Mersenne primes and class field theory

Jansen, B.J.H.

Mersenne primes and class field theory

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof.mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 18 december 2012
klokke 15:00 uur

door

Bastiaan Johannes Hendrikus Jansen
geboren te Gouda
in 1977

Samenstelling van de promotiecommissie

Promotor

prof.dr. H.W. Lenstra, Jr.

Copromotor

dr. B. de Smit

Overige leden

prof.dr. F. Beukers (Universiteit Utrecht)
prof.dr. S. J. Edixhoven
dr. F. Lemmermeyer (Universität Heidelberg)
prof.dr. P. Stevenhagen
prof.dr. Tijdeman

Mersenne primes and class field theory

Bas Jansen

Stellingen

Stelling 1
Zij q een positief geheel getal. Laat R_q de ring zijn gedefinieerd door

$$R_q = \bigcup_{\gcd(n,q)=1} \mathbb{Z}[\sqrt[n]{2}],$$

waar n loopt over alle positieve gehele getallen relatief priem met q. Dan is er precies één ringhomomorfisme van R_q naar $\mathbb{Z}/(2^q - 1)\mathbb{Z}$.

Stelling 2
Zij $t \in \bigcup_{n\geq 1} \mathbb{Q}(\sqrt[n]{2})$. Dan is $((-54468-61952\sqrt{2})t^4+(-123904+435744\sqrt{2})t^3+(326808+371712\sqrt{2})t^2+(123904-435744\sqrt{2})t-54468-61952\sqrt{2})/(t^2+1)^2$ een universele startwaarde (zie Definition 2.5).

Stelling 3
Zij $q, n \in \mathbb{Z}_{>1}$, $q \equiv -1 \bmod n$ en $q > 2n-1$. Dan geldt $\left(\frac{\sqrt[n]{2}-1}{M_q}\right) = 1$ (zie Definition 2.4).

Stelling 4
Zij n een positief geheel getal. Laat $\mathfrak{p}$ een priemideaal $\neq (0)$ zijn van $\mathbb{Z}[\sqrt[n]{2}]$ en laat $\mathfrak{P}$ een priemideaal van de ring van gehelen $\mathcal{O}$ van $\mathbb{Q}(\sqrt[n]{2})$ boven $\mathfrak{p}$ zijn. Dan is $\mathbb{Z}[\sqrt[n]{2}]/\mathfrak{p}$ isomorf met $\mathcal{O}/\mathfrak{P}$.

Stelling 5
Het kwadraat van 4103 kan als volgt worden bepaald.

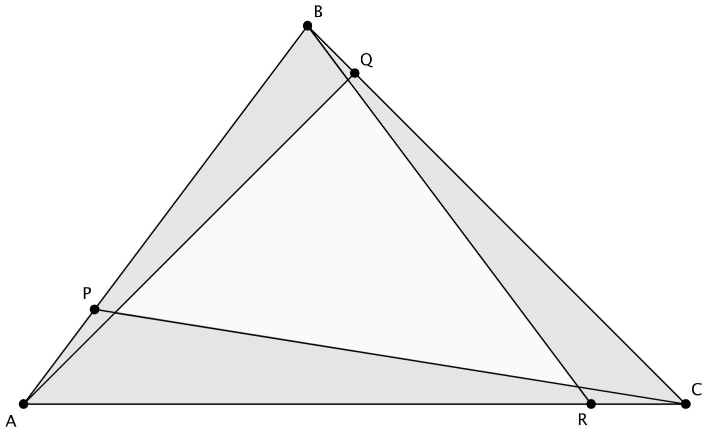
I	vooraan per cijfer één punt plaatsen	.	.	.	.	4	1	0	3
II	een getal naar links schuiven tot het aantal punten links ervan gelijk is aan het aantal cijfers erin; dit herhalen tot het kwadraat van elk los getal eenvoudig te bepalen is	.	4	.	.	.	1	0	3
		.	4	.	.	1	0	.	3
III	kwadrateren van de losse getallen uit II	1	6	.	1	0	0	.	9
IV	voor elk getal in II dat uit elkaar geschoven is in x en y, het getal $2xy$ links van y zetten bv $2 \cdot 4 \cdot 103 = 824$ staat links van 103						6	0	
				8	2	4			
V	getallen uit III en IV optellen	1	6	8	3	4	6	0	9

Het kwadraat van 4103 is 16834609. Deze methode werkt voor alle natuurlijke getallen.

Stelling 6
Zij $m \in \mathbb{Z}_{>0}$, $H_m = \{1/n \in \mathbb{Q} : n \in \mathbb{Z}_{>m}\}$ en V de verzameling van alle eindige deelverzamelingen van H_m. Definieer de functie $f : V \to \mathbb{Q}_{>0}$ door $f : W \mapsto \sum_{x \in W} x$. Dan is voor elke $x \in \mathbb{Q}_{>0}$ het aantal elementen van $f^{-1}(x)$ oneindig.

Stelling 7
Als bij een constructie met passer en liniaal het tekenen van een lijn of cirkel één euro kost, dan kun je een hoek van 15 graden construeren voor vijf euro.

Stelling 8
De oppervlakte van een driehoek ABC met punten P, Q en R op zijden AB, BC en CA respectievelijk zodat $\frac{\mathrm{AP}}{\mathrm{PB}} = \frac{1}{3}$, $\frac{\mathrm{BQ}}{\mathrm{QC}} = \frac{1}{6}$ en $\frac{\mathrm{CR}}{\mathrm{RA}} = \frac{1}{7}$ is twee keer zo groot als de oppervlakte ingesloten door de lijnstukken AQ, BR en CP (zie figuur).



De oppervlakte van driehoek ABC is twee keer zo groot als de oppervlakte van de lichtgrijze driehoek in het midden.

Abstract

Mersenne numbers are positive integers of the form $M_q = 2^q - 1$ with $q \in \mathbb{Z}_{>1}$. If a Mersenne number is prime then it is called a Mersenne prime. The Lucas-Lehmer-test is an algorithm that checks whether a Mersenne number is a prime number. The test is based on the following theorem.

Theorem (Lucas-Lehmer-test). *Let $q \in \mathbb{Z}_{>1}$ and let $s \in \mathbb{Z}/M_q\mathbb{Z}$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1, 2, \ldots, q-1\}$ by $s_1 = s$ and $s_{i+1} = s_i^2 - 2$. Then one has $s_{q-1} = 0$ if and only if M_q is prime and the Jacobi symbols $\left(\frac{s-2}{M_q}\right)$ and $\left(\frac{-s-2}{M_q}\right)$ are both* 1.

In practice one applies the Lucas-Lehmer-test only if q is a prime number, because $2^q - 1$ is composite if q is composite. To apply the Lucas-Lehmer-test one chooses a value $s \in \mathbb{Z}/M_q\mathbb{Z}$ for which $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$ holds. Then to find out whether M_q is prime, it suffices to calculate s_{q-1} and verify whether it is zero.

Familiar values that one can use for $q \neq 2$ are $s = (4 \bmod M_q)$ and $s = (10 \bmod M_q)$. If q is odd we can use the less familiar value $s = (2 \bmod M_q)(3 \bmod M_q)^{-1}$, which is denoted by $s = (2/3 \bmod M_q)$. Two examples of new values that can be used if q is odd are

$$s = \left(\frac{626}{363} \bmod M_q\right) \text{ and } s = \left(\frac{238}{507} + \frac{160}{169}\sqrt{2} \bmod M_q\right)$$

where $(\sqrt{2} \bmod M_q)$ is defined to be $(2^{(q+1)/2} \bmod M_q)$. The condition on q guarantees that $(2^{(q+1)/2} \bmod M_q)$ and the inverses of $(363 \bmod M_q)$, $(507 \bmod M_q)$ and $(169 \bmod M_q)$ are well-defined. In this thesis we will give a formula that produces infinitely many values in the field $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ that, when suitably interpreted modulo M_q, can be used to apply the Lucas-Lehmer-test.

Lehmer observed in the case $s_{q-1} = 0$ with q odd that s_{q-2} is either $+2^{(q+1)/2}$ or $-2^{(q+1)/2}$. In that case we define *the Lehmer symbol* $\epsilon(s, q) \in \{+1, -1\}$ by $s_{q-2} = \epsilon(s, q)2^{(q+1)/2}$. The main object of study in this thesis is the Lehmer symbol. At the moment the fastest way to calculate the sign $\epsilon(s, q)$ in the case $s = (4 \bmod M_q)$ for a Mersenne prime M_q is to calculate the sequence $s_1, s_2, \ldots, s_{q-2}$. In 2000 however S.Y. Gebre-Egziabher showed that in the case $s = (2/3 \bmod M_q)$ and $q \neq 5$ we have $\epsilon(s, q) = 1$ if and only if

$q \equiv 1 \bmod 4$. The first main result of this thesis yields a similar result for every $s \in K$ with the property that $4 - s^2$ is a square in K. That includes the result of Gebre-Egziabher, since for $s = 2/3$ one has $4 - s^2 = (4\sqrt{2}/3)^2$. Another example is the following theorem.

Theorem A. *Let $q \in \mathbb{Z}_{>1}$ with $q \neq 2, 5$ be such that M_q is prime. Let $s = (\frac{626}{363} \bmod M_q)$. Then $\epsilon(s, q) = 1$ if and only if $q \equiv 1$, 7, 9 or 13 mod 20.*

In 1996 G. Woltman conjectured that for $q \neq 2, 5$ the equation

$$\epsilon(4 \bmod M_q, q) \cdot \epsilon(10 \bmod M_q, q) = 1$$

holds if and only if $q \equiv 5$ or $7 \bmod 8$. Woltman's conjecture was proved four years later by Gebre-Egziabher. A generalization of this theorem is the second main result of this thesis. It gives sufficient conditions for two values s and t in K to give rise to a relation similar to Woltman's conjecture. These conditions are awkward to state, but they are similar to the conditions on s in the first main result. The second main result implies the following theorem.

Theorem B. *Let $s = \frac{1108}{529}$ and $t = \frac{5476}{529}$. Then*

$$\epsilon(s \bmod M_q, q) \cdot \epsilon(t \bmod M_q, q) = 1 \text{ if and only if } q \equiv 3, 4, 6, 9 \text{ or } 10 \bmod 11.$$

In the proofs of both main results we express the Lehmer symbol $\epsilon(s, q)$, for $s \in K$ interpretable in the ring $\mathbb{Z}/M_q\mathbb{Z}$ in the manner suggested above, in terms of the Frobenius symbol of a Mersenne prime $2^q - 1$ in a certain number field depending *only* on s. Then we can use the Artin map from class field theory to control the Frobenius symbol and hence the Lehmer symbol.

It is of interest to know whether the converses of both main results hold. Thus, if $s \in K$ is such that $\epsilon(s \bmod M_q, q)$ is a "periodic" function of q as in Theorem A, is $4 - s^2$ necessarily a square in K? This is currently beyond proof, but we will formulate a *working hypothesis* that implies an affirmative answer. Given a finite Galois extension of $\mathbb{Q}$, the working hypothesis tells us which conjugacy classes in the Galois group appear infinitely many times as the Frobenius symbol of a Mersenne prime. A strong necessary condition arises from the Artin map and the splitting behavior of Mersenne primes in the fields $\mathbb{Q}(\sqrt[n]{2})$ for $n \in \mathbb{Z}_{>0}$. The working hypothesis states that this condition is also sufficient. Restricted to abelian extensions of $\mathbb{Q}$, the working hypothesis may be reformulated as follows: for every pair of relatively prime integers $a, b \in \mathbb{Z}_{>0}$ there are infinitely many prime numbers q with $q \equiv a \bmod b$ such that $2^q - 1$ is a Mersenne prime. One might view this as Dirichlet's "theorem" for Mersenne primes.

Assuming the working hypothesis, we can prove that for the value $s = 4$ there do not exist positive integers m and n with the property that for any $p, q \in \mathbb{Z}_{>m}$ with M_p and M_q prime and $p \equiv q \bmod n$ one has $\epsilon(4, p) = \epsilon(4, q)$. The same applies to any $s \in K$ for which $4 - s^2$ is not a square in K. We prove a similar statement for the second main result assuming the working hypothesis.

Contents

Chapter 1

Introduction

Background

One of the most famous mathematical texts is the *Elements*, written by Euclid 300 B.C.. This work consist of 13 books. In Definition 22 of book VII he defines a number to be perfect if the sum of its proper divisors equals the number itself. For example 6 is a perfect number, since $1 + 2 + 3 = 6$. Also 28 is perfect because $1+2+4+7+14 = 28$. Two other perfect numbers were known to the Greeks, namely 496 and 8128. These four perfect numbers could be found using the following theorem of Euclid: for any $q \in \mathbb{Z}_{>0}$ for which $2^q - 1$ is prime, the number $2^{q-1}(2^q-1)$ is perfect (Euler (1707–1783) proved that every even perfect number is of this form). Hence finding even perfect numbers is equivalent to finding primes of the form $2^q - 1$ with $q \in \mathbb{Z}$. The fifth perfect number was found around 1456 by someone who remains unknown. Pietro Cataldi (1552–1626) found the next two perfect numbers. He also proved that $q \in \mathbb{Z}_{>0}$ is prime if $2^q - 1$ is prime. Marin Mersenne (1588–1648) claimed that

$$\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$$

is the list of all $q \in \mathbb{Z}_{>0}$ smaller than 258 for which $2^{q-1}(2^q - 1)$ is perfect. His claim is false only because $2^{67} - 1$ and $2^{257} - 1$ are composite and $2^{61} - 1$, $2^{89} - 1$ and $2^{107} - 1$ are prime. Nowadays, nevertheless, primes of the form $2^q - 1$ with $q \in \mathbb{Z}_{>0}$ are called *Mersenne primes*. Euler proved that $2^{31} - 1$ is prime by using a corollary of one of his theorems, namely prime divisors of $2^{31} - 1$ are 1 modulo 31. Until Edouard Lucas (1842–1891) no other Mersenne primes were found. By applying his very fast test, Lucas was able to show that $2^{127} - 1$ is prime. Later, Derrick Lehmer (1905–1991) extended Lucas's test. The main problem of the present thesis derives from the Lucas-Lehmer-test, which still produces the largest known primes nowadays (see appendix).

