \frac{\sqrt{5}-1}{2} \tag{5.4}$$

with a similar dramatic flair. The radical symbol in 5.3 and 5.4 should be interpreted as the real positive root on $\mathbb{R}$. Ramanujan communicated radical expressions for

$R\big(\sqrt{-5}\big)$ and $-R\big(\frac{5+\sqrt{-5}}{2}\big)$ in his second letter to Hardy, and several other values of R at imaginary quadratic arguments are recorded in his notebooks. The other name connected to the function R is that of L.J. Rogers, who proved the equality of 5.1 and 5.2 in 1894. This was discovered by Ramanujan after his arrival in England.

In this paper, we evaluate singular values of the Rogers-Ramanujan continued fraction. These are the function values of R taken at imaginary quadratic $\tau \in \mathbb{H}$. As R is a modular function of level 5 —a classical fact for which we furnish a proof— these values generate abelian extensions of $\mathbb{Q}(\tau)$. Exploiting the Galois action given by the Shimura reciprocity law, we give a method for constructing a nested radical for $R(\tau)$ that works whenever τ is imaginary quadratic. Our systematic approach extends the results of [2], [6], [13] and [27], which only apply to individual examples.

By way of example, we provide nested radicals for $R\big(\sqrt{-n}\big)$ for the integers $n = 1, 2, \ldots, 16$ with $n \not\equiv 3 \bmod 4$. Writing down nested radicals for $R(\tau)$ becomes increasingly unwieldy as the discriminant of τ grows, so in the case $n \equiv 3 \bmod 4$, where $\mathbb{Q}$ and $R(\frac{5+\sqrt{-n}}{2})$ generate a subfield of $\mathbb{Q}(R(\sqrt{-n}))$, we evaluate $R(\frac{5+\sqrt{-n}}{2})$ instead of $R(\sqrt{-n}\,)$. In the classical literature, the notation $S(z) = -R(\frac{5+z}{2})$ is frequently used.

5.2 The modular function field of level 5

A modular function of level N is a meromorphic function on the extended complex upper half plane $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ that is invariant under the natural action of the modular group $\Gamma(N) = \mathrm{Ker}[\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})]$ of level N. As such functions are invariant under $z \mapsto z + N$, they admit a Fourier expansion in the variable $q^{\frac{1}{N}} = e^{\frac{2\pi i z}{N}}$. The modular functions of level N with Fourier expansion in $\mathbb{Q}(\zeta_N)((q^{\frac{1}{N}}))$ form a field F_N, the function field of the modular curve $X(N)$ over $\mathbb{Q}(\zeta_N)$.

The extension F_N is Galois over F_1 with group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. For a proof, see [23], page 66, Theorem 3. One can describe the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on F_N explicitly. The group $(\mathbb{Z}/N\mathbb{Z})^*$ acts as a group of automorphisms of F_N over F_1, by restricting its natural cyclotomic action on $\mathbb{Q}(\zeta_N)((q^{\frac{1}{N}}))$. The natural action of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ induces a right action of $\Gamma(1)/\Gamma(N) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on F_N which leaves F_1 invariant. The homomorphisms

$$(\mathbb{Z}/N\mathbb{Z})^* \to \mathrm{Gal}\,(F_N/F_1) \quad \text{and} \quad \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{Gal}\,(F_N/F_1)$$

can be combined into an action of the semi-direct product

$$(\mathbb{Z}/N\mathbb{Z})^* \ltimes \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

on F_N. For this isomorphism, we identify $d \in (\mathbb{Z}/N\mathbb{Z})^*$ with the element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The resulting sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{Gal}\,(F_N/F_1) \longrightarrow 1 \tag{5.5}$$

is exact.

The modular invariant j generates F_1 over $\mathbb{Q}$, and induces the isomorphism $X(1) \simeq \mathbb{P}^1(\mathbb{Q})$. In a similar fashion, the curve $X(5)$ has genus 0, thus its function field F_5 can be generated by a single function over $\mathbb{Q}(\zeta_5)$. The Rogers-Ramanujan continued fraction R is such a generator. There are several ways to prove this classical fact. Our proof is based up the following two formulas of Ramanujan proofs of which were given by Watson [37]

$$\frac{1}{R(z)} - R(z) - 1 = \frac{\eta(z/5)}{\eta(5z)}, \tag{5.6}$$

$$\frac{1}{R^5(z)} - R^5(z) - 11 = \Big(\frac{\eta(z)}{\eta(5z)}\Big)^6, \tag{5.7}$$

which relate R to Dedekind's η-function

$$\eta(z) = q^{1/24} \prod_{m=1}^{\infty} \left(1 - q^n\right), \quad q^{1/24} = e^{2\pi i z/24}.$$

The above formulas 5.6 and 5.7 will prove useful in section 5.4, where we evaluate singular values of R. We define functions

$$\mathfrak{h}_0 = \frac{\eta \circ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 5 \end{smallmatrix}\right)}{\eta} \quad \text{and} \quad \mathfrak{h}_5 = \sqrt{5} \cdot \frac{\eta \circ \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)}{\eta},$$

so that equations 5.6 and 5.7 become

$$\frac{1}{R} - R - 1 = \sqrt{5} \cdot \frac{\mathfrak{h}_0}{\mathfrak{h}_5}, \tag{5.8}$$

$$\frac{1}{R^5} - R^5 - 11 = \frac{5^3}{\mathfrak{h}_5^6}. \tag{5.9}$$

We will derive the classical fact that R is modular from the modularity of the functions appearing on the right hand side of 5.8 and 5.9. This is well known for $\mathfrak{h}_5^6$ ([26], page 619), but for lack of a reference in the case of 5.8, we provide a proof that works in both cases.

In order to compute the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{h}_0$ and $\mathfrak{h}_5$, we begin by observing that the generating matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{Z})$ act on the Dedekind η-function as

$$\eta \circ S\,(z) = \sqrt{-iz}\,\eta(z) \quad \text{and} \quad \eta \circ T\,(z) = \zeta_{24}\eta(z)\,. \tag{5.10}$$

The radical sign stands for the holomorphic branch of the square root on $-i\mathbb{H}$ that is positive on the real axis. The observation $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 5 \end{smallmatrix}\right) \cdot S = S \cdot \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ gives $\mathfrak{h}_0 \circ S = \mathfrak{h}_5$.

with the help of 5.10. Let Δ_5 denote the set of 2×2 matrices with coefficients in $\mathbb{Z}$ that have determinant 5. The matrices

$$M_i = \left(\begin{smallmatrix} 1 & i \\ 0 & 5 \end{smallmatrix}\right), \ i = 0, 1, \ldots, 4 \quad \text{and} \quad M_5 = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

form a set of representatives for $\Gamma\backslash\Delta_5$. For $A \in \mathrm{SL}_2(\mathbb{Z})$ and $i \in \{0, 1, \ldots, 5\}$, we can find $B \in \mathrm{SL}_2(\mathbb{Z})$ and $j \in \{0, 1, \ldots, 5\}$ such that $M_i \cdot A = B \cdot M_j$ holds. We put

$$\mathfrak{h}_5 \quad = \quad \sqrt{5} \cdot \frac{\eta \circ M_5}{\eta} \qquad \text{and} \qquad \mathfrak{h}_i = \frac{\eta \circ M_i}{\eta} \ \text{ for } i = 0, 1, \ldots, 4. \tag{5.11}$$

Using 5.10 one computes

$$\begin{pmatrix} \mathfrak{h}_0 \\ \mathfrak{h}_1 \\ \mathfrak{h}_2 \\ \mathfrak{h}_3 \\ \mathfrak{h}_4 \\ \mathfrak{h}_5 \end{pmatrix} \circ S = \begin{pmatrix} \mathfrak{h}_5 \\ \zeta_{24}^{-3}\mathfrak{h}_4 \\ \mathfrak{h}_3 \\ \mathfrak{h}_2 \\ \zeta_{24}^{3}\mathfrak{h}_1 \\ \mathfrak{h}_0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathfrak{h}_0 \\ \mathfrak{h}_1 \\ \mathfrak{h}_2 \\ \mathfrak{h}_3 \\ \mathfrak{h}_4 \\ \mathfrak{h}_5 \end{pmatrix} \circ T = \begin{pmatrix} \zeta_{24}^{-1}\mathfrak{h}_1 \\ \zeta_{24}^{-1}\mathfrak{h}_2 \\ \zeta_{24}^{-1}\mathfrak{h}_3 \\ \zeta_{24}^{-1}\mathfrak{h}_4 \\ \mathfrak{h}_0 \\ \zeta_{24}^{4}\mathfrak{h}_5 \end{pmatrix}. \tag{5.12}$$

Lemma 124. *The functions $\mathfrak{h}_5^6$ and $\mathfrak{h}_0/\mathfrak{h}_5$ are modular of level 5.*

Proof. We will show that each of the functions $\mathfrak{h}_i^6$ and $\mathfrak{h}_i/\mathfrak{h}_j$ with $0 \le i, j \le 5$ are invariant under the action of $\Gamma(5)$. From [17] we know that $\Gamma(5)$ is the normal closure of $\langle T^5 \rangle$ in $\mathrm{SL}_2(\mathbb{Z})$. This means that $\Gamma(5)$ is generated by matrices of the form AT^5A^{-1} with $A \in \mathrm{SL}_2(\mathbb{Z})$. From 5.10 we observe

$$\mathfrak{h}_i \circ T^5 = \zeta_6^{-1} \cdot \mathfrak{h}_i \quad \text{ for } i = 0, 1, \ldots, 5\,.$$

For $A \in \mathrm{SL}_2(\mathbb{Z})$ and $j \in \{0, 1, \ldots, 5\}$, the equations 5.12 show that all $\mathfrak{h}_j \circ A$ are of the form $\mathfrak{h}_j \circ A = \zeta \cdot \mathfrak{h}_i$ for some $i \in \{0, 1, \ldots, 5\}$ and some root of unity ζ. Similarly

$$\mathfrak{h}_j \circ AT^5 = \zeta_6^{-1} \cdot \mathfrak{h}_j \circ A$$

holds for every $A \in \mathrm{SL}_2(\mathbb{Z})$. Thus $\mathfrak{h}_i^6$ is invariant under AT^5A^{-1} for all $A \in \mathrm{SL}_2(\mathbb{Z})$, as well as every quotient $\mathfrak{h}_i/\mathfrak{h}_j$.

It is easy to check that the Fourier expansions of the functions $\mathfrak{h}_0^6, \mathfrak{h}_5^6, \mathfrak{h}_0/\mathfrak{h}_5$ and $\mathfrak{h}_5/\mathfrak{h}_0$ are in $\mathbb{Q}(\zeta_5)((q^{1/5}))$. Those of the other functions are in $\mathbb{Q}(\zeta_{20})((q^{1/5}))$. □

Lemma 125. *The Rogers-Ramanujan continued fraction R is modular of level 5.*

Proof. From 5.1 we know that R is holomorphic on $\mathbb{H}$ and that its q-expansion is an element of $\mathbb{Q}(\zeta_5)((q^{1/5}))$. Therefore it suffices to show that $R \circ AT^5A^{-1} = R$ for all $A \in \mathrm{SL}_2(\mathbb{Z})$. From formula 5.8 one derives

$$\Big(X - R\Big)\Big(X + \frac{1}{R}\Big) \quad = \quad X^2 + \Big(\sqrt{5} \cdot \frac{\mathfrak{h}_0}{\mathfrak{h}_5} + 1\Big)X - 1. \tag{5.13}$$

As AT^5A^{-1} acts trivially on $\sqrt{5}\,\mathfrak{h}_0/\mathfrak{h}_5$, it maps R to either R or $-1/R$. Suppose the latter to be true. Then $R\circ AT^5 = -1/(R\circ A)$ holds. As the translation T^5 fixes the cusp $i\infty$, we have

$$R\circ A(i\infty) = R\circ AT^5(i\infty) = \frac{-1}{R\circ A(i\infty)}\ ,$$

which implies $R\circ A(i\infty) = \pm i$. Then formula 5.9 yields

$$\frac{5^3}{\big(\mathfrak{h}_5\circ A(i\infty)\big)^6} = \frac{1}{(\pm i)^5} - (\pm i)^5 - 11 = \pm 2i - 11. \tag{5.14}$$

On the other hand, we can evaluate $\mathfrak{h}_5\circ A(i\infty)$ by considering the product expansion for $\mathfrak{h}_5\circ A$ at $q=0$. By 5.12, one has $\mathfrak{h}_5\circ A = \zeta\cdot\mathfrak{h}_j$ for some root of unity ζ and some $j\in\{0,1,\ldots,5\}$. For $j=0,1,\ldots,4$, we compute

$$\mathfrak{h}_j(i\infty) = \lim_{N\to\infty}\frac{e^{2\pi i\left(\frac{iN+j}{5}\right)}}{e^{2\pi i(iN)}} = 0\ .$$

A similar calculation shows that $\mathfrak{h}_5$ has a pole at $i\infty$. Contradiction with 5.14. □

Lemma 126. *The minimum polynomial of R^5 over $F_1=\mathbb{Q}(j)$ is*

$$\begin{aligned}P(X) = {} & X^{12}+1+(j-684)(X^{11}-X)+(55j+157434)(X^{10}+X^2)\\ & +(1205j-12527460)(X^9-X^3)+(13090j+77460495)(X^8+X^4)\\ & +(69585j-130689144)(X^7-X^5)+(134761j-33211924)X^6.\end{aligned}$$

The minimum polynomial of R over $\mathbb{Q}(j)$ is $P(X^5)$, with P as above.

Proof. Weber shows, [38] page 256, that $\mathfrak{h}_0^2$ is a zero of $X^6+10X^3-\gamma_2X+5$, with γ_2 a cube root of j. Another zero is $\mathfrak{h}_5^2=(\mathfrak{h}_0\circ S)^2$ because S fixes γ_2. We obtain

$$j \;=\; \frac{\big(\mathfrak{h}_5^{12}+10\mathfrak{h}_5^6+5\big)^3}{\mathfrak{h}_5^6}\ . \tag{5.15}$$

Rewriting 5.9 gives the identity

$$\mathfrak{h}_5^6 = \frac{5^3\cdot R^5}{-R^{10}-11R^5+1}\ .$$

Substituting the above relation for $\mathfrak{h}_5^6$ into 5.15, we have

$$j \;=\; \frac{\big(1+228R^5+494R^{10}-228R^{15}+R^{20}\big)^3}{\big(-R+11R^6+R^{11}\big)^5}\ , \tag{5.16}$$

which readily yields $P(R^5) = 0$, with P as in lemma 126. To see that P is irreducible in $\mathbb{Z}[X, j]$, compose the evaluation map $\mathbb{Z}[X, j] \to \mathbb{Z}[X]$ defined by $j \mapsto 1$ with reduction modulo 2. We obtain a homomorphism $\mathbb{Z}[X, j] \to \mathbb{F}_2[X]$ that sends P to the cyclotomic polynomial $\Phi_{13} \in \mathbb{F}_2[X]$, which is irreducible because 2 is a primitive root modulo 13. As P is a monic polynomial in X, we conclude that it is the minimum polynomial of R^5 over $\mathbb{Q}(j)$.

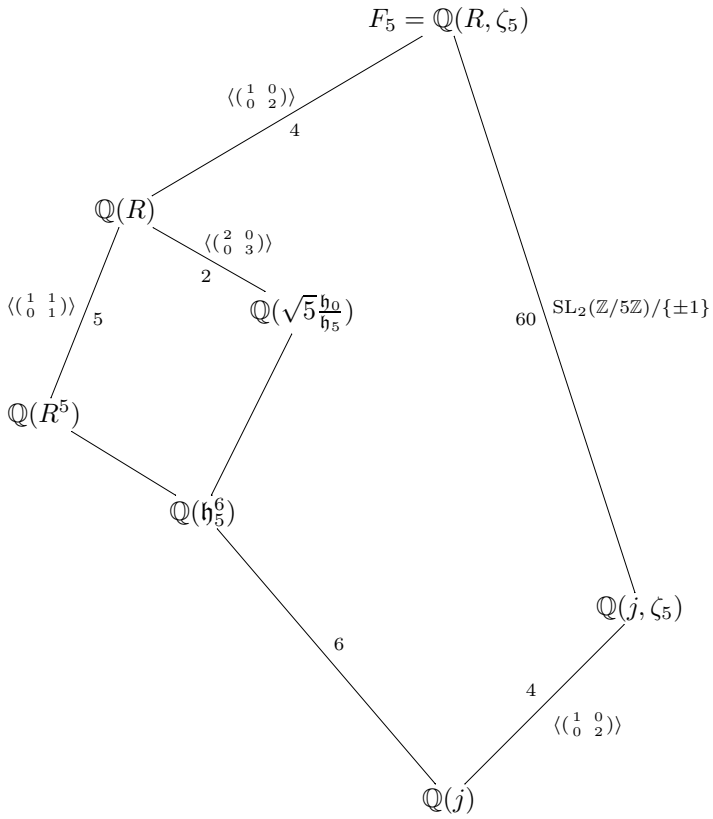
In order to see that $\mathbb{Q}(R)$ has degree $5 \cdot \big[\mathbb{Q}(R^5) : \mathbb{Q}(j)\big] = 60$ over $\mathbb{Q}(j)$, it suffices to observe that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, which acts as $R(z) \mapsto R(z+1) = \zeta_5 R(z)$ induces an automorphism of order five of $\mathbb{Q}(R)$ over $\mathbb{Q}(R^5)$. Thus $P(X^5)$ is the minimum polynomial of R over $\mathbb{Q}(j)$. □

Theorem 127. *The Rogers-Ramanujan continued fraction R generates F_5 over $\mathbb{Q}(\zeta_5)$.*

Proof. As R has rational Fourier coefficients, the subfields $\mathbb{Q}(R) = F_1(R)$ and $F_1(\zeta_5)$ of F_5 are linearly disjoint extensions of F_1 having degree 60 and 4, respectively. Their composite, which has degree $240 = \#\big(\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}\big)$ over F_1 is therefore equal to F_5. □

The rational function on the right hand side of 5.16 appears in Klein's study of the finite subgroups of $\mathrm{Aut}(\mathbb{P}^1(\mathbb{C}))$. His icosahedral group A_5 is isomorphic to $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$, and the natural map from $\mathbb{P}^1(\mathbb{C})$ to the orbit space of the icosahedral group ramifies above 3 points. The relation 5.16 defines a generator, [15] page 61 and 65, for the field of functions invariant under the icosahedral group. In our situation the natural map $X(5) \to X(1)$ ramifies over 3 points and the Galois group of $\mathbb{C}(R)$ over $\mathbb{C}(j)$ is $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$.

The subgroups of $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$ that stabilise the functions appearing in the equations 5.8 and 5.9 are given in the diagram below. The stabilisers of $\mathfrak{h}_5^6$ and $\sqrt{5} \cdot \mathfrak{h}_0/\mathfrak{h}_5$ in $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$ can be determined using 5.12.



5.3 Galois theory for singular values of modular functions

Let $\mathcal{O}$ be an imaginary quadratic order having $\mathbb{Z}$-basis $[\tau, 1]$. Define $H_N = H_{N,\mathcal{O}}$ to be the field generated over $K = \mathbb{Q}(\tau)$ by the function values $h(\tau)$, where h ranges over the modular functions in F_N that are pole-free at τ. The first main theorem of complex multiplication [23] states that H_N is an abelian extension of K. For $N = 1$, the field H_1 is the ring class field for $\mathcal{O}$. If $\mathcal{O}$ is a maximal quadratic order with field of fractions K, then H_N is the ray class field of conductor N over K, and H_1 is the Hilbert class field of K. For ray class fields of non-maximal orders, see for example [34].