Theorem. *Let $q \in \mathbb{Z}_{>2}$ be an integer. Define $s_i \in \mathbb{Z}/(2^q - 1)\mathbb{Z}$ for $i \in \{1, 2, \ldots, q - 1\}$ by $s_1 = 4$ and $s_{i+1} = s_i^2 - 2$. Then $2^q - 1$ is prime if and only if $s_{q-1} = 0$.*

To illustrate the Lucas-Lehmer-test we will apply the test to $q = 5$. In the ring $\mathbb{Z}/31\mathbb{Z}$ we have

$$\begin{aligned} s_1 &= 4, \\ s_2 &= 4^2 - 2 = 14, \\ s_3 &= 14^2 - 2 = 194 = 8, \\ s_4 &= 8^2 - 2 = 62 = 0. \end{aligned}$$

Since $s_4 = 0$, we conclude that 31 is a Mersenne prime. Lehmer observed: if $s_{q-1} = 0$ and q is odd then s_{q-2} is either $+2^{(q+1)/2}$ or $-2^{(q+1)/2}$ (see Proposition 5.1). The Lehmer symbol $\epsilon(4, q) \in \{+1, -1\}$ is defined for $q \in \mathbb{Z}_{>0}$ odd for which $M_q = 2^q - 1$ is prime by $s_{q-2} = \epsilon(4, q)2^{(q+1)/2}$. From the example above we read that the Lehmer symbol $\epsilon(4, 5)$ is $+1$, since $s_3 = +2^3$. We can also start the Lucas-Lehmer-test with $s_1 = 10$ instead of $s_1 = 4$. As in the case $s = 4$ the Lehmer symbol $\epsilon(10, n) \in \{+1, -1\}$ is defined for $q \in \mathbb{Z}_{>0}$ odd for which M_q is prime by $s_{q-2} = \epsilon(10, q)2^{(q+1)/2}$. The following table shows the Lehmer symbols $\epsilon(4, q)$ and $\epsilon(10, q)$ for q up to 521.

q	3	5	7	13	17	19	31	61	89	107	127	521
$\epsilon(4, q)$	$+$	$+$	$-$	$+$	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$
$\epsilon(10, q)$	$-$	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$

In 1996 George Woltman (1957) conjectured a relation between the table for $s = 4$ and the table for $s = 10$, namely these tables show the same sign if and only if $q \equiv 5$ or 7 modulo 8 and $q \neq 5$. Four years later S.Y. Gebre-Egziabher proved the conjecture of Woltman (see [3]). Moreover he showed that one can also start the Lucas-Lehmer-test with the rational value $s = 2/3$ and that the sign table of $s = 2/3$ is easy to write down since the sign is '+' if and only if q is 1 modulo 4 and $q \neq 5$. Of course "2/3 modulo M_q" is defined by $(2 \bmod M_q)(3 \bmod M_q)^{-1}$. In this thesis we generalize these results of Gebre-Egziabher.

Main results

Define $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$. Let $q \in \mathbb{Z}_{>1}$ and recall $M_q = 2^q - 1$. For every $s \in K$ there exists a non-zero integer k_s such that for all $q \in \mathbb{Z}_{>1}$ with $\gcd(q, k_s) = 1$ we can define a natural ring homomorphism $\mathbb{Z}[s] \to \mathbb{Z}/M_q\mathbb{Z}$ (see first paragraph of Chapter 2). This ring homomorphism allows us to use starting values of K for the Lucas-Lehmer-test. We call $s \in K$ a universal starting value if s can be used as a starting value in the Lucas-Lehmer-test for almost all prime numbers q (see Definition 2.5). The elements $4, 10$ and $2/3$ of K are examples of universal starting values. A new example of a universal starting value is $s = \frac{238}{507} + \frac{160}{169} \cdot \sqrt{2}$. Example 2.7 gives an infinite family of universal starting values. Moreover we show in Chapter 2 how one can make more families of universal starting values (see Theorem 2.9).

For every universal starting value s we can study the Lehmer symbol $\epsilon(s,q)$ (see Definition 5.2). The following theorem is the first main result of this thesis.

Theorem. *Let $s \in K$. Suppose $4 - s^2$ is a square in K^*. Then there exist positive integers l and m such that $\epsilon(s,p) = \epsilon(s,q)$ if $p, q \geq l$ and $p \equiv q \bmod m$. Moreover l and m are easy to compute by Theorem 7.5.*

Gebre-Egziabher's result for the universal starting value $s = 2/3$ described above follows from this theorem. Indeed, $4 - (2/3)^2$ equals $(4\sqrt{2}/3)^2 \in K^{*2}$. Other examples are Corollary 7.3, Corollary 7.6, Corollary 7.7 and Corollary 7.8. More examples can easily be made by taking a equal to b in Theorem 2.9.

Next we will describe a generalisation of Gebre-Egziabher's result on the conjecture of Woltman for related pairs of potential starting values (see Definition 8.1). An example of a related pair of potential starting values is 4 and 10. The following theorem is the second main result of this thesis.

Theorem. *Let $s, t \in K$ be a related pair of potential starting values. Suppose $(2 + \sqrt{2+s})(2 + \sqrt{2+t})$ is a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$. Then there exist positive integers l and m such that $\epsilon(s,p) \cdot \epsilon(t,p) = \epsilon(s,q) \cdot \epsilon(t,q)$ if $p, q \geq l$ and $p \equiv q \bmod m$. Moreover l and m are easy to compute by Corollary 9.4.*

Since $(2 + \sqrt{2+4})(2 + \sqrt{2+10})$ equals $(\sqrt[4]{2}(1 + \sqrt{2} + \sqrt{3}))^2 \in K(\sqrt{6}, \sqrt{-2})^{*^2}$, this theorem implies Woltman's conjecture. Other examples are Corollary 9.5 and Corollary 9.6.

Let $s \in K$. If for only finitely many $q \in \mathbb{Z}_{>1}$ the Lehmer symbol $\epsilon(s,q)$ is defined, then the two theorems above trivially hold. This is the case when there are only finitely many Mersenne primes or s is a starting value for only finitely many $q \in \mathbb{Z}_{>1}$ (for example $s = 5$ is not a starting value for any q). One might wonder if the two theorems above allow a converse for universal starting values if one assumes that there are infinitely many Mersenne primes. We were able to prove a weaker theorem (see two theorems below) by assuming a stronger hypothesis on Mersenne primes. We call this hypothesis the working hypothesis.

The working hypothesis roughly says that the only restrictions for Frobenius symbols of Mersenne primes in a finite Galois extension of $\mathbb{Q}$ come from abelian extensions of K. Let $L = \mathbb{Q}(\zeta_8, \sqrt[8]{5})$. The precise statement of the working hypothesis for the extension $L/\mathbb{Q}$ is: for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ with $\sigma|_{\mathbb{Q}(\zeta_8)}$ the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}))$ there are infinitely many Mersenne primes M_p such that the Frobenius symbol of M_p in the extension $L/\mathbb{Q}$ equals the conjugacy class of σ in $\mathrm{Gal}(L/\mathbb{Q})$. This statement is partly motivated by the fact that the Artin symbol of the prime ideal $(\sqrt[v]{2}^p - 1)$ in the abelian extension $\mathbb{Q}(\zeta_8, \sqrt{5})/\mathbb{Q}(\sqrt{2})$ is non-trivial. There are no other conditions for the Frobenius symbol of M_p in $L/\mathbb{Q}$ that we can come up with. The following two theorems can been seen as the converses of the two main results above.

Theorem. *Let $s \in K$ be a universal starting value. Suppose $4 - s^2$ is not a square in K^* and suppose that there exist positive integers l and m such that*

$\epsilon(s,p) = \epsilon(s,q)$ if $p, q \geq l$ and $p \equiv q \bmod m$. Then the working hypothesis is false.

Theorem. *Let $s, t \in K$ be a related pair of potential starting values and suppose both s and t are universal starting values. Suppose $(2+\sqrt{2+s})(2+\sqrt{2+t})$ is a not a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$ and suppose that there exist positive integers l and m such that $\epsilon(s,p) \cdot \epsilon(t,p) = \epsilon(s,q) \cdot \epsilon(t,q)$ if $p, q \geq l$ and $p \equiv q \bmod m$. Then the working hypothesis is false.*

Sketch of the proofs of the main results

Denote the Jacobi symbol by $\left(\frac{\cdot}{\cdot}\right)$ (see [1, §1, page 16]). Let $q \in \mathbb{Z}_{>1}$ and $M_q = 2^q - 1$. Let $s \in \mathbb{Z}/M_q\mathbb{Z}$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1, 2, \ldots, q-1\}$ by $s_1 = s$ and $s_{i+1} = s_i^2 - 2$. Then we have

$$s_{q-1} = 0 \Longleftrightarrow M_q \text{ is prime and } \left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$$

(see Theorem 2.1). In the proof of Theorem 2.1 we show that

$$s_{q-1} = 0 \Longrightarrow R = (\mathbb{Z}/M_q\mathbb{Z})[x]/(x^2 - sx + 1) \text{ is a field.}$$

From the definition of R one easily deduces the equalities

$$s_{i+1} = s_i^2 - 2 = x^{2^i} + x^{-2^i} \tag{1.1}$$

in R (see proof of Theorem 2.1). Suppose $s_{q-1} = 0$. Then the Lehmer symbol $\epsilon(s,q)$ is defined and R is a field. Equation (1.1) enables us to link the Lehmer symbol to the Frobenius automorphism $\mathrm{Frob} : x \mapsto x^{M_q}$ in an extension R' of R which contains an element y such that $y^8 = x$ (see proof of Theorem 5.6). Indeed, in R' we have

$$\epsilon(s,q)2^{\frac{q+1}{2}} = s_{q-2} = x^{2^{q-3}} + x^{-2^{q-3}} = y^{2^q} + y^{-2^q} = \mathrm{Frob}(y)y + \mathrm{Frob}(y^{-1})y^{-1}.$$

Next we study this Frobenius symbol in an extension of global fields. Let M_p be a Mersenne prime. Let $s \in K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ be a universal starting value such that s is a starting value for p. Let L_s be the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}(s)$ and let $K_s = L_s \cap K = \mathbb{Q}(\sqrt[n]{2})$. Note that a zero of f_s has the same algebraic properties as the element $y \in R'$ above. The equation in R' above shows that the Frobenius symbol of the prime ideal $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$ of K_s in L_s/K_s determines the Lehmer symbol $\epsilon(s,p)$. In the case $4 - s^2 \in K^{*2}$ the extension L_s/K_s is abelian. Hence we can determine the Frobenius symbol of $\mathfrak{m}_p$ easily via the Artin map. The integers l and m of the first main result stated above can be calculated using the conductor of L_s/K_s.

Next we describe the outline of the second main result. Let M_p be a Mersenne prime. Let $s, t \in K$ be a related pair of potential starting values and suppose that both s and t are universal starting values such that both s and t

are starting values for p. Let $L_{s,t} = L_s L_t$ and let $K_{s,t} = L_{s,t} \cap K = \mathbb{Q}(\sqrt[n]{2})$. The subgroup of $\mathrm{Gal}(L_{s,t}/K_{s,t})$ generated by the Frobenius symbol of any prime ideal of $L_{s,t}$ above of the prime ideal $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$ of $K_{s,t}$ in $L_{s,t}/K_{s,t}$ determines the product of Lehmer symbols $\epsilon(s,p) \cdot \epsilon(t,p)$. In the case that $(2+\sqrt{2+s})(2+\sqrt{2+t})$ is a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$ we can study this subgroup in an abelian extension of $K_{s,t}$. We can use the Artin symbol of $\mathfrak{m}_p$ to determine the subgroup and hence the value of $\epsilon(s,p) \cdot \epsilon(t,p)$. Similarly as above the conductor of this abelian extension of $K_{s,t}$ can be used to calculate the integers l and m in the second main result described above.

Overview of the chapters

In Chapter 2 we treat the Lucas-Lehmer-test and create families of universal starting values.

In Chapter 3 we define potential starting values $s \in K$ and show that if s is a starting value for some odd positive integer q, then s is a potential starting value. Potential starting values have some properties of universal starting values but their definition does not depend on Mersenne numbers.

In Chapter 4 we construct for potential starting values $s \in K$ a Galois extension and we define a map λ_s that maps certain elements of this Galois group to a sign. This map λ_s allows us to express the Lehmer symbol in terms of the Frobenius symbol

In Chapter 5 we make a connection between the Lehmer symbol $\epsilon(s,p)$ and the Frobenius symbol via a commutative diagram with the map λ_s.

In Chapter 6 we state the sufficient properties of the Artin map and we prove a theorem to estimate conductors.

In Chapter 7 we apply the connection made in Chapter 5 and the Artin map in order to prove the first main result of this thesis.

In Chapter 8 we construct a Galois extension for a related pair of potential starting values and we define a map $\lambda'_{s,t}$ that maps certain elements of this Galois group to a sign.

In Chapter 9 we make a connection between the product of two Lehmer symbols $\epsilon(s,p) \cdot \epsilon(t,p)$ and the Frobenius symbol via a commutative diagram with the map $\lambda'_{s,t}$. We use this diagram to prove the second main result of this thesis.

In Chapter 10 we introduce the working hypothesis for abelian extension over $\mathbb{Q}$.

In Chapter 11 we state the working hypothesis and reformulate it so that it can easily be applied in the next Chapter.

In Chapter 12 we prove, assuming the working hypothesis, the converse of the two main results of this thesis.

Chapter 2

The Lucas-Lehmer-test

In this chapter we discuss the Lucas-Lehmer-test, which is a primality test for integers of the form $M_q = 2^q - 1$, where $q \in \mathbb{Z}_{>1}$. To apply the test one calculates a sequence of elements in $\mathbb{Z}/(2^q - 1)\mathbb{Z}$ by iterating the map $x \mapsto x^2 - 2$ on a suitable *starting value* $s \in \mathbb{Z}/(2^q - 1)\mathbb{Z}$. The integer $2^q - 1$ is prime if after $q - 2$ iterations we get 0. Starting values will be obtained from a certain field K of algebraic numbers. This field has the property that any given element can be interpreted in $\mathbb{Z}/(2^q - 1)\mathbb{Z}$ for all $q \in \mathbb{Z}_{>1}$ relatively prime to some integer. Certain well-chosen elements in K can be used as starting values for each M_q with q relatively prime to some fixed integer. These well-chosen starting values will in Definition 2.5 be called *universal starting values.* The classical examples of universal starting values are $4, 10 \in \mathbb{Z}$. We will construct infinitely many additional universal starting values in K.

Many starting values

Denote the Jacobi symbol by $\left(\frac{\cdot}{\cdot}\right)$ (see [1, §1, page 16]).

Theorem 2.1. *Let $q \in \mathbb{Z}_{>1}$ and $M_q = 2^q - 1$. Let $s \in \mathbb{Z}/M_q\mathbb{Z}$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1, 2, \ldots, q-1\}$ by $s_1 = s$ and $s_{i+1} = s_i^2 - 2$. Then we have*

$$s_{q-1} = 0 \Longleftrightarrow M_q \textit{ is prime and } \left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1.$$

The Lucas-Lehmer-test (Theorem 2.1) will be proved in the next section. To illustrate this theorem we give the example $q = 7$ and $s = (4 \bmod 127)$. We calculate

$$\begin{aligned}
s_1 &= 4, \\
s_2 &= 4^2 - 2 = 14, \\
s_3 &= 14^2 - 2 = 194 = 67, \\
s_4 &= 67^2 - 2 = 4487 = 42,
\end{aligned}$$

$$\begin{aligned} s_5 &= 42^2 - 2 = 1762 = -16, \\ s_6 &= (-16)^2 - 2 = \ 254 = 0 \end{aligned}$$

in the ring $\mathbb{Z}/127\mathbb{Z}$. Hence using the theorem we conclude that 127 is prime and that $\left(\frac{2}{127}\right) = \left(\frac{-6}{127}\right) = 1$.

To apply Theorem 2.1 as a prime test one uses an element $s \in \mathbb{Z}/M_q\mathbb{Z}$ such that $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$. Such an element is called a *starting value for q*. With the quadratic reciprocity laws (see [2, Introduction]) one calculates that for the numbers $s = (4 \bmod M_q)$ and $s = (10 \bmod M_q)$ we have $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$ for all odd integers $q \in \mathbb{Z}_{>1}$. It follows that the numbers $s = (4 \bmod M_q)$ and $s = (10 \bmod M_q)$ are starting values for all odd integers $q \in \mathbb{Z}_{>1}$. In the same way one can show that number $s = (2 \bmod M_q)(3 \bmod M_q)^{-1}$ found by S.Y. Gebre-Egziabher is a starting value for all odd integers $q \in \mathbb{Z}_{>0}$ (see [3]). We prefer to denote $(2 \bmod M_q)(3 \bmod M_q)^{-1}$ by $(\frac{2}{3} \bmod M_q)$. In this case q is assumed to be odd to make sure that division by $(3 \bmod M_q)$ is possible. Below we will express the properties of 4, 10, and 2/3 just described, by saying that these numbers are universal starting values. Later we show that the number $s = (\frac{238}{507} + \frac{160}{169} \cdot 2^{(q+1)/2} \bmod M_q)$ is also a starting value for all odd $q \in \mathbb{Z}_{>1}$. Since $(2^{(q+1)/2} \bmod M_q)$ is a square root of $(2 \bmod M_q)$, we will denote s by $(\frac{238}{507} + \frac{160}{169} \cdot \sqrt{2} \bmod M_q)$. Hence we have the following example.

Example 2.2. *The number $s = \frac{238}{507} + \frac{160}{169} \cdot \sqrt{2}$ is a universal starting value.*

To make all this precise, we define K to be the subfield of the field $\mathbb{R}$ of real numbers obtained by adjoining all positive real roots of 2 to $\mathbb{Q}$, so $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ with $\sqrt[n]{2} \in \mathbb{R}$ the positive zero of the polynomial $x^n - 2$. We write $\sqrt{2}$ for $\sqrt[2]{2}$. We proceed to show that for every $s \in K$ there exists a positive integer k_s such that $s \bmod M_q$ has a natural meaning whenever q is relatively prime to k_s.

We fix $q \in \mathbb{Z}_{>1}$ and construct a large subring of K that maps to $\mathbb{Z}/(2^q - 1)\mathbb{Z}$. Define the ring R_q by

$$R_q = \bigcup_{\gcd(n,q)=1} \mathbb{Z}[\sqrt[n]{2}],$$

where n runs over all positive integers relatively prime to q. There is a unique ring homomorphism φ_q from R_q to $\mathbb{Z}/M_q\mathbb{Z}$ that sends $\sqrt[n]{2}$ to 2^a, where $a \in \mathbb{Z}_{>0}$ is such that $an \equiv 1 \mod q$. Note that $2^a \mod M_q$ is an n-th root of $2 \mod M_q$, since $(2^a)^n = (2^q)^{(an-1)/q} \cdot 2 \equiv 2 \bmod M_q$. Let $(\mathbb{Z}/M_q\mathbb{Z})^*$ be the group of units of $\mathbb{Z}/M_q\mathbb{Z}$ and denote the multiplicatively closed subset $\varphi_q^{-1}((\mathbb{Z}/M_q\mathbb{Z})^*)$ of R_q by S_q. Clearly we can extend φ_q uniquely to a ring homomorphism from the ring $S_q^{-1}R_q = \{\frac{v}{w} \in K : v \in R_q \text{ and } w \in S_q\}$ to $\mathbb{Z}/M_q\mathbb{Z}$, which we again denote by φ_q.

The following theorem, which will be proved in the next section, leads directly to our definition of $s \bmod M_q$.

Theorem 2.3. *For every $s \in K$ there exists a non-zero integer k_s such that for all $q \in \mathbb{Z}_{>1}$ with $\gcd(q, k_s) = 1$ we have $s \in S_q^{-1}R_q$.*

We motivate Theorem 2.3 with the universal starting value s of Example 2.2. So let s be as in Example 2.2. We can choose $k_s = 2$. To illustrate this we show that $s \in S_q^{-1}R_q$ for $q \in \mathbb{Z}_{>1}$ odd. The integer k_s is relatively prime to q. Therefore $\sqrt{2}$ is an element of R_q. The map $\varphi_q : R_q \to \mathbb{Z}/(2^q-1)\mathbb{Z}$ sends $\sqrt{2}$ to $(2^{(q+1)/2} \bmod 2^q - 1)$. The only prime divisors of 169 and 507 are 3 and 13. The multiplicative orders of $(2 \bmod 3)$ and $(2 \bmod 13)$ are 2 and 12 respectively. Since both orders are divisible by k_s, it follows that neither 3 nor 13 divides $2^q - 1$ for q relatively prime to k_s. This implies that both $(3 \bmod 2^q - 1)$ and $(13 \bmod 2^q - 1)$ are elements of $(\mathbb{Z}/(2^q-1)\mathbb{Z})^*$. Therefore the multiplicative set S_q contains the elements 3 and 13. Hence $s \in S_q^{-1}R_q$. In particular one can calculate that $\varphi_5(s)$ equals

$$(21 \bmod 31)(11 \bmod 31)^{-1} + (5 \bmod 31)(14 \bmod 31)^{-1}(2^3 \bmod 31)$$

which is $(10 \bmod 31)$.

Definition 2.4. *Let $q \in \mathbb{Z}_{>1}$ be an integer and let $s \in S_q^{-1}R_q$. We define $(s \bmod M_q) \in \mathbb{Z}/M_q\mathbb{Z}$ and $\left(\frac{s}{M_q}\right)$ by*

$$(s \bmod M_q) = \varphi_q(s) \text{ and } \left(\tfrac{s}{M_q}\right) = \left(\tfrac{\varphi_q(s)}{M_q}\right).$$

By the phrase “for almost all” we mean that a finite number of exceptions are allowed. For the next definition it is useful to note that if $s \in K$ then for almost all prime numbers p we have $s \in S_p^{-1}R_p$ (see Theorem 2.3).

Definition 2.5. *Let $q \in \mathbb{Z}_{>1}$. A starting value for q is an element $s \in S_q^{-1}R_q$ with the property $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$. We call s a universal starting value if s is a starting value for almost all prime numbers.*

To prove Example 2.2 one verifies the equalities

$$s - 2 = \frac{(24-10\sqrt{2})^2}{-3 \cdot 13^2},$$

$$-s - 2 = \frac{(10+24\sqrt{2})^2}{-3 \cdot 13^2},$$

and $\left(\frac{-3}{M_q}\right) = 1$ for $q \in \mathbb{Z}_{>1}$ odd, and then one applies the multiplicative property of the Legendre symbol to conclude that

$$\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1.$$

Hence the value of s in Example 2.2 is a universal starting value.

For a universal starting value s we call a prime number p *bad* if s is not a starting value for p. For the universal starting value of Example 2.2 only 2 is a bad prime. From Theorem 2.1 and the fact that M_q is prime only if q is prime, one easily derives the following theorem, which justifies the term ‘universal starting value’ in Definition 2.5.

Theorem 2.6. *Let $s \in K$ be a universal starting value, let $k_s \in \mathbb{Z}_{>0}$ be as in Theorem 2.3, let $q \in \mathbb{Z}_{>1}$ be an integer relatively prime to k_s and q not a bad prime, and let $M_q = 2^q - 1$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1, 2, \ldots, q-1\}$ by $s_1 = (s \bmod M_q)$ and $s_{i+1} = s_i^2 - 2$. Then we have*

$$s_{q-1} = 0 \Leftrightarrow M_q \text{ is prime.}$$

In the next section we prove Theorem 2.6. The proof shows that the theorem is also valid with the condition $\gcd(k_s, q) = 1$ replaced by the weaker condition $s \in S_q^{-1} R_q$.

We illustrate Theorem 2.6 with the universal starting value s of Example 2.2 and $q = 5$. We already showed that $s_1 = (10 \bmod 31)$. The next values in the sequence are $s_2 = s_1^2 - 2 = (5 \bmod 31)$, $s_3 = s_2^2 - 2 = (23 \bmod 31)$ and $s_4 = s_3^2 - 2 = (0 \bmod 31)$. Theorem 2.6 implies that M_5 is prime.

In the last section of the present chapter we describe a method to construct families of universal starting values. The following example is made with this method.

Example 2.7. *For every $t \in K$ the element*

$$4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2}$$

is a universal starting value.

In the next section we prove Example 2.7 using the two equalities

$$4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2} - 2 = \frac{(\sqrt{2}(t^2 + 2\sqrt{2}t - 1))^2}{(t^2 - \sqrt{2}t - 1)^2},$$

$$-4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2} - 2 = \frac{-3(\sqrt{2}(t^2 + 1))^2}{(t^2 - \sqrt{2}t - 1)^2}$$

and $\left(\frac{-3}{M_q}\right) = 1$ for $q \in \mathbb{Z}_{>0}$ odd. Taking $t = 0$ and $t = 1$ in Example 2.7 we obtain the two well-known universal starting values 4 and 10 respectively.

Correctness of the Lucas-Lehmer-test

In this section we prove Theorem 2.1, Theorem 2.3, Theorem 2.6, and Example 2.7. We start with a lemma that will be applied in the proof of Theorem 2.1.