Before we can describe the explicit action of $\mathrm{Gal}\,(H_N/K)$ on elements of H_N, we first look at $\mathrm{Gal}\,(H_N/H_1)$, which fits in a short exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow (\mathcal{O}/N\mathcal{O})^* \xrightarrow{A} \mathrm{Gal}\,(H_N/H_1) \longrightarrow 1.$$

In order to describe the Artin map A, we write the elements of $\mathcal{O}/N\mathcal{O}$ as row vectors with respect to the $\mathbb{Z}/N\mathbb{Z}$-basis $[\tau, 1]$. If τ has minimum polynomial $X^2 + BX + C \in \mathbb{Z}[X]$, define the homomorphism

$$\begin{array}{rcl} g_\tau : (\mathcal{O}/N\mathcal{O})^* & \to & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\ s\tau + t & \mapsto & \left(\begin{smallmatrix} t-Bs & -Cs \\ s & t \end{smallmatrix}\right). \end{array} \tag{5.17}$$

The matrix $g_\tau(x)$ represents multiplication by x on $\mathcal{O}/N\mathcal{O}$ with respect to the $\mathbb{Z}/N\mathbb{Z}$-basis $[\tau, 1]$. For $h \in F_N$, the Shimura reciprocity law [30] gives the action of $x \in (\mathcal{O}/N\mathcal{O})^*$ on $h(\tau)$ as

$$\big(h(\tau)\big)^{x^{-1}} \quad = \quad h^{g_\tau(x)}(\tau). \tag{5.18}$$

Here $g_\tau(x) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $h \in F_N$ as described in 5.5. Moreover, if $h \in F_N$ is a function for which $\mathbb{Q}(h) \subset F_N$ is Galois, then $K\big(h(\tau)\big)$ is the fixed field of

$$\{x \in (\mathcal{O}/N\mathcal{O})^* \mid h^{g_\tau(x)} = h\} \quad \subset \quad (\mathcal{O}/N\mathcal{O})^*. \tag{5.19}$$

For any $h \in F_N$, we aim to compute the conjugates of $h(\tau)$ with respect to the full group $\mathrm{Gal}\,(H_N/K)$. In the case $N = 1$, the Galois group of $H_1 = K\big(j(\tau)\big)$ over K is isomorphic to the ideal class group $\mathrm{C}(\mathcal{O})$ of $\mathcal{O}$. The elements of $\mathrm{C}(\mathcal{O})$ can be represented as primitive quadratic forms $[a, b, c]$ of discriminant $D = b^2 - 4ac$, where D is the discriminant of $\mathcal{O}$. The $\mathbb{Z}$-module having basis $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ is an $\mathcal{O}$-ideal in the class of $[a, b, c]$, and the class of $[a, -b, c]$ acts on $j(\tau)$ as

$$j(\tau)^{[a,-b,c]} \quad = \quad j\left(\frac{-b + \sqrt{D}}{2a}\right). \tag{5.20}$$

In the general case for $N > 1$, we need the elements of $\mathrm{Gal}\,(H_N/K)$ that lift (3.5) for each representative $[a, b, c]$ in $\mathrm{C}(\mathcal{O})$. The formula [9], Theorem 20 produces one element $\sigma \in \mathrm{Gal}\,(H_N/K)$ along with a matrix $M_N = M_N(a, b, c)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that for all $h \in F_N$, the relation

$$h(\tau)^\sigma \quad = \quad h^{M_N}\left(\frac{-b + \sqrt{D}}{2a}\right) \tag{5.21}$$

holds. The automorphism σ clearly lifts the action in 5.20 to $\mathrm{Gal}\,(H_N/K)$ because $M_N \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts trivially on $j \in F_1$. As every automorphism in $\mathrm{Gal}\,(H_N/K)$ is obtained by composing elements of $\mathrm{Gal}\,(H_N/H_1)$ with one of the coset representatives for $\mathrm{Gal}\,(H_1/K)$ in 5.21, we can determine the conjugates of $h(\tau)$ under $\mathrm{Gal}\,(H_N/K)$ for any $h \in F_N$.

Given this explicit action on H_N over K we can compute representations for singular values of modular functions by minimal polynomials as well as radical expressions over $\mathbb{Q}$.

The natural way to describe an algebraic number is its minimum polynomial over $\mathbb{Q}$. Let $h \in F_N$ be a function for which $h(\tau)$ is an algebraic integer. The conjugates of $h(\tau)$ over K can be approximated numerically when the Fourier expansion for h is known. One expresses each conjugate in the form $h^M(\theta)$, with $M \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\theta \in K$, and then writes $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right) \cdot A$ with $x = \det(M)$ and $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. After modifying the Fourier coefficients of h with respect to $\zeta_N \mapsto \zeta_N^x$, one evaluates the new expansion at $\tilde{A}(z)$, where $\tilde{A} \in \mathrm{SL}_2(\mathbb{Z})$ is a lift of A. We calculate the minimum polynomial f of $h(\tau)$ over $\mathbb{Q}$ by approximating the conjugates of $h(\tau)$ over K. Adjoining complex conjugates gives a full set of conjugates over $\mathbb{Q}$. In order to determine the polynomial $f \in \mathbb{Z}[X]$, we need only to approximate its coefficients accurate to the nearest integer.

Because H_5 is abelian over K, one can also express $h(\tau)$ as a nested radical over $\mathbb{Q}$ in the spirit of Ramanujan's evaluations 5.3 and 5.4. Unlike the minimum polynomial f, which is unique, many different nested radicals over $\mathbb{Q}$ exist that all represent $h(\tau)$. Given *any* abelian extension H/K of degree greater than 1 and any $w \in H$, the following standard procedure expresses w as a radical expression over a field H' with the property $[H' : K] < [H : K]$. Applying the procedure recursively produces a nested radical for w over K.

We *choose* an automorphism $\sigma \in \mathrm{Gal}\,(H/K)$ of order $m > 1$ and set $H' = H^\sigma(\zeta_m)$, where H^σ denotes the fixed field of $\langle\sigma\rangle$. Then H'/K is an abelian extension of degree

$$[H' : K] \le \varphi(m) \cdot [H^\sigma : K] < m \cdot [H^\sigma : K] = [H : H^\sigma][H^\sigma : K] = [H : K] \; .$$

We write

$$w \;\; = \;\; \frac{1}{m}\big(h_0 + h_1 + h_2 + \cdots + h_{m-1}\big) \; , \tag{5.22}$$

where

$$h_i = \sum_{k=1}^{m} \zeta_m^{ik} \cdot w^{(\sigma^k)} \; , \qquad i = 0, 1, \ldots, m-1$$

are the Lagrange resolvents for w with respect to σ. Note that $h_0 = \mathrm{Tr}_{H/H^\sigma}(w)$ is an element of H'. Every $\rho \in \mathrm{Gal}\,(H(\zeta_m)/H')$ acts trivially on ζ_m and as some $\sigma^a \in \langle\sigma\rangle$ on H. For $i = 1, 2, \ldots, m-1$, we have

$$h_i^\rho = \sum_{k=1}^{n} \zeta_m^{ik} \cdot w^{(\sigma^{k+a})} = \zeta_m^{-ia} \cdot h_i \; ,$$

which means $h_1^m, h_2^m, \ldots, h_{m-1}^m \in H'$. As $h_i = \sqrt[m]{h_i^m}$ for the appropriate choice of the m-th root, equation 5.22 represents w as a radical expression over H'. The recursion step is applied to $h_0, h_1^m, h_2^m, \ldots, h_{m-1}^m \in H'$.

Suppose $h \in F_N$ such that $h(\tau)$ is an algebraic integer. In order to apply the recursive procedure above to $h(\tau)$, one needs not only the action of $\mathrm{Gal}\,(H_N/K)$,

but also that of $\mathrm{Gal}\,(H_N(\zeta_d)/K)$ for various numbers $d > 1$. This is obtained by restricting the action of $\mathrm{Gal}\,(H_{dN}/K)$ to $H_N(\zeta_d)$. The elements computed in the final recursion step are in $\mathcal{O}_K$, which is a discrete subgroup of $\mathbb{C}$. An approximation of their coordinates with respect to a $\mathbb{Z}$-basis for $\mathcal{O}_K$, that is accurate to the nearest integer, produces a nested radical for $h(\tau)$ over $\mathbb{Q}$.

The methods above can be extended to arbitrary imaginary quadratic numbers $\theta \in \mathbb{H}$ that are not necessarily algebraic integers. In order to compute the conjugates of $h(\theta)$ over $K = \mathbb{Q}(\theta)$ we take an integral basis $[\tau, 1]$ for K and write $\theta = \frac{a}{d}\tau + \frac{b}{d}$ with $a, b, d \in \mathbb{Z}$. One evaluates $h \circ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in F_{adN}$ at τ, which is contained in H_{adN}. Again, 5.18 and 5.21 allow us to calculate the conjugates of $h(\theta)$ over K.