Lemma 2.8. *Let $R \neq 0$ be a finite commutative ring. Suppose that for all ideals $\mathfrak{a} \neq R$ of R we have $\#\mathfrak{a} < \sqrt{\#R}$. Then R is a field.*

Proof. Take $x \in R$. Define $\mathfrak{a} = \{r \in R : rx = 0\}$. Then we have $\#Rx = [R : \mathfrak{a}]$, so $\#Rx \cdot \#\mathfrak{a} = \#R$. Since Rx and $\mathfrak{a}$ are both ideals, it follows by our assumption that either $Rx = R$ or $\mathfrak{a} = R$. Hence either $x \in R^*$ or $x = 0$. Since R is also commutative, we conclude that R is a field. □

Proof of Theorem 2.1. Let $M = M_q$. Define the ring R by

$$R = (\mathbb{Z}/M\mathbb{Z})[x]/(x^2 - sx + 1).$$

The equality $x^2 - sx + 1 = 0$ in R implies $x \in R^*$ and $s = x + x^{-1}$. Hence from $s_1 = s = x + x^{-1}$ and $s_{i+1} = s_i^2 - 2$ we get $s_i = x^{2^{i-1}} + x^{-2^{i-1}}$ for all $i \geq 1$, and in particular

$$s_{q-1} = x^{2^{q-2}} + x^{-2^{q-2}}. \tag{2.1}$$

The straightforward calculation $(x-1)^2 = x^2 - 2x + 1 = sx - 2x = (s-2)x$ shows that

$$(x-1)^2 = (s-2)x. \tag{2.2}$$

Assume that R is a field. Then M is prime, $x^2 - sx + 1$ is irreducible in $\mathbb{Z}[x]$ and R over $\mathbb{Z}/M\mathbb{Z}$ is a Galois extension of degree two. The Frobenius map $R \to R$ defined by Frob : $a \mapsto a^M$ is the non-trivial element of this group (see [6, Chapter 5, §5]). On the other hand one knows that Frob maps one zero of the polynomial $x^2 - sx + 1$ to the other zero of this polynomial, therefore

$$\mathrm{Frob}(x) = x^{-1}. \tag{2.3}$$

The element x is not in the prime field of R, so $x - 1$ is nonzero in the field R and therefore a unit. Raising both sides of (2.2) to the power $\frac{M-1}{2}$ yields $\frac{(x-1)^M}{x-1} = \big(\frac{s-2}{M}\big)x^{(M-1)/2}$. The numerator $(x-1)^M$ equals $\mathrm{Frob}(x-1)$ by definition of the Frobenius map, so via (2.3) we see that $\frac{(x-1)^M}{x-1} = \frac{x^{-1}-1}{x-1} = -x^{-1}$. Therefore $-x^{-1} = \big(\frac{s-2}{M}\big)x^{(M-1)/2}$, hence

$$x^{(M+1)/2} = -\Big(\frac{s-2}{M}\Big). \tag{2.4}$$

Now we drop the assumption R is a field.

"⇐": Suppose that M is prime and $\big(\frac{s-2}{M}\big) = \big(\frac{-s-2}{M}\big) = 1$. The discriminant of $x^2 - sx + 1$ is $s^2 - 4$. From $\big(\frac{-1}{M}\big) = -1$ it follows that $\big(\frac{s^2-4}{M}\big) = \big(\frac{s+2}{M}\big) = -1$. Hence the ring R is a field. From (2.4) it follows that $x^{(M+1)/2} = -1$. Hence by (2.1) we have $s_{q-1} = x^{(M+1)/4} + x^{-(M+1)/4} = (x^{(M+1)/2} + 1)x^{-(M+1)/4} = 0$.

"⇒": Suppose $s_{q-1} = 0$. Recall that $x \in R^*$. Then we have $s_{q-1} = x^{(M+1)/4} + x^{-(M+1)/4} = (x^{(M+1)/2} + 1)x^{-(M+1)/4} = 0$. Therefore $x^{(M+1)/2}$ equals -1. Let $\mathfrak{a} \neq R$ be an ideal of R. We have the natural ring homomorphism $R \to R/\mathfrak{a}$. The integers 2 and M are relatively prime. So $1 \neq 0$ and $M = 0$ in $R/\mathfrak{a}$ imply $2 \neq 0$ in $R/\mathfrak{a}$. Hence $1 \neq -1$ in $R/\mathfrak{a}$. Note that $(M+1)/2$ is a power of 2. Therefore the identity $x^{(M+1)/2} = -1$ in $R/\mathfrak{a}$ implies that the order of x in $(R/\mathfrak{a})^*$ is $M + 1$. This yields $\#(R/\mathfrak{a}) > M = \sqrt{\#R}$, which implies $\#\mathfrak{a} < \sqrt{\#R}$. By Lemma 2.8 it follows that R is a field. Hence M is prime and $x^2 - sx + 1$ is irreducible in $(\mathbb{Z}/M\mathbb{Z})[x]$. The discriminant of the irreducible polynomial $x^2 - sx + 1$ is $s^2 - 4$, therefore $\big(\frac{s^2-4}{M}\big) = -1$. From $x^{(M+1)/2} = -1$ and (2.4) it follows that $\big(\frac{s-2}{M}\big) = 1$. Since $\big(\frac{s^2-4}{M}\big) = \big(\frac{s-2}{M}\big)\big(\frac{s+2}{M}\big) = -1$ and $\big(\frac{-1}{M}\big) = -1$, we conclude that $\big(\frac{-s-2}{M}\big) = 1$. □

Proof of Theorem 2.3. Let $n \in \mathbb{Z}_{>0}$ be such that $s \in \mathbb{Q}(\sqrt[n]{2})$. Write s as

$$\frac{1}{2^e c} \cdot \sum_{i=0}^{n-1} a_i \sqrt[n]{2}^i,$$

where $a_i \in \mathbb{Z}$, $c, e \in \mathbb{Z}_{\geq 0}$ and c odd. Take $k_s \in \mathbb{Z}_{>0}$ divisible by n and by $\operatorname{order}(2 \bmod p)$ for all prime divisors p of c, where $\operatorname{order}(2 \bmod p)$ denotes the order of $(2 \bmod p)$ in the group $(\mathbb{Z}/p\mathbb{Z})^*$. Let $q \in \mathbb{Z}_{>0}$ be such that $\gcd(q, k_s) = 1$. We prove that $s \in S_q^{-1} R_q$. From the definition of R_q it follows that $\sqrt[n]{2} \in R_q$. The inverse of $(2 \bmod 2^q - 1)$ is $(2^{q-1} \bmod 2^q - 1)$, so $2 \in S_q$. In order to prove that $s \in S_q^{-1} R_q$, it suffices to show that for all prime divisors p of c we have $p \in S_q$. Let p be any prime divisor of c. By our assumption on k_s we have $\gcd(q, \operatorname{order}(2 \bmod p)) = 1$. Since $\operatorname{order}(2 \bmod p) > 1$, this implies $2^q - 1 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Therefore $\gcd(2^q - 1, p) = 1$, and so $p \in (\mathbb{Z}/(2^q - 1)\mathbb{Z})^*$. Hence we can conclude that $p \in S_q$. □

Proof of Theorem 2.6. Since $\gcd(q, k_s) = 1$, we have $s \in S_q^{-1} R_q$, hence $s \bmod M_q$ is well defined. Suppose that $s_{q-1} = 0$. Then from Theorem 2.1 it follows that M_q is prime.

Suppose M_q is prime. Then q is prime. Since s is a universal starting value, q is prime and $q \notin B_s$, we conclude that s is a starting value for q. Applying Theorem 2.1 yields $s_{q-1} = 0$. □

Proof of Example 2.7. The discriminant of $t^2 - \sqrt{2}t - 1$ is 6. Now we apply Theorem 3.4 (the proof of Theorem 3.4 does not use Example 2.7) to conclude that $t^2 - \sqrt{2}t - 1$ has no zeros in K. By Theorem 2.3 there exists an integer $k \in \mathbb{Z}_{>0}$ such that t, $t^2 - \sqrt{2}t - 1$, $t^2 + 2\sqrt{2}t - 1$, $t^2 + 1$ and $\sqrt{2}$ are elements of $S_q^{-1} R_q$ if $\gcd(k, q) = 1$. Hence

$$s = 4 \cdot \frac{t^4 + \sqrt{2}t^3 + 3t^2 - \sqrt{2}t + 1}{(t^2 - \sqrt{2}t - 1)^2} \in S_q^{-1} R_q$$

and the two equalities below Example 2.7 can be interpreted in $S_q^{-1} R_q$ if k and q are relatively prime. Let p be an odd prime number not dividing k. Then we have $s \in S_p^{-1} R_p$. From the two equalities below Example 2.7, the identity $\left(\frac{-3}{M_p}\right) = 1$ and the fact that φ_p is a ring homomorphism it follows that s is a starting value for p. Hence s is a universal starting value. □

Constructing universal starting values

In this section we give a method to produce theorems similar to Example 2.7. In particular we show how one can find identities just like the one following Example 2.7.

In this section we call an element $a \in K$ a *pseudo-square* if $\left(\frac{a}{M_p}\right) = 1$ for almost all prime numbers p. Anarghya Vardhana found the following 9 multiplicatively independent pseudo-squares (see [17]):

$$\begin{aligned} &2, \\ -3 &= -1 \cdot 3, \\ -91 &= -1 \cdot 7 \cdot 13, \\ -6355 &= -1 \cdot 5 \cdot 31 \cdot 41, \\ -76627 &= -1 \cdot 19 \cdot 37 \cdot 109, \\ -8435 &= -1 \cdot 5 \cdot 7 \cdot 241, \\ 790097 &= 7 \cdot 11 \cdot 31 \cdot 331, \\ 133845041 &= 11 \cdot 61 \cdot 151 \cdot 1321, \\ -33678726917899 &= -1 \cdot 7 \cdot 43 \cdot 1429 \cdot 5419 \cdot 14449. \end{aligned}$$

Theorem 2.9. *Let $a, b \in K$ be pseudo-squares, let $x, y \in K$ be such that $-4 = ax^2 + by^2$. Then $\frac{ax^2 - by^2}{2}$ is a universal starting value. Moreover if we write*

$$\begin{aligned} c_0 &= a^3x^2 - a^2by^2, \\ c_1 &= 8a^2bxy, \\ c_2 &= -6a^2bx^2 + 6ab^2y^2, \\ c_3 &= -8ab^2xy, \\ c_4 &= ab^2x^2 - b^3y^2. \end{aligned}$$

then for each $t \in K$ the element $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/(2(bt^2 + a)^2)$ is a universal starting value.

Proof. Define s by $2s = ax^2 - by^2$. We will prove that s is a universal starting value. From the identity $2s = ax^2 - by^2$ and the identity $-4 = ax^2 + by^2$ it follows that $s - 2 = ax^2$ and $-s - 2 = by^2$. Theorem 2.3 and the fact that both a and b are pseudo-squares imply that $\left(\frac{s-2}{M_p}\right) = \left(\frac{-s-2}{M_p}\right) = 1$ for almost all prime numbers p. Hence $s = (ax^2 - by^2)/2$ is a universal starting value.

Next we show that $bt^2 + a \neq 0$. Suppose for a contradiction that there exists $t \in K$ such that $bt^2 + a = 0$. This yields $bt^2 = -a$, but then both a and $-a$ are pseudo-squares. This is a contradiction since $\left(\frac{-1}{M_p}\right) = -1$ for all integers $p > 1$. Hence $bt^2 + a \neq 0$.

Via the identity $-4 = ax^2 + by^2$ we can parametrize all $v, w \in K$ such that $-4 = av^2 + bw^2$ (see [15, Chapter 1, §1]). The parametrization $w(t) = t \cdot (v(t) - x) + y$ and some calculations (as described in [15, Chapter 1, §1]) yield $v(t) = \frac{-bxt^2+2byt+ax}{bt^2+a}$ and $w(t) = \frac{-byt^2-2axt+ay}{bt^2+a}$. Now the definition of c_0, c_1, c_2, c_3 and c_4 are such that $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/2(bt^2 + a)^2 = (a \cdot v(t)^2 - b \cdot w(t)^2)/2$ holds. Hence the first part of Theorem 2.9 implies that $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/2(bt^2 + a)^2$ is a universal starting value. □

Example 2.10. Take $a = b = -3$ as pseudo-squares. Take $x = \frac{2}{3}$ and $y = \frac{2}{3}\sqrt{2}$. Then

$$\begin{aligned}
c_0 &= 12,\\
c_1 &= -96\sqrt{2},\\
c_2 &= -72,\\
c_3 &= 96\sqrt{2},\\
c_4 &= 12
\end{aligned}$$

and for every $t \in K$ the value $f(t) = (c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/(2(a + bt^2)^2)$ is a universal starting value. For example

$$\begin{aligned}
&f(0) = \tfrac{2}{3},\\
&f(2) = -\tfrac{14}{75} + \tfrac{32}{25}\sqrt{2} \text{ and}\\
&f(-\tfrac{1}{2}\sqrt[4]{2}) = \tfrac{118}{49} - \tfrac{800}{147}\sqrt[4]{2} - \tfrac{96}{49}\sqrt[4]{2}^2 + \tfrac{704}{147}\sqrt[4]{2}^3
\end{aligned}$$

are all three examples of universal starting values.

Example 2.11. Take $a = b = -3 \cdot 5 \cdot 13 \cdot 241$ as pseudo-squares. Take $x = -121 + 32\sqrt{2}$ and $y = 32 + 121\sqrt{2}$. Then

$$\begin{aligned}
c_0 &= 54468 - 61952\sqrt{2},\\
c_1 &= 123904 - 435744\sqrt{2},\\
c_2 &= 326808 + 371712\sqrt{2},\\
c_3 &= -123904 + 435744\sqrt{2},\\
c_4 &= -54468 - 61952\sqrt{2}.
\end{aligned}$$

and for every $t \in K$ the value $(c_4t^4 + c_3t^3 + c_2t^2 + c_1t + c_0)/(2(a + bt^2)^2)$ is a universal starting value.

Remark. Searching for $x, y \in K$ such that $-4 = ax^2 + by^2$ can be done using Hasse-Minkowski theorem as described in the introduction of [16, § Introduction, page 2], or in the case that $a = b \in \mathbb{Z}$ by solving the equation $-4a = (x + \mathrm{i}y)(x - \mathrm{i}y)$ in the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers.

Chapter 3

Potential starting values

In this chapter we prove a necessary condition for elements in $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ to occur as a starting value. Elements of the field K satisfying this condition will be called potential starting values. In the next chapter we will calculate certain Galois groups of Galois extensions of K for these starting values.

We also prove in this chapter, with the help of Capelli's theorem, that each number field contained in K is of the form $\mathbb{Q}(\sqrt[n]{2})$ with $n \in \mathbb{Z}_{>0}$.

A property of starting values

We start with the definition of a potential starting value.

Definition 3.1. *A potential starting value is an element $s \in K$ for which none of the elements $s+2$, $-s+2$ and s^2-4 is in K^{*2}. We denote by $\mathcal{S}$ the set of potential starting values.*

Theorem 3.2. *Let $s \in K$. If s is a starting value for some odd $q \in \mathbb{Z}_{>1}$, then s is a potential starting value.*

We prove this theorem in the last section of this chapter. The assumption that q be odd in Theorem 3.2 cannot be omitted. Indeed, $s = 0 \in K$ is a starting value for $q = 2$, but s is not a potential starting value, since $s + 2 \in K^{*2}$. The converse of Theorem 3.2 is not true. For example one can verify that $s = 5 \in \mathbb{Z}$ is a potential starting value, but there does not exist $q \in \mathbb{Z}_{>1}$ for which s is a starting value.

Denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in the field of complex numbers. Let $\mathrm{i} \in \overline{\mathbb{Q}}$ be a primitive 4-th root of unity. We can define the set $\mathcal{S}$ from Definition 3.1 in an alternative way.

Proposition 3.3. *The set $\mathcal{S}$ of potential starting values is equal to the set*

$$\{s \in K : \mathrm{i} \notin K(\sqrt{s-2}, \sqrt{-s-2})\}.$$

We prove this proposition in the last section of this chapter.

The following results, which we prove in the next section, will be useful throughout this thesis; in particular the next theorem will be used in the proof of Theorem 3.2 and it has already been used in the proof of Example 2.7.

Theorem 3.4. *Every subfield of K of finite degree over $\mathbb{Q}$ equals $\mathbb{Q}(\sqrt[n]{2})$ for some integer $n \in \mathbb{Z}_{>0}$.*

Corollary 3.5. *For every $n \in \mathbb{Z}_{>0}$ the maximal Galois extension of $\mathbb{Q}(\sqrt[n]{2})$ in K is $\mathbb{Q}(\sqrt[2n]{2})$.*

Corollary 3.6. *Let $n \in \mathbb{Z}_{>0}$ and let $E/\mathbb{Q}(\sqrt[n]{2})$ be an abelian extension of number fields. Then we have $[E \cap K : \mathbb{Q}(\sqrt[n]{2})] \leq 2$.*

Proposition 3.7. *Let $n \in \mathbb{Z}_{>0}$, let $E/\mathbb{Q}(\sqrt[n]{2})$ be a finite Galois extension and let F/E be an abelian extension such that the Galois group of F/E is a 2-group. Suppose that $\mathrm{i} \notin EK$. Then we have $[F \cap K : E \cap K] \leq 2$. Moreover if in addition to the above assumptions F/E is cyclic and $\mathrm{i} \in F$, then $F \cap K$ equals $E \cap K$.*

Recall the definition of pseudo-squares (see the last section of Chapter 2).

Proposition 3.8. *Let $n \in \mathbb{Z}_{>0}$, let $\alpha_1, \ldots, \alpha_n \in K$ be pseudo-squares and let $E = K(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n})$. Then we have $\mathrm{i} \notin E$.*

Subfields of a radical extension

In this section we look at subfields of the radical extension $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ of $\mathbb{Q}$. We will use the next theorem of Capelli in our proofs.

Theorem 3.9. *Let L be a field, let $a \in L^*$ and $n \in \mathbb{Z}_{>0}$. Then the following two statements are equivalent:*

(i) *For all prime numbers p such that $p \mid n$ we have $a \notin L^{*p}$, and if $4 \mid n$ then $a \notin -4L^{*4}$.*

(ii) *The polynomial $x^n - a$ is irreducible in $L[x]$.*

For a proof of Capelli's theorem see ([6, Chapter 6, §9]).

Lemma 3.10. *For every $n \in \mathbb{Z}_{>0}$ we have $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.*

Proof. The Eisenstein criterion implies that $x^n - 2$ is irreducible over $\mathbb{Q}$, hence $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. □

Lemma 3.11. *Let $n, m \in \mathbb{Z}_{>0}$. We have $\mathbb{Q}(\sqrt[m]{2}) \subset \mathbb{Q}(\sqrt[n]{2})$ if and only if $m \mid n$.*

Proof. "$\Leftarrow$": Suppose $m \mid n$. Then we have $n/m \in \mathbb{Z}$, so $\sqrt[n]{2}^{n/m} = \sqrt[m]{2}$. (Recall that $\sqrt[n]{2}, \sqrt[m]{2} \in \mathbb{R}_{>0}$ by definition, see Chapter 2.) Hence we have $\mathbb{Q}(\sqrt[m]{2}) \subset \mathbb{Q}(\sqrt[n]{2})$.

"$\Rightarrow$": Suppose $\mathbb{Q}(\sqrt[m]{2}) \subset \mathbb{Q}(\sqrt[n]{2})$. From Lemma 3.10 we get

$$n = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}(\sqrt[m]{2})] \cdot [\mathbb{Q}(\sqrt[m]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}(\sqrt[m]{2})] \cdot m.$$

Hence m divides n. □

Proof of Theorem 3.4. Let L be a finite extension of $\mathbb{Q}$ contained in K. Take $m \in \mathbb{Z}_{>0}$ maximal and $n \in \mathbb{Z}_{>0}$ such that $\mathbb{Q}(\sqrt[m]{2}) \subset L \subset \mathbb{Q}(\sqrt[n]{2})$. Using Lemma 3.11 we see that $r = n/m \in \mathbb{Z}_{>0}$. We will show using Theorem 3.9 that $x^r - \sqrt[m]{2}$ is irreducible in $L[x]$. By maximality of m it follows that for all prime numbers p we have $\sqrt[m]{2} \notin L^{*p}$. Since $\sqrt[m]{2} > 0$, it follows that $\sqrt[m]{2} \notin -4L^{*4}$. Therefore $x^r - \sqrt[m]{2}$ is irreducible in $L[x]$, so $[\mathbb{Q}(\sqrt[n]{2}) : L] = r$. From this we see that $[L : \mathbb{Q}(\sqrt[m]{2})] = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}(\sqrt[m]{2})]/[\mathbb{Q}(\sqrt[n]{2}) : L] = r/r = 1$, so $L = \mathbb{Q}(\sqrt[m]{2})$. □

Proof of Corollary 3.5. Since $[\mathbb{Q}(\sqrt[2n]{2}) : \mathbb{Q}(\sqrt[n]{2})]$ is 2, the extension $\mathbb{Q}(\sqrt[2n]{2})$ over $\mathbb{Q}(\sqrt[n]{2})$ is Galois.

Let $L \subset K$ be a finite Galois extension of $\mathbb{Q}(\sqrt[n]{2})$. Theorem 3.4 implies $L = \mathbb{Q}(\sqrt[l]{2})$ for some $l \in \mathbb{Z}_{>0}$. By Lemma 3.10 and Lemma 3.11 we have $[\mathbb{Q}(\sqrt[l]{2}) : \mathbb{Q}(\sqrt[n]{2})] = l/n$. Hence the l/n-th roots of unity are contained in $\mathbb{Q}(\sqrt[n]{2})$. Since $L \subset K \subset \mathbb{R}$, we have $l/n = 1$ or $l/n = 2$. Hence $L = \mathbb{Q}(\sqrt[n]{2})$ or $L = \mathbb{Q}(\sqrt[2n]{2})$. □

Proof of Corollary 3.6. By assumption the extension $E/\mathbb{Q}(\sqrt[n]{2})$ is abelian. Hence $(E \cap K)/\mathbb{Q}(\sqrt[n]{2})$ is abelian. Corollary 3.5 implies $[E \cap K : \mathbb{Q}(\sqrt[n]{2})] \leq 2$. □

The following theorem will be used in the proof of Proposition 3.7.

Theorem 3.12. *Let M be a Galois extension of field L, let F be an arbitrary field extension of L and assume that M, F are subfields of some other field. Then MF is Galois over F, and M is Galois over $M \cap F$. Let H be the Galois group of MF over F, and G the Galois group of M over L. If $\sigma \in H$ then the restriction of σ to M is in G, and the map $\sigma \mapsto \sigma|K$ gives an isomorphism of H with the Galois group of M over $M \cap F$.*

For a proof of Theorem 3.12 see [6, Chapter VI, §1, Theorem 1.12].

Proof of Proposition 3.7. Consider the following diagram.

$$\begin{tikzcd}
F \arrow[dr, dash] & & EK \arrow[dl, dash] \\
& E(F \cap K) \arrow[dl, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & F \cap K \arrow[dl, dash] \\
& E \cap K &
\end{tikzcd}$$

The intersection of E and $F \cap K$ is $E \cap K$. Hence Theorem 3.12 implies $[E : E \cap K] = [E(F \cap K) : F \cap K)]$. Therefore we have $[E(F \cap K) : E] = [F \cap K) : E \cap K)]$.

Let $t = [F \cap K : E \cap K]$. Let $m = [E \cap K : \mathbb{Q}]$, so that $E \cap K = \mathbb{Q}(\sqrt[m]{2})$. Then $E(F \cap K) = E(\sqrt[tm]{2})$ and $x^t - \sqrt[m]{2}$ is irreducible in $E[x]$. Since F/E is abelian, the extension $E(\sqrt[tm]{2})/E$ is Galois. Hence $E(\sqrt[tm]{2})$ contains a primitive t-th root of unity. The Galois group of F/E is a 2-group, so the only prime number that can divide t is 2. However $\mathrm{i} \notin EK$, so $t = 1$ or 2. This proves the first part of the proposition.

To prove the second part of the proposition we assume (for a contradiction) that $t = 2$. Since F/E is a cyclic 2-group and $\mathrm{i} \in F$, we have $E(\sqrt[2m]{2}) = E(\mathrm{i})$. This contradicts $\mathrm{i} \notin EK$. □

Proof of Proposition 3.8. Suppose for a contradiction that -1 is a square in E^*. Define the subgroup H of K^* by $H = H_n = \langle \alpha_1, \dots, \alpha_n \rangle$. If we apply Kummer theory (see [6, Chapter VI, §8]) to the extension E/K, then we get $-1 \in HK^{*2}$. Now we write -1 as $-1 = hk^2$ with $h \in H$ and $k \in K^*$. By Theorem 2.3 there exists a positive integer m such that for all prime numbers $p > m$ the inclusion $H \cup \{k\} \subset (S_p^{-1}R_p)^*$ holds. Let $p \in \mathbb{Z}_{>m}$ be a prime number. Since all elements of H are pseudo-squares, we get the contradiction $-1 = \left(\frac{-1}{M_p}\right) = \left(\frac{hk^2}{M_p}\right) = \left(\frac{h}{M_p}\right)\left(\frac{k^2}{M_p}\right) = 1$. We conclude that -1 is not a square in E^*. □

The following proposition will be used in Chapter 8.

Proposition 3.13. *Let E_1 and E_2 be field extensions of a number field F contained in some common field. If E_1 and E_2 are Galois over F, then E_1E_2 and $E_1 \cap E_2$ are Galois over F, and the restriction map* $\mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$ *defined by $\sigma \mapsto (\sigma|E_1, \sigma|E_2)$ is an injective homomorphism with image*

$$\{(\sigma_1, \sigma_2) \in \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) : \sigma_1|(E_1 \cap E_2) = \sigma_2|(E_1 \cap E_2)\}.$$

For a proof of Proposition 3.13 see [12, Chapter 3, The fundamental theorem of Galois theory, Proposition 3.20].

Starting values are potential starting values

In this section we prove Proposition 3.3 and Theorem 3.2.

Proof of Proposition 3.3. It suffices to prove that $s \notin \mathcal{S}$ if and only if $x^2 + 1$ is reducible in $K(\sqrt{s-2}, \sqrt{-s-2})[x]$. Suppose $s \notin \mathcal{S}$. Then we can choose $a \in \{s+2, -s+2, s^2-4\}$ such that $a \in K^{*2}$. Hence $\sqrt{a}$ and $\sqrt{-a}$ are elements of $K(\sqrt{s-2}, \sqrt{-s-2})$, so $\mathrm{i} \in K(\sqrt{s-2}, \sqrt{-s-2})$. It follows that $x^2 + 1$ is reducible in $K(\sqrt{s-2}, \sqrt{-s-2})[x]$.