Example 128. Define $\tau_6 = \sqrt{-6}$, we will explain how to compute a nested radical for $v(\tau_6)$ where

$$v = \frac{h_0}{h_5} + \frac{h_5}{h_0}.$$

Let K denote $\mathbb{Q}(\sqrt{-24}\,)$ and let H be the Hilbert class field of K. As $v \in F_5$ we find in [9] that the Galois action of $H(v(\tau_6))/H$ is given by the matrix $A = \left(\begin{smallmatrix} 1 & 4 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$. The Galois group of the extension H/K is given by the class group of K. The tower of field extensions in a diagram:

$$\begin{array}{l} H\big(v(\tau_6)\big) \\ \quad 2 \,\big|\, \langle\sigma\rangle \\ \quad H \\ \quad 2 \,\big|\, \langle\rho\rangle \\ \quad K = \mathbb{Q}(\sqrt{-24}\,) \\ \quad 2 \,\big| \\ \quad \mathbb{Q} \end{array}$$

If we have $\mathrm{Gal}(H(v(\tau_6))/H) = \langle\sigma\rangle$ then $v(\tau_6)+v(\tau_6)^\sigma$ and $\big(v(\tau_6)-v(\tau_6)^\sigma\big)^2 \in H$. We determine the conjugates of these elements by the action of $\mathrm{Gal}(H/K) = \langle\rho\rangle$. The elements of the class group of K are the classes of the quadratic forms $[1,0,6]$ and $[2,0,3]$. They induce ([9], Theorem 20) matrices $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $M = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Formula 5.21 tells us how to determine $\big(v(\tau_6) + v(\tau_6)^\sigma\big)^\rho$. We find

$$\big(v(\tau_6) + v(\tau_6)^\sigma\big)^\rho = (v + v^A)(\tau_6)^{[2,0,3]} = (v^M + v^{AM})\Big(\frac{-0 + \sqrt{-24}}{4}\Big).$$

To determine v^M and v^{AM} we first write each of the matrices as a product of a matrix of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, where d denotes the determinant, and a matrix in $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$.

This gives

$$M = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) \quad \text{and} \quad A \cdot M = \left(\begin{smallmatrix} 2 & 4 \\ 2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 2 & 4 \\ 3 & 4 \end{smallmatrix}\right).$$

Then we determine matrices of determinant 1 in $\mathrm{GL}_2(\mathbb{Z})$ that are representatives for the matrices in $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$. They are $\left(\begin{smallmatrix} 2 & 5 \\ 5 & 13 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & -1 \\ 3 & -1 \end{smallmatrix}\right)$. Then we get

$$(v^M + v^{AM})\Big(\frac{-0+\sqrt{-24}}{4}\Big) = \Big(\frac{2}{5}\Big) \cdot v\Big(\frac{1/2 \cdot \sqrt{-6}+5}{5/2 \cdot \sqrt{-6}+13}\Big) + \Big(\frac{4}{5}\Big) \cdot v\Big(\frac{\sqrt{-6}-1}{3/2 \cdot \sqrt{-6}-1}\Big),$$

where $(\frac{\cdot}{\cdot})$ denotes the Jacobi symbol.

Similar computations yield all conjugates of the elements $v(\tau_6) + v(\tau_6)^\sigma$ and $\big(v(\tau_6) - v(\tau_6)^\sigma\big)^2$. Define v_1, v_2, v_3, v_4 by

$$\begin{aligned} v_1 &= v(\tau_6) & v_3 &= -v\Big(\tfrac{\tau_6+5}{5/2\cdot\tau_6+13}\Big) \\ v_2 &= -v\Big(\tfrac{11\cdot\tau_6+29}{3\cdot\tau_6+8}\Big) & v_4 &= v\Big(\tfrac{\tau_6-1}{3/2\cdot\tau_6-1}\Big), \end{aligned}$$

then these conjugates are $v_1 + v_2$, $v_3 + v_4$, $v_1^2 - v_2^2$ and $v_3^2 - v_4^2$ in H.

To compute a nested radical for $v(\tau_6) = v_1$ we determine an accurate approximation for $v_1 + v_2 + v_3 + v_4 \in \mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$, rounding gives that

$$v_1 + v_2 + v_3 + v_4 = 8.$$

By approximating we also find

$$((v_1 + v_2) - (v_3 + v_4))^2 = 200 \quad \text{and} \quad (v_1 + v_2) - (v_3 + v_4) > 0,$$

$$(v_1 - v_2)^2 + (v_3 - v_4)^2 = 60,$$

$$((v_1 - v_2)^2 - (v_3 - v_4)^2)^2 = 3200 \quad \text{and} \quad (v_1 - v_2)^2 - (v_3 - v_4)^2 > 0.$$

Thus we have the equalities

$$1/2 \cdot (8 + \sqrt{200}\,) = v_1 + v_2$$

and

$$1/2 \cdot (60 + \sqrt{3200}\,) = (v_1 - v_2)^2.$$

From which follows, as $v_1 - v_2 > 0$,

$$\begin{aligned} v(\tau_6) = v_1 &= 1/4 \cdot \big(8 + \sqrt{200}\,\big) + 1/2 \cdot \sqrt{30 + 1/2 \cdot \sqrt{3200}} \\ &= 1/2 \cdot \left(4 + 5\sqrt{2} + 10 \cdot \sqrt{3 + 2\sqrt{2}}\right) \\ &= 1/2 \cdot \big(4 + 5\sqrt{2} + \sqrt{10} + 2\sqrt{5}\,\big) \end{aligned}$$

5.4 The ray class field H_5

We turn our attention back to the functions of level 5 from section 2. In this section, we compute some singular values $R(\tau)$ of the Rogers-Ramanujan continued fraction. As the singular values of j are known to be algebraic integers, the same holds true for R because the polynomial P of lemma 126 has coefficients in $\mathbb{Z}[j]$. We fix $\mathcal{O} = [\tau, 1]$ to be an order in some imaginary quadratic number field K. We state a few properties of $R(\tau)$ before computing some examples.

Lemma 129. *The class field $H_5 = H_{5,\mathcal{O}}$ is generated by $R(\tau)$ over K.*

Proof. As we have $F_5 = \mathbb{Q}(R, \zeta_5)$ by Theorem 127, the extension $F_5/\mathbb{Q}(R)$ is Galois and we are in the situation for which 5.19 applies. As $\mathbb{Q}(R)$ is the subfield of F_5 fixed by

$$\left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \mid d \in (\mathbb{Z}/5\mathbb{Z})^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) \ ,$$

the class field $K\big(R(\tau)\big)$ is the subfield of H_5 fixed by

$$G = \{x \in (\mathcal{O}/5\mathcal{O})^* \mid g_\tau(x) = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \text{ for some } d \in (\mathbb{Z}/5\mathbb{Z})^*\} \subset (\mathcal{O}/5\mathcal{O})^* \ .$$

From formula 5.17 we see that the only diagonal matrices appearing in the image $g_\tau[(\mathcal{O}/5\mathcal{O})^*]$ are scalar. We conclude $G = \{\pm 1\}$ and $K\big(R(\tau)\big) = H_5$. □

Let $w(z) = \eta(\frac{z}{5})/\eta(5z)$ denote the function that appears on the right hand side of equation 5.6. Thus we have

$$\frac{1}{R(z)} - R(z) - 1 \quad = \quad w(z). \tag{5.23}$$

Lemma 130. *The singular values $R(\tau)$ and $-1/R(\tau)$ are conjugate over the field $K\big(w(\tau)\big)$. Furthermore, H_5 is generated over K by ζ_5 together with $w(\tau)$.*

Proof. The polynomial

$$X^2 + \big(w(\tau) + 1\big)X - 1 \quad \in \quad K\big(w(\tau)\big)[X] \tag{5.24}$$

derived from 5.23 has zeroes $R(\tau)$ and $-1/R(\tau)$. To show that 5.24 is irreducible in $K\big(w(\tau)\big)[X]$ we consider the homomorphism $g_\tau : (\mathcal{O}/5\mathcal{O})^* \to \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ in 5.17. By 5.18, the group $\mathrm{Gal}\,(H_5/H_1)$ contains the automorphism $R(\tau) \mapsto R^{g_\tau(2)}(\tau)$. In order to determine the action action of

$$g_\tau(2) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

on F_5, we recall that R and w have rational Fourier coefficients and thus are fixed by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$. Using 5.12 one checks that w is stabilised by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$. Theorem 127 together with equation 5.23 tells us that this matrix $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ sends R to $-1/R$,

so $R(\tau)$ and $-1/R(\tau)$ are conjugates over K. As $K\big(R(\tau)\big) = H_5$ contains ζ_5, the situation $R(\tau) = -1/R(\tau) = \pm i$ is impossible. We conclude that 5.24 is irreducible in $K\big(w(\tau)\big)[X]$.

We have $[H_5 : K\big(w(\tau)\big)] = 2$. In fact, $K\big(w(\tau)\big)$ is the subfield of H_5 fixed by the subgroup of $(\mathcal{O}/5\mathcal{O})^*$ generated by 2 and the image of $\mathcal{O}^*$. By 5.24 the action of $2 \in (\mathcal{O}/5\mathcal{O})^*$ on $\zeta_5 \in H_5$ is $\zeta_5 \mapsto \zeta_5^{-1}$. We conclude $\zeta_5 \notin K\big(w(\tau)\big)$ and $H_5 = K\big(w(\tau), \zeta_5\big)$. □

To determine the minimum polynomial of $R(\tau)$ over $\mathbb{Q}$, it is convenient, although certainly not necessary, to first compute the polynomial for $w(\tau)$ and then recover $R(\tau)$ with 5.23. As both values $R(\tau)$ and $1/R(\tau)$ are algebraic integers, it follows that $w(\tau)$ is an algebraic integer too. In particular, the method of section 5.4 for computing $f_{\mathbb{Q}}^{w(\tau)}$ works here.

Working with values of w is easier than working with R directly as there are only half as many conjugates over K to compute. More importantly, the Dedekind η-function is implemented in several software packages that quickly compute $\eta(z)$ to a high degree of accuracy. These routines make use of $\mathrm{SL}_2(\mathbb{Z})$-transformations to ensure that the imaginary part of z is sufficiently large to guarantee rapid convergence of the Fourier expansion of $\eta(z)$. For the expansion 5.1 of the function $R(z)$ such a standard implementation does not appear to be available.