Suppose $x^2 + 1$ is reducible in $K(\sqrt{s-2}, \sqrt{-s-2})[x]$. Then i is an element of $K(\sqrt{s-2}, \sqrt{-s-2})$. Since $\mathrm{i} \notin \mathbb{R}$ and $K \subset \mathbb{R}$, the element i is not in K. From Galois theory it follows that $K(\mathrm{i}) = K(\sqrt{b})$ for some $b \in \{s-2, -s-2, 4-s^2\}$. Let σ be the non-trivial element of $\mathrm{Gal}(K(\mathrm{i})/K)$. Then σ keeps $\mathrm{i}\sqrt{b}$ fixed. Hence $\mathrm{i}\sqrt{b} \in K^*$ and therefore $-b \in K^{*2}$. Hence $s \notin \mathcal{S}$. □

Lemma 3.14. *Let q, $n \in \mathbb{Z}_{>0}$ and $q > 1$. Suppose that* $\gcd(q, n) = 1$ *and suppose $\varphi : \mathbb{Z}[\sqrt[n]{2}] \to \mathbb{Z}/M_q\mathbb{Z}$ is a ring homomorphism. Let $p \in \mathbb{Z}_{>0}$ be a prime divisor of M_q. Then there exist an odd positive integer u and a ring homomorphism φ' from the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}$ of $\mathbb{Q}(\sqrt[n]{2})$ to the finite field $\mathbb{F}_{p^u}$ of p^u elements, such that the diagram*

$$\begin{tikzcd}
\mathbb{Z}[\sqrt[n]{2}] \arrow[r, "\varphi"] \arrow[d] & \mathbb{Z}/M_q\mathbb{Z} \arrow[r, two heads, "r"] & \mathbb{F}_p \arrow[d] \\
\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})} \arrow[rr, "\varphi'"'] & & \mathbb{F}_{p^u}
\end{tikzcd}$$

of ring homomorphisms commutes, where the two unlabeled arrows and r are the natural ones.

Proof. Write $n = m \cdot p^t$ with $p \nmid m \in \mathbb{Z}_{>0}$ and $t \in \mathbb{Z}_{\geq 0}$. Let $\mathfrak{p}$ be the ideal $\{x \in \mathbb{Z}[\sqrt[m]{2}] : (r \circ \varphi)(x) = 0\}$. Since $\mathbb{F}_p$ is a field of characteristic p, the ideal $\mathfrak{p}$ is prime and $p \in \mathfrak{p}$. Let $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$ be the ring of integers of the field $\mathbb{Q}(\sqrt[m]{2})$. Since $p \nmid m$, the index $(\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})} : \mathbb{Z}[\sqrt[m]{2}])$ is not divisible by p. Hence there is a ring homomorphism, extending the restriction of φ to $\mathbb{Z}[\sqrt[m]{2}]$, from $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$ to $\mathbb{F}_p$ with kernel $\mathfrak{q}$, such that $\mathfrak{q}$ lies above $\mathfrak{p}$. Let e denote the ramification index and f the inertia degree of primes of $\mathbb{Q}(\sqrt[n]{2})$ above $\mathfrak{q}$. Then we have

$$\sum_{\mathfrak{r}|\mathfrak{q}} e(\mathfrak{r}/\mathfrak{q}) f(\mathfrak{r}/\mathfrak{q}) = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}(\sqrt[m]{2})] = p^t,$$

where the sum is taken over all primes $\mathfrak{r}$ of $\mathbb{Q}(\sqrt[n]{2})$ that divide $\mathfrak{q}$. Hence we can choose a prime $\mathfrak{r}$ of $\mathbb{Q}(\sqrt[n]{2})$ above $\mathfrak{q}$ such that $f(\mathfrak{r}/\mathfrak{q})$ is odd. Therefore we can define a ring homomorphism φ', with kernel $\mathfrak{r}$, from $\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}$ to $\mathbb{F}_{p^u}$ where $u = f(\mathfrak{r}/\mathfrak{q})$. The prime ideal $\mathfrak{r}$ lies above $\mathfrak{p}$, so the map φ' is an extension of the restriction of φ to $\mathbb{Z}[\sqrt[m]{2}]$. Hence we have $r \circ \varphi(\sqrt[m]{2}) = \varphi'(\sqrt[m]{2})$. The map $\sigma : x \mapsto x^{p^t}$ is a automorphism of $\mathbb{F}_{p^u}$ and $\sqrt[m]{2} = \sqrt[n]{2}^{p^t}$, so an image of $\sqrt[n]{2} \in \mathbb{Z}[\sqrt[n]{2}]$ in $\mathbb{F}_{p^u}$ induced by the diagram above equals σ^{-1} applied on the image of $\sqrt[m]{2} \in \mathbb{Z}[\sqrt[n]{2}]$ in $\mathbb{F}_{p^u}$ induced by the diagram above. Therefore the diagram above commutes. □

Lemma 3.15. *Let q, $n \in \mathbb{Z}_{>0}$ and $q > 1$. Suppose that* $\gcd(q, n) = 1$. *Let $\varphi : \mathbb{Z}[\sqrt[n]{2}] \to \mathbb{Z}/M_q\mathbb{Z}$ be a ring homomorphism and let $a \in \mathbb{Z}[\sqrt[n]{2}] \cap {\mathbb{Q}(\sqrt[n]{2})^*}^2$. Then*

$$\left(\frac{\varphi(a)}{M_q}\right) \textit{ equals } 0 \textit{ or } 1.$$

Proof. Since $a \in \mathbb{Z}[\sqrt[n]{2}] \cap {\mathbb{Q}(\sqrt[n]{2})^*}^2$, there exists an element $b \in \mathbb{Q}(\sqrt[n]{2})^*$ such that $b^2 = a$. Moreover a is an algebraic integer, so $b \in \mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}$. Let p be a prime divisor of M_q. The hypotheses of Lemma 3.14 hold and we let $u \in \mathbb{Z}_{>0}$ and

φ' be as in Lemma 3.14. We have $\varphi'(a) = \varphi'(b)^2$, so $\varphi'(a)$ is a square in $\mathbb{F}_{p^u}$. However from $2 \nmid [\mathbb{F}_{p^u} : \mathbb{F}_p]$ it follows that $[\mathbb{F}_p(\sqrt{\varphi'(a)}) : \mathbb{F}_p] = 1$, so $\varphi'(a)$ is a square in $\mathbb{F}_p$. By Lemma 3.14 we have

$$\left(\frac{\varphi(a)}{M_q}\right) = \prod_{p|M_q} \left(\frac{\varphi'(a)}{p}\right)^{\mathrm{ord}_p(M_q)} = 0 \text{ or } 1. \qquad \square$$

Corollary 3.16. *Let $q \in \mathbb{Z}_{>1}$ be odd, let $\varphi_q : S_q^{-1}R_q \to \mathbb{Z}/M_q\mathbb{Z}$ be defined as just before Theorem 2.3, and let $a \in S_q^{-1}R_q \cap K^{*2}$. Then*

$$\left(\frac{\varphi_q(a)}{M_q}\right) \textit{ equals } 0 \textit{ or } 1.$$

Proof. Let $a \in S_q^{-1}R_q \cap K^{*2}$. Take $b \in R_q$ and $c \in S_q$ such that $a = b/c$. Choose $m \in \mathbb{Z}_{>0}$ such that $\gcd(q, m) = 1$ and $b, c \in \mathbb{Z}[\sqrt[m]{2}]$. Since $bc = a \cdot c^2 \in K^{*2} \cap \mathbb{Q}(\sqrt[m]{2})$, we have

$$bc \in \mathbb{Q}(\sqrt[m]{2}, \sqrt{bc})^{*^2} \subset \mathbb{Q}(\sqrt[2m]{2})^{*^2},$$

where the last inclusion follows from Theorem 3.4. Let $n = 2m$. Since q is odd, we have $\mathbb{Z}[\sqrt[n]{2}] \subset R_q$. Hence we can restrict the map φ_q to a map $\varphi : \mathbb{Z}[\sqrt[n]{2}] \to \mathbb{Z}/M_q\mathbb{Z}$. Since $bc \in \mathbb{Z}[\sqrt[n]{2}] \cap \mathbb{Q}(\sqrt[n]{2})^{*^2}$, we have by Lemma 3.15

$$\left(\frac{\varphi_q(a)}{M_q}\right) = \left(\frac{\varphi_q(b/c)}{M_q}\right) = \left(\frac{\varphi_q(bc)}{M_q}\right) = 0 \text{ or } 1. \qquad \square$$

Proof of Theorem 3.2. Let s be a starting value for $q \in \mathbb{Z}_{>1}$ odd. Then

$$\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = \left(\frac{4-s^2}{M_q}\right) = 1.$$

Since $\left(\frac{-1}{M_q}\right) = -1$, we see that

$$\left(\frac{-s+2}{M_q}\right) = \left(\frac{s+2}{M_q}\right) = \left(\frac{s^2-4}{M_q}\right) = -1.$$

By Corollary 3.16 we see that none of the elements $-s+2$, $s+2$ and s^2-4 is in $S_q^{-1}R_q \cap K^{*2}$. Since $-s+2$, $s+2$ and s^2-4 are elements of $S_q^{-1}R_q$, we conclude that none of the elements $-s+2$, $s+2$ and s^2-4 is in K^{*2}. Hence s is a potential starting value. $\square$

Chapter 4

Auxiliary fields

In this chapter we construct, for every potential starting value in K, a Galois extension that is useful to calculate its Lehmer symbol. The orders of their Galois groups will divide 32.

Auxiliary Galois groups

We recall that $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ inside the field of complex numbers. Let

$$K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$$

be as in Chapter 2. For $s \in K$ let $f_s = x^{16} - sx^8 + 1 \in K[x]$. In this chapter we will study the Galois group G_s of f_s over K for potential starting values s in K .

We define, for $s \in K$, a Galois extension of number fields with a Galois group that is naturally isomorphic to G_s. Our results on G_s will be stated in terms of this Galois group of number fields. Let L_s be the splitting field of f_s over $\mathbb{Q}(s)$. Define K_s by $K_s = K \cap L_s$. The elements of G_s can be restricted to the field L_s. This restriction induces a natural isomorphism from G_s to $\mathrm{Gal}(L_s/K_s)$ (see Theorem 3.12). In the remainder of this chapter we will study $\mathrm{Gal}(L_s/K_s)$, which we will also denoted by G_s.

To describe G_s we use some field extensions of K_s that are contained in L_s. Let

$$K_s' = K_s(\sqrt{4-s^2})$$

and let

$$K_s'' = K_s(\sqrt{s-2}, \sqrt{-s-2}).$$

Let $\alpha \in \overline{\mathbb{Q}}$ be a zero of f_s and let $\zeta_8 \in \overline{\mathbb{Q}}$ be a primitive 8th root of unity that satisfies $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ (recall that $\sqrt{2} \in \mathbb{R}_{>0}$). The zeros of f_s are $\zeta_8^i \alpha^{\pm 1}$ where $i \in \mathbb{Z}/8\mathbb{Z}$. Let

$$L_s' = K_s'(\alpha + \alpha^{-1}).$$

Proposition 4.1 implies that L'_s does not depend on the choice of α.

The following three propositions, which we prove in the last section, state the information about the Galois group of f_s over K_s that we will use.

Proposition 4.1. *Let $s \in K$. Let α and β be zeros of f_s. Then L_s is $K''_s(\alpha + \alpha^{-1})$, the extension L'_s/K_s is Galois, $K'_s(\alpha + \alpha^{-1})$ equals $K'_s(\beta + \beta^{-1})$ and $[K''_s : K_s]$ equals* 2 *or* 4.

From this proposition we get the field diagram

$$\begin{tikzcd}
 & L_s \arrow[dl, dash] \arrow[dr, dash] & \\
L'_s \arrow[dr, dash] & & K''_s \arrow[dl, dash] \\
 & K'_s \arrow[dl, dash] & \\
K_s & &
\end{tikzcd}$$

in which every field is Galois over K_s.

For our purposes it suffices to study $\mathrm{Gal}(L_s/K'_s)$ and $\mathrm{Gal}(L'_s/K_s)$ rather than the entire Galois group of L_s over K_s. Furthermore we will concentrate on potential starting values $s \in K$, i.e. $s \in \mathcal{S}$ (see Proposition 3.3).

Proposition 4.2. *Let $s \in \mathcal{S}$. Then the restriction map from $\mathrm{Gal}(L_s/K'_s)$ to $\mathrm{Gal}(L'_s/K'_s) \times \mathrm{Gal}(K''_s/K'_s)$ is an isomorphism and the group $\mathrm{Gal}(L_s/K''_s)$ is cyclic of order* 8. *Furthermore $\mathrm{Gal}(L_s/K''_s)$ is generated by a unique element ω that satisfies $\omega(\alpha) = \zeta_8^{-1}\alpha^{-1}$ and $\omega(\zeta_8) = \zeta_8^{-1}$.*

From Proposition 4.2 we conclude that $\mathrm{Gal}(L'_s/K_s)$ is cyclic of order 8 if $K_s = K'_s$ and $s \in \mathcal{S}$. The following proposition describes the Galois group of L'_s over K_s also if $K_s \neq K'_s$.

Proposition 4.3. *Let $s \in \mathcal{S}$. Then the exact sequence*

$$1 \to \mathrm{Gal}(L'_s/K'_s) \to \mathrm{Gal}(L'_s/K_s) \to \mathrm{Gal}(K'_s/K_s) \to 1$$

splits, where $\mathrm{Gal}(L'_s/K'_s)$ is cyclic of order 8 *and $\mathrm{Gal}(K'_s/K_s)$ has order* 1 *or* 2. *If $\mathrm{Gal}(K'_s/K_s)$ has order* 2*, then the action of the non-trivial element of $\mathrm{Gal}(K'_s/K_s)$ on $\mathrm{Gal}(L'_s/K'_s)$ sends a group element to its inverse.*

Define $\mathbb{Q}''_s = \mathbb{Q}(s, \sqrt{2}, \sqrt{s-2}, \sqrt{-s-2})$. The next proposition, which we prove in the last section, is useful for calculating the field K_s.