One obtains the minimal polynomial of $R(\tau)$ over $\mathbb{Q}$ from $f_{\mathbb{Q}}^{w(\tau)}$ by writing

$$w = \frac{1 - R - R^2}{R}$$

using 5.6. Then $R(\tau)$ is a zero of the monic polynomial

$$X^{\deg.} f_{\mathbb{Q}}^{w(\tau)}\Big(\frac{1 - X - X^2}{X}\Big) \in \mathbb{Q}[X]$$

with $\deg = \deg(f_{\mathbb{Q}}^{w(\tau)})$. According to lemma 130, the resulting polynomial is irreducible because its degree is $2 \cdot \deg$.

An inspection of product expansion 5.1 shows $R(z) \in \mathbb{R}$ whenever the real part of $z \in \mathbb{H}$ is an integer multiple of $\frac{5}{2}$. For the singular arguments

$$\tau_n = \begin{cases} \sqrt{-n} & \text{if } n \not\equiv 3 \bmod 4 \\ \frac{5+\sqrt{-n}}{2} & \text{if } n \equiv 3 \bmod 4 \end{cases}$$

the value $R(\tau_n)$ is a real, and its minimum polynomial over K is contained in $\mathbb{Z}[X]$ because complex conjugation acts as

$$\overline{f_K^{R(\tau_n)}} = f_K^{\overline{R(\tau_n)}} = f_K^{R(\tau_n)} .$$

Lemma 130 implies that $f_{\mathbb{Q}}^{R(\tau)} = \sum_{i=0}^{2d} c_i X^i$ is the minimum polynomial for both $R(\tau)$ and $-1/R(\tau)$, thus the coefficients satisfy $c_i = (-1)^i c_{2d-i}$. For this reason we only list the first half of the coefficients $c_{2d}, c_{2d-1}, \ldots, c_d$ in table 1, where we give the minimum polynomials for $R(\tau_n)$ with $1 \le n \le 16$.

Table 1. *The minimum polynomials of $R(\tau_n)$ over $\mathbb{Q}$*

n	degree	first half of coefficients $c_{2d}, c_{2d-1} \ldots c_d$
1	4	$1, 2, -6$
2	12	$1, 6, -1, 0, 50, -14, 16$
3	4	$1, -3, -1$
4	8	$1, 14, 22, 22, 30$
5	20	$1, 10, -90, 280, -730, 1022, -2410, 2540, -3330, 1730, -2006$
6	16	$1, 28, 140, 60, -365, 264, 482, 340, 2035$
7	12	$1, -4, -1, -25, -25, -14, 31$
8	24	$1, 32, -96, 268, 51, -328, -1446, -5112, 996, 3972, 10594, 4208, -6924$
9	16	$1, 38, -240, -300, -235, -726, 92, -1840, -675$
10	20	$1, 60, 360, -120, 120, -1728, 3540, 840, 4320, -7620, -1006$
11	8	$1, -6, -13, -28, 5$
12	24	$1, 82, 329, -282, -74, 3672, -3846, 4238, 13521, -9028, 7844, 2408, 43651$
13	24	$1, 82, -996, 968, 1051, 1422, -96, -24912, 7896, 16722, 28844, 13658, -114024$
14	32	$1, 116, 614, -3040, 25230, 17988, -103372, 184292, 207725, -409400, -323390, -129140, 2879690, 3515800, -5057000, -4838560, 7624315$
15	20	$1, -15, 60, -270, 720, -1353, 2115, -2610, 2970, -1095, 3119$
16	16	$1, 148, -670, 240, 1570, -2616, 302, 1180, -1610$

A nice way of generating $H_5 = K(w(\tau_n), \zeta_5)$ comes from lemma 130. The subfield $K(w(\tau_n))$ of H_5 is the fixed field for the subgroup generated by 2 and $\mathcal{O}^*$ in $(\mathcal{O}/5\mathcal{O})^*$. Because $\sqrt{5}$ is invariant under $g_{\tau_n}(2) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, we conclude $\sqrt{5} \in K(w(\tau_n))$. Thus for the function

$$\tilde{w} = \frac{w}{\sqrt{5}} = \frac{\mathfrak{h}_0}{\mathfrak{h}_5}$$

we have $\tilde{w}(\tau_n) \subset K(w(\tau_n))$ and $H_5 = K(\tilde{w}(\tau_n), \zeta_5)$.

Lemma 131. *The value $\tilde{w}(\tau_n)$ is an algebraic integer. If $5 \nmid n$ then $\tilde{w}(\tau_n)$ is a unit in H_5, the ray class field of conductor 5 over $\mathcal{O} = [\tau_n, 1]$.*

Proof. Hasse and Deuring, [8] page 43, determine exactly the ideals generated by singular values of the lattice functions

$$\varphi_M(z) = \frac{\Delta\left(M\binom{z}{1}\right)}{\Delta\binom{z}{1}} ,$$

with M a 2×2 matrix having coefficients in $\mathbb{Z}$. Our functions $\mathfrak{h}_0$ and $\mathfrak{h}_5$ were defined in 5.11 as

$$\mathfrak{h}_0 = \frac{\eta\circ M_0}{\eta}\ , \quad \mathfrak{h}_5 = \sqrt{5}\cdot\frac{\eta\circ M_5}{\eta} \quad \text{with } M_0 = \left(\begin{smallmatrix}1 & 0\\ 0 & 5\end{smallmatrix}\right),\ M_5 = \left(\begin{smallmatrix}5 & 0\\ 0 & 1\end{smallmatrix}\right).$$

Thus we have

$$\varphi_{M_0}\begin{pmatrix}z\\1\end{pmatrix} = \mathfrak{h}_0(z)^{24} \quad \text{and} \quad \varphi_{M_5}\begin{pmatrix}z\\1\end{pmatrix} = \mathfrak{h}_5(z)^{24}\ ,$$

and

$$\tilde{w}(\tau_n)^{24} = \frac{\varphi_{M_0}\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)}{\varphi_{M_5}\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)}\ .$$

If n is not divisible by 5, then

$$M_0\begin{pmatrix}\tau_n\\1\end{pmatrix} = [\tau_n, 5] \quad \text{and} \quad M_5\begin{pmatrix}\tau_n\\1\end{pmatrix} = [5\tau_n, 1]$$

are both proper ideals of $\mathcal{O} = [\tau_n, 1]$. Deuring's theorem, [8] page 42, shows that $\varphi_{M_0}\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)$ and $\varphi_{M_5}\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)$ are associate elements in the ring of integral algebraic numbers; one writes

$$\varphi_{M_0}\begin{pmatrix}\tau_n\\1\end{pmatrix} \approx \varphi_{M_5}\begin{pmatrix}\tau_n\\1\end{pmatrix}.$$

It follows that the quotient $\tilde{w}(\tau_n)^{24}$ is a unit.

If $5 \mid n$ but $25 \nmid n$, then $\varphi_{M_0}\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)$ is again a proper $\mathcal{O}$-ideal. However, the multiplicator ring for $M_5\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)$ is not $\mathcal{O}$, but $[5\tau_n, 1]$. Deuring's formulas, [8] page 43, yield

$$\varphi_{M_0}\begin{pmatrix}\tau_n\\1\end{pmatrix} \approx 5^6 \text{ in } \mathcal{O} \text{ and } \varphi_{M_1}\begin{pmatrix}\tau_n\\1\end{pmatrix} \approx 5^{6/5} \text{ in } [5\tau_n, 1].$$

We find $\tilde{w}(\tau_n) \approx 5^{1/5}$.

When n is divisible by 25, the multiplicator rings for $M_0\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)$ and $M_5\left(\begin{smallmatrix}\tau_n\\1\end{smallmatrix}\right)$ are $\mathcal{O}$ and $[1, \tau_n/5]$ respectively. In this case, the formulas, [8] page 43, show that $\tilde{w}(\tau_n)$ is again associated to a positive rational power of 5. □

When $n \in \mathbb{Z}$ is not divisible by 5, the Galois action 5.5 for the matrix $g_{\tau_n}(\tau_n)$ of 5.17 sends $\tilde{w}$ to $\left(\frac{n}{5}\right)\cdot\tilde{w}^{-1}$. We define

$$v(\tau_n) = \tilde{w}(\tau_n) + \left(\frac{n}{5}\right)\tilde{w}(\tau_n)^{-1}\ .$$

Clearly we have $\tilde{w}(\tau_n) = v(\tau_n)$ when n is divisible by 5. However, if $n > 1$ with $5 \nmid n$ then $\tilde{w}(\tau_n)$ has degree 2 over $v(\tau_n)$. In these cases the minimum polynomial for $\tilde{w}(\tau_n)$ satisfies

$$f_{\mathbb{Q}}^{\tilde{w}(\tau_n)} = X^{\deg} \cdot f_{\mathbb{Q}}^{v(\tau_n)}\Big(\frac{X^2 + \left(\frac{n}{5}\right)}{X}\Big)$$

with $\deg = \deg(f_{\mathbb{Q}}^{v(\tau_n)})$. Table 2 lists the minimum polynomials over $\mathbb{Q}$ for $v(\tau_n)$ for $1 \le n \le 16$.

Table 2. *The minimum polynomials over $\mathbb{Q}$ for $v(\tau_n)$*

n	degree	coefficients
1	1	$1, 2$
2	3	$1, -2, 3, -4$
3	1	$1, 1$
4	2	$1, -6, 4$
5	10	$1, -10, 25, -30, 25, -10, 25, 0, 25, 0, 25$
6	4	$1, -8, -16, 28, 31$
7	3	$1, 2, 3, 9$
8	6	$1, -16, 20, -100, 25, -156, -124$
9	4	$1, -22, 54, 62, -59$
10	10	$1, -20, -75, -60, -75, -20, -25, 0, -25, 0, -25$
11	2	$1, 4, -1$
12	6	$1, -34, -5, -150, -75, -144, -99$
13	6	$1, -46, 210, -290, 905, -456, 576$
14	8	$1, -44, -238, 88, 520, -2508, -4978, -176, 2711$
15	10	$1, 5, 0, 15, 0, 5, -25, 0, -25, 0, -25$
16	4	$1, -68, 14, 328, -284$

5.5 Nested radicals

In order to obtain nested radicals for $R(\tau_n)$ over $\mathbb{Q}$ it suffices to have radicals for $\tilde{w}(\tau_n)$. On the imaginary axis, $R(\tau)$ and $w(\tau)$ and $\tilde{w}(\tau)$ take positive real values, and when $\mathrm{Re}(\tau) = \frac{5}{2}$, each of the values $R(\tau)$ and $w(\tau)$ and $\tilde{w}(\tau)$ are real negative numbers. As the conjugate of $R(\tau)$ over $K(w)$ is $-1/R(\tau)$, equation 5.13 gives

$$R(\tau) = \begin{cases} -\frac{1+w(\tau)}{2} + \sqrt{\left(\frac{1+w(\tau)}{2}\right)^2 + 1} & \text{if } n \not\equiv 3 \bmod 4 \\ -\frac{1+w(\tau)}{2} - \sqrt{\left(\frac{1+w(\tau)}{2}\right)^2 + 1} & \text{if } n \equiv 3 \bmod 4 \end{cases}$$

where $\sqrt{\cdot}$ is always the positive square root of a positive real number.

When $n > 1$ and $5 \nmid n$, the algebraic number $\tilde{w}(\tau_n)$ has degree 2 over $\mathbb{Q}(v(\tau_n))$. As the absolute value of $\tilde{w}(\tau_n)$ satisfies $|\tilde{w}(\tau_n)| > 2$ when $n > 1$, one recovers $\tilde{w}(\tau_n)$

from $v(\tau_n)$ as

$$2\tilde{w}(\tau_n) = \begin{cases} v(\tau_n) + \sqrt{v(\tau_n)^2 - 4\left(\frac{n}{5}\right)} & \text{if } n \not\equiv 3 \bmod 4 \\ v(\tau_n) - \sqrt{v(\tau_n)^2 - 4\left(\frac{n}{5}\right)} & \text{if } n \equiv 3 \bmod 4\ . \end{cases}$$

Note that the radicands above are positive real numbers. This is obvious for $\left(\frac{n}{5}\right) = -1$. When $\left(\frac{n}{5}\right) = 1$, we have $|v(\tau_n)| = |\tilde{w}(\tau_n) + 1/\tilde{w}(\tau_n)| > 2$. One easily recovers $R(\tau_n)$ from $\sqrt{5}\cdot\tilde{w}(\tau_n) = w(\tau_n)$. In the case n is divisible by 5, one simply has $v(\tau_n) = \tilde{w}(\tau_n)$.

Below, we give nested radicals for $v(\tau_n)$ with $1 \le n \le 16$, computed as in example 128. In many cases the radicals below have undergone some cosmetic modifications made by factorising elements in real quadratic orders of class number one. Every root appearing in our examples should be interpreted as the real positive root of its real positive argument. Our computation $v(\tau_1) = 2$ for example, leads to $\tilde{w}(\sqrt{-1}) = 1$ and $w(\sqrt{-1}) = \sqrt{5}$, which gives Ramanujan's formula 5.3. The value $v(\tau_3)$ also gives a trivial extension of $\mathbb{Q}$.

$$v(\tau_1) = 2$$

$$v(\tau_3) = -1$$

For $n = 4, 6, 9, 11, 14, 16$ the degree $[\mathbb{Q}(v(\tau_n)) : \mathbb{Q}]$ is a power of 2. In these cases we opt for a tower of quadratic extensions in solving for $v(\tau_n)$.

$$\begin{aligned} v(\tau_4) &= 3 + \sqrt{5} \\ v(\tau_6) &= \tfrac{1}{2}\left(4 + 5\sqrt{2} + \sqrt{10} + 2\sqrt{5}\right) \\ v(\tau_9) &= \tfrac{1}{2}\left(11 + 5\sqrt{3} + 3\sqrt{5} + 3\sqrt{15}\right) \\ v(\tau_{11}) &= -2 - \sqrt{5} \\ v(\tau_{14}) &= (\tfrac{1+\sqrt{2}}{2})^2\Bigg(6 + \sqrt{2} + 5\sqrt{-2 + 4\sqrt{2}} \\ &\qquad + 2\sqrt{5\left(21 - 10\sqrt{2} + (15 - 2\sqrt{2})\sqrt{-11 + 8\sqrt{2}}\right)}\ \Bigg) \\ v(\tau_{16}) &= \tfrac{1}{2}\left(34 + 25\sqrt{2} + 11\sqrt{10} + 14\sqrt{5}\right). \end{aligned}$$

For $n \equiv \pm 2 \bmod 5$, the group $(\mathcal{O}/5\mathcal{O})^*$ is cyclic of order 24. If the discriminant D of $\mathcal{O} = [\tau_n, 1]$ satisfies $D < -4$, then $v(\tau_n)$ generates a degree 3 extension over the ring class field $H_{\mathcal{O}}$. In the examples below, we choose the field tower $H_{\mathcal{O}}(v(\tau_n)) \supset$

$H_{\mathcal{O}} \supseteq \mathbb{Q}(\sqrt{-n})$ to solve for $v(\tau_n)$.

$$
\begin{aligned}
v(\tau_2) &= \tfrac{1}{3}\big(2 + \sqrt[3]{35+15\sqrt{6}} - \sqrt[3]{-35+15\sqrt{6}}\,\big)\\
v(\tau_7) &= \tfrac{1}{6}\Big(-4 + \sqrt[3]{20(-41+9\sqrt{21}\,)} - \sqrt[3]{20(41+9\sqrt{21}\,)}\Big)\\
v(\tau_8) &= \tfrac{1}{3}\Big(8+5\sqrt{2} + \sqrt[3]{\tfrac{5}{2}\Big(782+565\sqrt{2}+3\sqrt{6(7771+5490\sqrt{2}\,)}\Big)}\\
&\qquad + \sqrt[3]{\tfrac{5}{2}\Big(782+565\sqrt{2}-3\sqrt{6(7771+5490\sqrt{2}\,)}\Big)}\ \Big)\\
v(\tau_{12}) &= \tfrac{1}{3}\big(17+10\sqrt{3}+4\sqrt[3]{260+150\sqrt{3}}+\sqrt[3]{23975+13875\sqrt{3}}\big)\\
v(\tau_{13}) &= \tfrac{1}{3}\Big(23+5\sqrt{13}+\sqrt[3]{\tfrac{5}{2}\Big(14123+3905\sqrt{13}+9\sqrt{274434+76110\sqrt{13}}\,\Big)}\\
&\qquad + \sqrt[3]{\tfrac{5}{2}\Big(14123+3905\sqrt{13}-9\sqrt{274434+76110\sqrt{13}}\Big)}\ \Big)
\end{aligned}
$$

When n is divisible by 5, the value of v at τ_n generates a field extension of degree 5 over the ring class field for $\mathcal{O} = [\tau_n, 1]$. In applying the algorithm of section 3, our first step solves for $v(\tau_n)$ over $H_{\mathcal{O}}$.

$$
\begin{aligned}
v(\tau_5) &= 1 + \tfrac{1}{\sqrt{5}}\left(\sqrt[5]{a_1}+\sqrt[5]{a_2}+\sqrt[5]{a_3}+\sqrt[5]{a_4}\right), \quad \text{where}\\
a_1, a_2 &= 10\Big(55+25\sqrt{5} \pm \sqrt{5050+2258\sqrt{5}}\,\Big)\\
a_3, a_4 &= \tfrac{5}{2}\Big(55+25\sqrt{5} \pm \sqrt{50+22\sqrt{5}}\,\Big)\\
v(\tau_{10}) &= \tfrac{1}{\sqrt{5}}\left(5+2\sqrt{5}+\sqrt[5]{a_1}+\sqrt[5]{a_2}+\sqrt[5]{a_3}+\sqrt[5]{a_4}\right), \quad \text{where}\\
a_1, a_2 &= 20\Big(5(3+\sqrt{5}\,)(16+\sqrt{5}\,)(9+4\sqrt{5}\,) \pm 51\Big(\frac{1+\sqrt{5}}{2}\Big)^6\sqrt{2(5+2\sqrt{5}\,)}\,\Big)\\
a_3, a_4 &= 5\Big(5\Big(\frac{1+\sqrt{5}}{2}\Big)^{12}(22-3\sqrt{5}\,) \pm 3\Big(\frac{1+\sqrt{5}}{2}\Big)^6\sqrt{2(5+2\sqrt{5}\,)}\,\Big)\\
v(\tau_{15}) &= -\tfrac{1}{5}\Big(\tfrac{1}{2}(5+5\sqrt{5}) + \sqrt[5]{a_1}+\sqrt[5]{a_2}+\sqrt[5]{a_3}+\sqrt[5]{a_4}\Big), \quad \text{where}\\
a_1, a_2 &= \tfrac{125}{4}\Big(5(25+13\sqrt{5}\,) \pm 14\sqrt{\tfrac{15}{2}(25+11\sqrt{5}\,)}\,\Big)\\
a_3, a_4 &= \tfrac{125}{4}\Big(5(15+7\sqrt{5}\,) \pm 2\sqrt{\tfrac{15}{2}(25+11\sqrt{5}\,)}\,\Big)
\end{aligned}
$$

Bibliography

[1] B.C. Berndt, *Ramanujan's notebooks* IV, Springer-Verlag, New York, 1994.