Proposition 4.4. *Let $s \in \mathcal{S}$. Then we have $K''_s = \mathbb{Q}''_s$, $K_s = \mathbb{Q}''_s \cap K$ and $[K_s : \mathbb{Q}(s)] \leq 2$.*

Remark. Define $\mathbb{Q}'_s = \mathbb{Q}(s, \sqrt{2}, \sqrt{4-s^2})$. Then $[K'_s : \mathbb{Q}'_s]$ is 2 for $s = \sqrt{2} + 2 \in \mathcal{S}$. Hence in general we do not have $K'_s = \mathbb{Q}'_s$.

Galois groups and signs

The proposition and definitions of this section will be used in the next chapter to relate certain elements of the Galois group of L_s/K_s to the Lehmer symbol.

Let $s \in \mathcal{S}$. By Proposition 3.3 we have $\mathrm{i} \notin K_s''$. Since $\mathrm{i} \in L_s$, Proposition 4.2 implies that each element of $\mathrm{Gal}(L_s/K_s'')\backslash\mathrm{Gal}(L_s/K_s''(\mathrm{i}))$ generates $\mathrm{Gal}(L_s/K_s'')$. We denote $\mathrm{Gal}(L_s/K_s'')\backslash\mathrm{Gal}(L_s/K_s''(\mathrm{i}))$ by $\mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}$.

Now we define the equivalence relation $\sim$ for $\sigma, \tau \in G_s$ by $\sigma \sim \tau$ if σ is conjugate to τ. We denote the equivalence class of $\sigma \in G_s$ by $[\sigma]$. Since $\mathrm{Gal}(L_s/K_s'')$ is a normal subgroup of G_s and conjugate elements have the same order, the set $\mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}$ is a union of conjugacy classes.

Proposition 4.5. *Let $s \in \mathcal{S}$. Then the map*

$$\lambda_s : \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/\!\sim\, \to \{+1, -1\}$$

defined by

$$\lambda_s : [\rho] \mapsto \frac{\rho(\alpha)\alpha + \rho(\alpha^{-1})\alpha^{-1}}{\sqrt{2}},$$

does not depend on the choice of $\alpha \in \overline{\mathbb{Q}}$. Moreover, if ω is as in Proposition 4.2, then $\lambda_s^{-1}(+1)$ equals $\{[\omega], [\omega^7]\}$ and $\lambda_s^{-1}(-1)$ equals $\{[\omega^3], [\omega^5]\}$.

A proof of this proposition can be found in the last section of this chapter.

By Proposition 4.3 the Galois group $\mathrm{Gal}(L_s'/K_s')$ is cyclic of order 8. We denote the set of elements of order 8 of $\mathrm{Gal}(L_s'/K_s')$ by $\mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}$. Similarly as above we can define an equivalence relation $\sim$ on $\mathrm{Gal}(L_s'/K_s)$: for $\sigma, \tau \in \mathrm{Gal}(L_s'/K_s)$ we have $\sigma \sim \tau$ if σ is conjugate to τ. Proposition 4.1 and Proposition 4.2 imply that the restriction map $\mathrm{Gal}(L_s/K_s'') \to \mathrm{Gal}(L_s'/K_s')$ is an isomorphism. This map induces a bijective map $r : \mathrm{Gal}(L_s''/K_s)^{\mathrm{gen}}/\!\sim\, \to \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/\!\sim$. Now we can give the following definition.

Definition 4.6. *Let $s \in \mathcal{S}$. We define the map*

$$\lambda_s' : \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/\!\sim\, \to \{+1, -1\}$$

by $\lambda_s' = \lambda_s \circ r^{-1}$.

Next we describe the set $\mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}$. By definition of K_s'' the field $K_s''(\mathrm{i})$ equals $K_s''(\sqrt{s+2})$ and by Proposition 3.3 we have $\sqrt{s+2} \notin K_s''$, so $K_s'(\sqrt{s+2})$ is a quadratic extension of K_s'. By definition of α we get $(\alpha^8)^2 - s\alpha^8 + 1 = 0$, so the identity $s = \alpha^8 + \alpha^{-8}$ holds. From this identity we see that $s + 2 = (((\alpha + \alpha^{-1})^2 - 2)^2 - 2)^2$. By definition L_s' equals $K_s'(\alpha + \alpha^{-1})$, so $K_s'(\sqrt{s+2})$ is a subfield of L_s'. Hence the only quadratic extension of L_s'/K_s' is $K_s'(\sqrt{s+2})$. This leads to the following description of $\mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}$.

Proposition 4.7. *Let $s \in \mathcal{S}$. Then the set* $\mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}$ *is equal to set* $\mathrm{Gal}(L_s'/K_s')\backslash\mathrm{Gal}(L_s/K_s''(\sqrt{s+2}))$.

Examples

In this section we calculate the Galois extensions L_s of K_s and their groups for $s = 2/3$, $s = 4$, $s = \sqrt{2}$, $s = 0$, $s = -2$ and $s = 2$. We recall that $\mathcal{S}$ is the set of potential starting values in K and $G_s = \mathrm{Gal}(L_s/K_s)$. For $n \in \mathbb{Z}_{>0}$ we write C_n for a cyclic group of order n.

Example $s = 2/3$**.** In this case s is a universal starting value, so by Theorem 3.2 we have $s \in \mathcal{S}$. Note that $\sqrt{4 - s^2} = 4\sqrt{2}/3$, so by Proposition 4.4 we have $K_s = \mathbb{Q}(\sqrt{2})$ and by definition of K'_s we have $K_s = K'_s$. Hence Proposition 4.1 and Proposition 4.2 imply that G_s is isomorphic to $C_8 \times C_2$.

Example $s = 4$**.** In this case s is a universal starting value, so by Theorem 3.2 we have $s \in \mathcal{S}$. Note that $\sqrt{s - 2} = \sqrt{2}$, so by Proposition 4.4 we have $K_s = \mathbb{Q}(\sqrt{2})$ and by definition of K''_s we have $K'_s = K''_s$. Hence Proposition 4.1 and Proposition 4.3 imply that G_s is a dihedral group of 16 elements.

Example $s = \sqrt{2}$**.** Set $s_1 = s$ and $s_{i+1} = s_i^2 - 2$ for $i \in \mathbb{Z}_{>0}$. Then $s_2 = 0$, $s_3 = -2$ and $s_i = 2$ for $i > 3$, so for $q \in \mathbb{Z}_{>0}$ we have $s_{q-1} \equiv 0 \bmod M_q$ if and only if $q = 3$. By Theorem 2.1 the value s is a starting value for $q = 3$, so by Theorem 3.2 we have $s \in \mathcal{S}$. Let ζ_{64} be a primitive 64-th root of unity such that $\zeta_{64}^8 = \zeta_8$. The identity $\zeta_{64}^{16} - (\zeta_8 + \zeta_8^{-1})\zeta_{64}^8 + 1 = 0$ shows that ζ_{64} is a zero of f_s. Hence L_s is the cyclotomic field $\mathbb{Q}(\zeta_{64})$. The identity $\sqrt{4 - s^2} = \sqrt{2}$ yields $K_s = K'_s$. By Corollary 3.5 we have $\mathbb{Q}(s) = K_s = \mathbb{Q}(\sqrt{2})$. We have $32 = [\mathbb{Q}(\zeta_{64}) : \mathbb{Q}] = [L_s : K'_s] \cdot [K'_s : \mathbb{Q}] = [L_s : K'_s] \cdot 2$, so $[L_s : K'_s] = 16$. Hence Proposition 4.2 implies that G_s is isomorphic to $C_8 \times C_2$.

Example $s = 0$**.** Note that $s \notin \mathcal{S}$. Let ζ_{32} be a primitive 32-nd root of unity. The field L_s is $\mathbb{Q}(\zeta_{32})$. The extension $L_s/\mathbb{Q}$ is abelian, therefore Corollary 3.6 implies $K_s \subset \mathbb{Q}(\sqrt{2})$. On the other hand $\sqrt{2} \in K_s$, so $K_s = \mathbb{Q}(\sqrt{2})$. Note that $\sqrt{4 - s^2} = 2$, hence $K_s = K'_s = \mathbb{Q}(\sqrt{2})$. Since $K_s = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_{32}^4 + \zeta_{32}^{-4})$, it follows that the Galois group of L_s over K_s is isomorphic to the group $\{a \in (\mathbb{Z}/32\mathbb{Z})^* : \zeta_{32}^4 + \zeta_{32}^{-4} = \zeta_{32}^{4a} + \zeta_{32}^{-4a}\} = \langle 7, -1 \rangle$, i.e. G_s is isomorphic to $C_4 \times C_2$.

Example $s = -2$**.** Note that $s \notin \mathcal{S}$. Let ζ_{16} be a primitive 16-th root of unity. The field L_s is $\mathbb{Q}(\zeta_{16})$. The extension $L_s/\mathbb{Q}$ is abelian, therefore Corollary 3.6 implies $K_s \subset \mathbb{Q}(\sqrt{2})$. On the other hand $\sqrt{2} \in K_s$, so $K_s = \mathbb{Q}(\sqrt{2})$. Note that $\sqrt{4 - s^2} = 0$, hence $K_s = K'_s = \mathbb{Q}(\sqrt{2})$. Since $K_s = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_{16}^2 + \zeta_{16}^{-2})$, it follows that the Galois group of L_s over K_s is isomorphic to the group $\{a \in (\mathbb{Z}/16\mathbb{Z})^* : \zeta_{16}^2 + \zeta_{16}^{-2} = \zeta_{16}^{2a} + \zeta_{16}^{-2a}\} = \langle 7, -1 \rangle$, i.e. G_s is isomorphic to $C_2 \times C_2$.

Example $s = 2$**.** Note that $s \notin \mathcal{S}$. Let ζ_8 be a primitive 8-th root of unity. The field L_s is $\mathbb{Q}(\zeta_8)$. The extension $L_s/\mathbb{Q}$ is abelian, therefore Corollary 3.6 implies $K_s \subset \mathbb{Q}(\sqrt{2})$. On the other hand $\sqrt{2} \in K_s$, so $K_s = \mathbb{Q}(\sqrt{2})$. Note that

$\sqrt{4-s^2}=0$, hence $K_s=K'_s=\mathbb{Q}(\sqrt{2})$. Hence G_s is isomorphic to C_2.

Calculating a Galois group

In this last section we prove the propositions of the first section and Proposition 4.5 of this chapter.

For convenience we give an overview of the fields defined in this chapter.

$$\begin{tikzcd}
 & & L_s \arrow[dl, dash] \arrow[dr, dash] & & \\
 & L'_s \arrow[dl, dash] \arrow[dr, dash] & & K''_s \arrow[dl, dash] \arrow[dr, dash] & \\
L''_s \arrow[dr, dash] & & K'_s \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Q}''_s \arrow[dl, dash] \\
 & K_s \arrow[dr, dash] & & \mathbb{Q}'_s \arrow[dl, dash] & \\
 & & \mathbb{Q}_s & &
\end{tikzcd}$$

Let $s\in K$, let $f_s=x^{16}-sx^8+1$ and let L_s be the splitting field of f_s over $\mathbb{Q}(s)$. Define $\mathbb{Q}_s=\mathbb{Q}(s,\sqrt{2})$. In this section we study the Galois group $\mathrm{Gal}(L_s/\mathbb{Q}_s)$. Recall $K_s=L_s\cap K$. Note that this Galois group contains $G_s=\mathrm{Gal}(L_s/K_s)$. Define $\mathbb{Q}'_s=\mathbb{Q}_s(\sqrt{4-s^2})$ and recall $\mathbb{Q}''_s=\mathbb{Q}_s(\sqrt{s-2},\sqrt{-s-2})$. Recall that α is a zero of f_s. Define $L''_s=K_s(\alpha+\alpha^{-1})$. The field L''_s may depend on the choice of α. Recall the definitions of the fields K'_s, K''_s, L'_s and L_s. For convenience we give an overview of the fields defined in this chapter. The inclusions $L'_s\subset L_s$ and $K''_s\subset L_s$ follow from the next proposition. All other inclusions in the field diagram above follow directly from the definitions of the fields. We stress again that L''_s may depend on the choice of α. However from the next proposition it follows that L'_s does not depend on the choice of α.

Proposition 4.8. *Let $s\in K$. Let α and β be zeros of f_s. Then L_s equals $\mathbb{Q}''_s(\alpha+\alpha^{-1})$, the extension $\mathbb{Q}'_s(\alpha+\alpha^{-1})/\mathbb{Q}_s$ is Galois and $\mathbb{Q}'_s(\alpha+\alpha^{-1})$ equals $\mathbb{Q}'_s(\beta+\beta^{-1})$.*

Proof. Let $E=\mathbb{Q}''_s(\alpha+\alpha^{-1})$. First we prove $E\subset L_s$. Since α is a zero of $f_s=x^{16}-sx^8+1$, it follows that

$$\alpha^8+\alpha^{-8}=s, \tag{4.1}$$

hence

$$(\alpha^4+\alpha^{-4})^2=s+2 \tag{4.2}$$

and

$$(\alpha^4-\alpha^{-4})^2=s-2. \tag{4.3}$$

The element ζ_8 is contained in L_s, so L_s also contains the square roots of $-s-2$. Hence $\mathbb{Q}''_s\subset L_s$. Since $\alpha\in L_s$, we see $\alpha+\alpha^{-1}\in L_s$, so $E\subset L_s$, as desired. Next we show $L_s\subset E$. It suffices to show that $\zeta_8,\alpha\in E$. Equation (4.2) implies

$\sqrt{s+2} \in E$. By definition $s-2$ is a square in $\mathbb{Q}_s''$, so in the case $s=-2$ we have $\sqrt{-4} \in E$ and in the case $s \neq -2$ we have $\sqrt{-s-2}/\sqrt{s+2} = \sqrt{-1} \in E$. Since $\sqrt{2} \in E$, we conclude $\zeta_8 \in E$. Suppose $\alpha^2+\alpha^{-2}=0$ or $\alpha+\alpha^{-1}=0$. Then α is an element of the multiplicative group $\langle\zeta_8\rangle$, so $L_s \subset E$. Now suppose that both $\alpha^2+\alpha^{-2}$ and $\alpha+\alpha^{-1}$ are non-zero. Then the equation $(\alpha^2+\alpha^{-2})(\alpha^2-\alpha^{-2}) = \alpha^4-\alpha^{-4}$ yields $\alpha^2-\alpha^{-2} \in E$. Similarly $(\alpha+\alpha^{-1})(\alpha-\alpha^{-1}) = \alpha^2-\alpha^{-2}$ implies $\alpha-\alpha^{-1} \in E$. Hence $\alpha \in E$, so $L_s \subset E$. We conclude $L_s = \mathbb{Q}_s''(\alpha+\alpha^{-1})$.