[2] B.C. Berndt, H.H. Chan, L.C. Zhang, 'Explicit evaluations of the Rogers-Ramanujan continued fraction', *Journal für die Reine und Angewandte Mathematik*, **480**, 1996, 141–159.

[3] A.S. Besicovitch, 'On the lineair independence of fractional powers of integers', *Journal of the London Mathematical Society*, **15**, 1940, 3–6.

[4] J. Blömer, 'How to denest Ramanujan's nested radicals', *Proceedings of the 33rd annual IEEE Symposium on foundations of computer science*, 1992, 447–456.

[5] A. Borodin, R. Fagin, J.E. Hopcroft and M. Tompa, 'Decreasing the nesting depth of expressions involving square roots', *Journal of Symbolic Computation*, **1**, 1985, 169–188.

[6] H.H. Chan, V. Tan, 'On the explicit evaluations of the Rogers-Ramanujan continued fraction', *Continued fractions: from analytic number theory to constructive approximation (Columbia, MO, 1998), Contemp. Math.*, **236**, 1999, 127–136.

[7] C.F. Cotner, *The nesting depth of radical expressions*, dissertation at UC Berkeley, 1995.

[8] M. Deuring, 'Die Klassenkörper der komplexen Multiplikation', *Enzyklopädie der Mathematischen Wissenschaften*, Band I,2. Teil, Heft 10, Teil II.

[9] A.C.P. Gee, 'Class invariants by Shimura's reciprocity law', *Journal de Théorie des Nombres Bordeaux*, **11**, 1999, 45–72.

[10] A.C.P. Gee, *Class fields by Shimura reciprocity*, dissertation at Universiteit van Amsterdam, 2001.

[11] C. Greither and D.K. Harrison, 'A Galois correspondence for radical extensions of fields', *Journal of Pure and Applied Algebra*, **43**, 1986, 257–270.

[12] K. Gruenberg, 'Profinite groups', printed in J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, Orlando, Florida, 1967, 116–161.

[13] S.Y. Kang, 'Ramanujan's formulas for the explicit evaluation of the Rogers-Ramanujan continued fraction and theta-functions', *Acta Arithmetica*, 1999, 49–68.

[14] L.-C. Kappe, B. Warren, 'An elementary test for the Galois group of a quartic polynomial' *American Mathematical Monthly*, **96**, nr. 2, 1989, 133–137.

[15] F. Klein, *The icosahedron and solution of equations of the fifth degree*, Dover, New York, 1956.

[16] M. Kneser, 'Lineare Abhängingkeit von Wurzeln', *Acta Arithmetica* **26**, 1975, 307–308.

[17] M.I. Knopp, 'A note on subgroups of the modular group', *Proceedings of the Mathematical Society*, **14**, 1963, 95–97.

[18] F. Halter-Koch, 'Eine Galoiskorrespondenz für Radikalerweiterungen', *Journal of Algebra*, **63**, nr. 2, 1980, 318–330.

[19] D.S. Kubert and S. Lang, *Modular units*, Springer Grundleren 244, 1981.

[20] S. Landau, 'Simplifications of nested radicals', *SIAM Journal on Computing*, **21**, nr. 1, feb. 1992, 85–110.

[21] S. Landau, 'How to tangle with a nested radical', *The Mathematical Intelligencer*, **16**, nr. 2, 1994, 49–55, Springer-Verlag New York.

[22] S. Lang, *Algebra*, Third Edition, Addison-Wesley Reading, Massachusetts, 1993, reprinted june 1994.

[23] S. Lang, *Elliptic functions*, Second edition, Springer GTM 112, 1987.

[24] H.W. Lenstra, *Galois theory for schemes*, lecture notes, University of Amsterdam, Amsterdam, 1985.

[25] L.J. Mordell, 'On the lineair independence of algebraic numbers', *Pacific Journal of Mathematics*, **3**, 1953, 625–630.

[26] H. Rademacher, 'The Ramanujan identities under modular substiutions', *Transactions of the American Mathematical Society*, **51**, 1942, 609–636.

[27] K.G. Ramanathan, 'Some applications of Kronecker's limit formula', *Journal of the Indian Mathematical Society*, **52**, 1987, 71–89.

[28] S. Ramanujan, 'Questions and solutions', *Collected papers of S. Ramanujan*, Cambridge University Press, Cambridge, 1927.

[29] A. Schinzel, 'Abelian binomials, power residues and exponential congruences', *Acta Arithmetica*, **32**, 1977, 245–274.

[30] G. Shimura, 'Complex multiplication', *Modular functions of one variable I*, Springer LNM 320, 1973, 39-56.

[31] F. Seidelmann, *'Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich'*, Inaugural-Dissertation, Erlangen, 1916.

[32] F. Seidelmann, 'Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich', *Math. Annalen*, **18**, 1918, 230–233.

[33] C.L. Siegel, 'Algebraische Abhängigkeit von Wurzeln', *Acta Arithmetica*, **21**, 1972, 59–64.

[34] P. Stevenhagen, 'Hilbert's 12th problem, complex multiplication and Shimura reciprocity', Class field theory–its centenary and prospect, *Advanced Studies in Pure Mathematics*, **30**, 2001, 161–176.

[35] P. Stevenhagen, *Ray class groups and governing fields*, dissertation at Universiteit van Amsterdam, 1989.

[36] M.A. de Orozco, W.Y. Vélez, 'The lattice of subfields of a radical extension', *Journal of Number Theory*, **15**, 1982, 388–405.

[37] G.N. Watson, 'Theorems stated by Ramanujan (VII): Theorems on continued fractions', *Journal of the London Mathematical Society*, **4**, 1929, 39–48.

[38] H. Weber, *Lehrbuch der Algebra, Band III, Second edition*, Chelsea reprint, original edition 1908.

[39] C.A.Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics, Cambridge University Press, Cambridge, 1994.

[40] R. Zippel, 'Simplification of expressions involving radicals', *Journal of Symbolic Computation*, **1**, 1985, 189–210.

Samenvatting

Wiskundigen gebruiken computeralgebrapakketten om lastig rekenwerk voor hen op te knappen. Kenmerkend voor deze pakketten is dat ze symbolisch kunnen rekenen. Een getal als $\sqrt{2}$ wordt niet afgerond op een aantal decimalen, maar wordt weergegeven als een symbool waarvan de computer weet dat het in het kwadraat gelijk aan 2 is. Dit heeft het grote voordeel dat je exacte berekeningen kunt doen. Helaas kleven hier bij berekeningen met wortels ook wel nadelen aan. Er zijn bijvoorbeeld twee getallen die in het kwadraat 2 opleveren: $\sqrt{2}$ en $-\sqrt{2}$. Algebraïsch gezien zijn ze ononderscheidbaar, beide hebben minimumpolynoom $x^2 - 2$. Wil je toch specifiek voor een van deze getallen je berekening doen, dan zul je naast de symbolische weergave ook een numerieke benadering bij moeten houden. Verder kan het rekenen met wortels nodeloos ingewikkelde termen opleveren. Neem nu bijvoorbeeld het getal

$$A = \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}.$$

We bedoelen hier, zoals gebruikelijk, met $\sqrt{5}$ de positieve reële wortel uit het getal 5; ook de twee derdemachtswortels geven hier de unieke reële derdemachtswortel uit de getallen $\sqrt{5} \pm 2$ aan. Ook in de andere voorbeelden in deze samenvatting zullen we alleen de positieve reële wortels uit positieve reële getallen beschouwen. Als je A numeriek benadert lijkt het wel heel veel op het getal 1:

$$\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2} = 1.618033988\ldots - 0.618033988\ldots.$$

Met behulp van symbolisch rekenen kun je laten zien dat A een nulpunt is van het polynoom $x^3 + 3x - 4$, dat gelijk is aan $(x-1)(x^2+x+4)$. Het enige reële nulpunt van dit polynoom is 1, dus geldt $A = 1$.

Graag zou je hebben dat de computer voor je controleert of de uitdrukking eenvoudiger geschreven kan worden. De eerste vraag die hierbij beantwoord moet worden is wat je onder een zo eenvoudig mogelijke uitdrukking verstaat. In het verleden hebben verschillende wiskundigen voorbeelden gegeven van gelijkheden van worteluitdrukkingen ([1], [5], [20], [21], [28], [40]). Zo is de volgende gelijkheid van Richard Zippel ([40]) afkomstig

$$\sqrt[6]{7\sqrt[3]{20} - 19} = \sqrt[3]{5/3} - \sqrt[3]{2/3}.$$

In de uitdrukking aan de rechterkant van het gelijkteken staan minder worteltekens onder elkaar dan in de uitdrukking aan de linkerkant van het gelijkteken; we zullen een worteluitdrukking eenvoudig noemen als er weinig worteltekens onder elkaar staan. We definiëren de worteldiepte van een getal α als het minimum van dit aantal onder elkaar staande worteltekens voor alle worteluitdrukkingen voor α. Zo is dus de worteldiepte van het getal $\sqrt[6]{7\sqrt[3]{20}-19}$ gelijk aan 1: omdat $\sqrt[3]{20}$ niet rationaal is hebben we minstens 1 wortelteken nodig en hierboven zagen we al dat je dit getal in een uitdrukking zonder geneste wortels weer kunt geven.

Susan Landau ([20]) gaf, gebruikmakend van Galoistheorie, een methode om een worteluitdrukking W te berekenen voor een getal van worteldiepte $r \in \mathbb{N}$, zodat in W ten hoogste $r+1$ worteltekens onder elkaar staan.

In specifieke gevallen kun je ook eenvoudige algoritmen geven die een uitdrukking van minimale worteldiepte opleveren. Dit is wat we in het derde en vierde hoofdstuk van dit proefschrift doen voor uitdrukkingen van worteldiepte 2 die uit een enkele term bestaan.

Laat α en β gehele getallen zijn en definieer $B = \sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$. In hoofdstuk 3 laten we, met behulp van de Galoisgroep van de normale afsluiting van $\mathbb{Q}(B)$ over $\mathbb{Q}$, zien dat B te vereenvoudigen is dan en slechts dan als $\sqrt[3]{\alpha}+\sqrt[3]{\beta}$ gelijk is aan het produkt van een kwadraat in $\mathbb{Q}(\sqrt[3]{\alpha},\sqrt[3]{\beta})$ en een eenvoudige factor. Daarmee bewijzen we dat B te vereenvoudigen is dan en slechts dan als óf β/α een derdemacht is óf er gehele getallen m en n zijn met

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}.$$

Als zulke m en n bestaan geven we een formule die ons de vereenvoudiging geeft. Zo vinden we voor $m = n = 1$ bijvoorbeeld

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \tfrac{1}{3}(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}).$$

Algemener definiëren we voor een lichaam K van karakteristiek 0 het lichaam van alle getallen die met worteldiepte 1 over K geschreven kunnen worden:

$$K^{(1)} = K(\{\alpha \in \bar{K} \text{ met } \alpha^n \in K \text{ zekere } n \in \mathbb{Z}_{>0}\}).$$

Laat L een deellichaam van $K^{(1)}$ zijn. We beschouwen elementen van de vorm $\sqrt[n]{\delta}$, met δ in $L \setminus K$. We laten zien dat ook in dit geval $\sqrt[n]{\delta} \in K^{(1)}$ impliceert dat δ een n-de macht in L is vermenigvuldigd met een eenvoudige factor. Zo laten we ook zien dat $\sqrt[3]{1+\sqrt{2}}$ geen element is van $K^{(1)}$: het element $1+\sqrt{2}$ is niet te schrijven als een kwadraat in $\mathbb{Q}(\sqrt{2})$ maal een eenvoudige factor.

Ook de gelijkheid van Zippel geldt omdat $7\sqrt[3]{20}-19$ 'bijna een zesde macht is in het lichaam $\mathbb{Q}(\sqrt[3]{20})$'; er geldt

$$7\sqrt[3]{20}-19 = \frac{1}{144}\left(\sqrt[3]{20}-2\right)^6$$

en we hebben

$$\sqrt[6]{\frac{1}{144}}\left(\sqrt[3]{20}-2\right)=\sqrt[3]{1/12}\left(\sqrt[3]{20}-\sqrt[3]{8}\right)=\sqrt[3]{5/3}-\sqrt[3]{2/3}.$$

Dit 'bijna-n-de macht zijn van een worteluitdrukking' is een voorwaarde voor vereenvoudiging die intuïtief voor de hand ligt. We leiden deze af met behulp van Galoistheorie voor radicaaluitbreidingen. In de eerste twee hoofdstukken van dit proefschrift bestuderen we Galoisgroepen van dit soort uitbreidingen. Laat L over K een lichaamsuitbreiding zijn voortgebracht door n-de machtswortels uit elementen van K voor een zeker positief geheel getal n. Als het grondlichaam K een primitieve n-de eenheidswortel bevat, dan heet de uitbreiding een Kummeruitbreiding. Zo is bijvoorbeeld $\mathbb{Q}(\sqrt{3},\sqrt{5}\,)$ een Kummeruitbreiding voor $n=2$ omdat $\mathbb{Q}$ de primitieve 2-de eenheidswortel -1 bevat. Als we nu W definiëren als de multiplicatieve groep $\langle\mathbb{Q}^*,\sqrt{3},\sqrt{5}\rangle$, dan wordt elk tussenlichaam van $\mathbb{Q}(\sqrt{3},\sqrt{5}\,)$ voortgebracht door een ondergroep W' van W. De tussenlichamen van $\mathbb{Q}(\sqrt{3},\sqrt{5}\,)$ zijn dus

$$\mathbb{Q},\quad \mathbb{Q}(\sqrt{3}\,),\quad \mathbb{Q}(\sqrt{5}\,),\quad \mathbb{Q}(\sqrt{15}\,)\quad\text{and}\quad \mathbb{Q}(\sqrt{3},\sqrt{5}\,).$$

In het algemene geval hebben we een grondlichaam K, met $\zeta_n\in K$ voor een primitieve n-de eenheidswortel ζ_n. Het lichaam L is van de vorm $K(\alpha_1,\alpha_2,\ldots)$ voor $\alpha_i\in\bar{K}$ met $\alpha_i^n\in K$ en W is $\langle K^*,\alpha_1,\alpha_2,\ldots\rangle$. We leiden voor $\delta\in K$ af dat $\sqrt[n]{\delta}$ in L is bevat dan en slechts dan als δ een element van W is.

We bepalen ook de Galoisgroep van uitbreidingen van de vorm

$$L=K(\{\alpha\in\bar{K}\text{ met }\alpha^n\in K\text{ voor zekere }n\in I\}),$$

waarbij I een deelverzameling is van $\mathbb{Z}_{>0}$ zodat $\zeta_n\in K$ voor alle $n\in I$.

Verder bestuderen we de situatie waar het grondlichaam de vereiste eenheidswortels uit Kummertheorie niet bevat. In dit geval schrijven we de Galoisgroep als een semidirekt produkt van twee groepen, een 'Kummerachtige' groep en de Galoisgroep van de uitbreiding voortgebracht door de eenheidswortels uit de verzameling $\{\alpha\in\bar{K}^*:\alpha^n\in K\text{ voor zekere }n\in I\}$.

Wanneer het grondlichaam de vereiste eenheidswortels niet bevat blijk je ook tussenlichamen te kunnen krijgen die niet voortgebracht worden door een ondergroep van de voortbrengende radicalen W. Laat bijvoorbeeld ζ_7 een primitieve 7-de eenheidswortel zijn. Het lichaam $\mathbb{Q}(\zeta_7)$ heeft twee niet-triviale tussenlichamen, die geen van beide door een macht van ζ_7 voortgebracht worden. Toch zijn er ook uitbreidingen, zoals $\mathbb{Q}(\alpha)/\mathbb{Q}$ met $\alpha^4=-3$, waarbij zo'n eenheidswortel niet in het grondlichaam zit en toch alle deellichamen van de verwachte vorm zijn.

In het tweede hoofdstuk bestuderen we het eenvoudigste geval dat op kan treden: we nemen K gelijk aan $\mathbb{Q}$ en beschouwen een uitbreiding voortgebracht door één radicaal α. We karakteriseren de radicalen α waarvoor alle tussenlichamen van $\mathbb{Q}(\alpha)$ voortgebracht worden door een ondergroep van $\langle\mathbb{Q}^*,\alpha\rangle$.

Tot nog toe hebben we het vooral gehad over het vereenvoudigen van worteluitdrukkingen. Echter, het is ook goed mogelijk dat je een getal op een andere wijze gegeven hebt en dat je bijvoorbeeld uit een stelling weet dat er een worteluitdrukking voor gegeven kan worden. Een voorbeeld is dat je het getal gegeven hebt als nulpunt van een oplosbare veelterm. In hoofdstuk 5 kijken we naar zo'n situatie. We bepalen worteluitdrukkingen voor singuliere waarden van de Rogers-Ramanujan kettingbreuk

$$R(z) = q^{\frac{1}{5}} \prod_{n=1}^{\infty} \left(1 - q^n\right)^{\left(\frac{n}{5}\right)};$$

hierbij is z een element uit het complexe bovenhalfvlak, q is $e^{2\pi iz}$ en $\left(\frac{n}{5}\right)$ is een Legendre symbool. We bewijzen dat voor τ een voortbrenger van een orde in een imaginair kwadratisch lichaam geldt dat $R(\tau)$ met een worteluitdrukking weergegeven kan worden. We beschrijven een algemene methode om zo'n worteluitdrukking te bepalen door weer de bijbehorende lichaamsuitbreiding en Galoisgroep uit te rekenen en deze te gebruiken om een worteluitdrukking te construeren. We geven zo'n uitdrukking voor $R(\tau_n)$, met

$$\tau_n = \begin{cases} \sqrt{-n} & \text{indien } n \not\equiv 3 \bmod 4 \\ \frac{5+\sqrt{-n}}{2} & \text{indien } n \equiv 3 \bmod 4 \end{cases}$$

voor $1 \leq n \leq 16$.

Curriculum Vitae

Mascha Honsbeek is geboren op 25 oktober 1971 in Haarlem. Al op jonge leeftijd bleek haar interesse voor rekenen. Een van haar favoriete spelletjes was het cijfersdeel uit het tv-programma 'Cijfers & Letters'.

Tijdens de VWO-opleiding aan het Liemers College te Zevenaar ging haar voorkeur uit naar de bètavakken. Ze rondde de opleiding in 1990 cum laude af.

Geheel naar verwachting ging ze daarna wiskunde studeren aan de Katholieke Universiteit Nijmegen. Naast studeren besteedde ze veel tijd aan sport en aan allerlei activiteiten van de studievereniging Desda. Verder was ze studentassistent en studentlid van de opleidingscommissie wiskunde. Haar scriptie 'Het vereenvoudigen van worteluitdrukkingen', geschreven onder leiding van Frans Keune, was een opstapje voor het onderzoek in dit proefschrift. Ze studeerde af in augustus 1996.

Aansluitend startte ze als AIO met haar promotieonderzoek. Toen deze aanstelling na vier jaar ophield, werd ze coördinator van het door Frans Keune opgestarte project Ratio, waar wiskunde-onderwijs voor het VWO ontwikkeld wordt, en werkte ze als voorlichter van de wiskundestudie aan de KUN. Dit deed ze tot september 2004. In de vrije uurtjes rondde ze het proefschrift af.

Nu is ze een geheel nieuwe carrière begonnen als docente wiskunde aan het Bernard Nieuwentijt College, locatie Damstede, een HAVO-VWO school in Amsterdam Noord.