Next we prove $\mathbb{Q}_s'(\alpha+\alpha^{-1})/\mathbb{Q}_s$ is Galois and $\mathbb{Q}_s'(\alpha+\alpha^{-1}) = \mathbb{Q}_s'(\beta+\beta^{-1})$. If $s=\pm 2$, then this follows from the fact that $L_s \subset \mathbb{Q}(\zeta_{16})$ and $\alpha+\alpha^{-1} \in \mathbb{Q}_s'$ (see the last two examples in the previous section). Suppose $s \neq \pm 2$. The field L_s is defined to be the splitting field of f_s over $\mathbb{Q}(s)$, so L_s is Galois over $\mathbb{Q}(s)$ and also over $\mathbb{Q}_s$. Let σ be an element of the Galois group of L_s over $\mathbb{Q}_s'(\alpha+\alpha^{-1})$. The equation $\alpha+\alpha^{-1} = \sigma(\alpha+\alpha^{-1})$ implies that σ keeps the coefficients of $(x-\alpha)(x-\alpha^{-1})$ fixed, so $\sigma(\alpha)=\alpha^{\pm 1}$. Since $\sqrt{2} \in \mathbb{Q}_s$, we also have $\sigma(\zeta_8) = \zeta_8^{\pm 1}$. From equation (4.2) and (4.3) we get

$$(\zeta_8^2(\alpha^8-\alpha^{-8}))^2 = 4-s^2. \tag{4.4}$$

Since $s \neq \pm 2$, equation (4.4) yields $\alpha \neq \alpha^{-1}$. We have $\sqrt{4-s^2} \in \mathbb{Q}_s'$, so σ keeps $\zeta_8^2(\alpha^8-\alpha^{-8})$ fixed. Hence either σ acts trivially on both α and ζ_8 or σ sends both α and ζ_8 to their multiplicative inverses. This implies that σ either is the identity or sends every zero of f_s to its multiplicative inverse. Therefore σ is in the center of G_s. Hence $\mathbb{Q}_s'(\alpha+\alpha^{-1})/\mathbb{Q}_s$ is Galois.

The element β is also a root of f_s, thus $\sigma(\beta+\beta^{-1}) = \beta+\beta^{-1}$. Hence $\beta+\beta^{-1} \in \mathbb{Q}_s'(\alpha+\alpha^{-1})$ and by symmetry $\alpha+\alpha^{-1} \in \mathbb{Q}_s'(\beta+\beta^{-1})$, so $\mathbb{Q}_s'(\alpha+\alpha^{-1}) = \mathbb{Q}_s'(\beta+\beta^{-1})$. □

Recall the definition of K_s''.

Proof of Proposition 4.1. The first three statements of Proposition 4.1 follow directly from Proposition 4.8 and the inclusions in the field diagram above.

It remains to show that $[K_s'' : K_s] = 2$ or 4. From the definition of K_s'' it is clear that $[K_s'' : K_s] = 1, 2$ or 4. The sum of $s-2$ and $-s-2$ is negative. Therefore K_s'' contains a square root of a negative real number, so K_s'' is not contained in $\mathbb{R}$. Since $K_s \subset \mathbb{R}$, the results follows. □

Proposition 4.9. *Let $s \in \mathcal{S}$. Then the group* $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$ *is cyclic of order* 8. *Furthermore* $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$ *is generated by a unique element ω that satisfies $\omega(\alpha) = \zeta_8^{-1}\alpha^{-1}$ and $\omega(\zeta_8) = \zeta_8^{-1}$.*

Proof. Proposition 3.3 implies $\mathrm{i} \notin \mathbb{Q}_s''$, so there exists an element σ in the Galois group $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$ such that $\sigma(\mathrm{i}) = -\mathrm{i}$. Since $\zeta_8+\zeta_8^{-1} \in \mathbb{Q}_s''$, we have $\sigma(\zeta_8) = \zeta_8^{-1}$. From $\sqrt{-s-2} \in \mathbb{Q}_s''$ we get $\mathbb{Q}_s''(\sqrt{s+2}) = \mathbb{Q}_s''(\mathrm{i})$, so $\sigma(\sqrt{s+2}) = -\sqrt{s+2}$. Since $\sqrt{s-2} \in \mathbb{Q}_s''$, we have

$$\sigma((\sqrt{s-2}+\sqrt{s+2})/2) \cdot (\sqrt{s-2}+\sqrt{s+2})/2 = (s-2-(s+2))/4 = -1.$$

Equations (4.2) and (4.3) imply $\alpha^4 = (\sqrt{s-2}+\sqrt{s+2})/2$ for some choice of $\sqrt{s+2}$ and $\sqrt{s-2}$. By the above calculation $\sigma(\alpha^4)\alpha^4 = -1$. Hence $\sigma(\alpha) =$

$\zeta_8^i\alpha^{-1}$ where $i \in \{1,3,5,7\}$. Since $\sigma^2(\alpha) = \pm\mathrm{i}\alpha$ and $\sigma^4(\alpha) = -\alpha$, we see that σ has order 8. Taking a suitable odd power of σ we get $\omega \in \mathrm{Gal}(L_s/\mathbb{Q}_s'')$ as defined in the proposition. Clearly the order of ω is 8. By equation (4.2) the element $\alpha+\alpha^{-1}$ is a zero of the polynomial $((x^2-2)^2-2)^2-(s+2)$. From Proposition 4.8 we get $L_s = \mathbb{Q}_s''(\alpha+\alpha^{-1})$. This yields $[L_s : \mathbb{Q}_s''] \leq 8$. Hence ω generates $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$, so $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$ is cyclic of order 8. □

Proof of Proposition 4.4. By definition of $\mathbb{Q}_s''$ the Galois group of $\mathbb{Q}_s''/\mathbb{Q}(s)$ is an abelian 2-group. Proposition 4.9 yields that $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$ is cyclic of order 8. Proposition 3.3 implies $\mathrm{i} \notin \mathbb{Q}_s''K$. Since $\zeta_8 \in L_s$, we have $\mathrm{i} \in L_s$. If we set $n = [\mathbb{Q}(s) : \mathbb{Q}]$, $E = \mathbb{Q}_s''$ and $F = L_s$, then all the hypotheses of Proposition 3.7 are satisfied. Proposition 3.7 implies $[L_s \cap K : \mathbb{Q}_s'' \cap K] = 1$ and Corollary 3.6 implies $[\mathbb{Q}_s'' \cap K : \mathbb{Q}(s)] \leq 2$. By definition $K_s = L_s \cap K$, therefore $[K_s : \mathbb{Q}(s)] = [\mathbb{Q}_s'' \cap K : \mathbb{Q}(s)] \leq 2$ and $K_s = L_s \cap K = \mathbb{Q}_s'' \cap K$. Thus $K_s \subset \mathbb{Q}_s''$, so $K_s'' \subset \mathbb{Q}_s''$. Clearly $\mathbb{Q}_s'' \subset K_s''$, thus we have $K_s'' = \mathbb{Q}_s''$. □

Lemma 4.10. *Let $s \in K$ be a potential starting value. Then $L_s' \cap K_s'' = K_s'$ and $L_s'' \cap K_s' = K_s$.*

Proof. By Proposition 4.4 we have $K_s'' = \mathbb{Q}_s''$ and from Proposition 4.8 we get $L_s = K_s''(\alpha+\alpha^{-1})$. Hence Proposition 4.9 implies $[L_s : K_s''] = 8$. This yields $[L_s' : K_s'] \geq 8$ and $[L_s'' : K_s] \geq 8$. Since the element $\alpha+\alpha^{-1}$ is a zero of the polynomial $((x^2-2)^2-2)^2-(s+2)$, we can conclude that $[L_s' : K_s'] = 8$ and $[L_s'' : K_s] = 8$. We have $8 = [L_s : K_s''] \leq [L_s' : L_s' \cap K_s''] \leq [L_s' : K_s'] = 8$, so $L_s' \cap K_s'' = K_s'$. Similarly we have $8 = [L_s' : K_s'] \leq [L_s'' : L_s'' \cap K_s'] \leq [L_s'' : K_s] = 8$, so $L_s'' \cap K_s' = K_s$. □

Proof of Proposition 4.2. Let $s \in \mathcal{S}$. Then Proposition 4.1, Proposition 4.4 and Lemma 4.10 imply $L_s = K_s''L_s'$, $L_s' \cap K_s'' = K_s'$ and both L_s'/K_s' and K_s''/K_s' are Galois. Hence the restriction map from $\mathrm{Gal}(L_s/K_s')$ to $\mathrm{Gal}(L_s'/K_s') \times \mathrm{Gal}(K_s''/K_s')$ is an isomorphism. The second part of the proposition follows directly from Proposition 4.4 and Proposition 4.9. □

Proof of Proposition 4.3. By definition of L_s' we have $L_s' = L_s''K_s'$. From Lemma 4.10 we get $L_s'' \cap K_s' = K_s$. The group $\mathrm{Gal}(L_s'/K_s')$ is normal in $\mathrm{Gal}(L_s'/K_s)$. Hence $G_s = \mathrm{Gal}(L_s'/L_s'')\mathrm{Gal}(L_s'/K_s')$ and $\mathrm{Gal}(L_s'/L_s'') \cap \mathrm{Gal}(L_s'/K_s')$ is the trivial subgroup of G_s, so the exact sequence in the proposition splits.

Proposition 4.2 implies that $\mathrm{Gal}(L_s'/K_s')$ is cyclic of order 8. From the definition of K_s' we see $[K_s' : K_s] = 1$ or 2. Suppose $[K_s' : K_s] = 2$. Then by Lemma 4.10 we have $[L_s' : L_s''] = 2$. Let $\sigma \in \mathrm{Gal}(L_s/L_s'') \backslash \mathrm{Gal}(L_s/L_s')$. The equation $\alpha+\alpha^{-1} = \sigma(\alpha+\alpha^{-1})$ implies that σ keeps the coefficients of $(x-\alpha)(x-\alpha^{-1})$ fixed, so $\sigma(\alpha) = \alpha^{\pm1}$. Since σ does not leave $\sqrt{4-s^2}$ fixed and $\zeta_8 + \zeta_8^{-1} \in K_s$, equation (4.4) implies: if $\sigma(\alpha) = \alpha$ then $\sigma(\zeta_8) = \zeta_8^{-1}$, and if $\sigma(\alpha) = \alpha^{-1}$ then $\sigma(\zeta_8) = \zeta_8$. These two possibilities yield $\sigma(\zeta_8\alpha) = \zeta_8^{-1}\alpha$ or $\zeta_8\alpha^{-1}$. Let ω be as in Proposition 4.2. Now we calculate $\sigma\omega\sigma\omega(\alpha+\alpha^{-1})$. We have $\sigma\omega\sigma\omega(\alpha+\alpha^{-1}) = \sigma\omega\sigma(\zeta_8^{-1}\alpha^{-1}+\zeta_8\alpha) = \sigma\omega(\zeta_8^{-1}\alpha+\zeta_8\alpha^{-1}) = \sigma(\zeta_8\zeta_8^{-1}\alpha^{-1}+\zeta_8^{-1}\zeta_8\alpha) = \sigma(\alpha+\alpha^{-1}) = \alpha+\alpha^{-1}$. One easily sees $\sigma\omega\sigma\omega(\zeta_8) = \zeta_8$.

Hence $\sigma\omega\sigma\omega$ is the identity of $\mathrm{Gal}(L_s/L_s'')$, so $\sigma\omega\sigma = \omega^{-1}$. Now we restrict every element in the identity $\sigma\omega\sigma = \omega^{-1}$ to the field L_s' in order to conclude that the non-trivial element of $\mathrm{Gal}(K_s'/K_s)$ acts as -1 on $\mathrm{Gal}(L_s'/K_s')$. □

Proof of Proposition 4.5. Let $s \in \mathcal{S}$ and let α a zero of f_s. In the following table we calculated the action of ω^i on α and ζ_8 for $i \in \mathbb{Z}_{\geq 0}$.

ω^0	ω^1	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
α	$\zeta_8^{-1}\alpha^{-1}$	$\zeta_8^2\alpha$	$\zeta_8^{-3}\alpha^{-1}$	$\zeta_8^4\alpha$	$\zeta_8^{-5}\alpha^{-1}$	$\zeta_8^6\alpha$	$\zeta_8^{-7}\alpha^{-1}$
ζ_8	ζ_8^{-1}	ζ_8	ζ_8^{-1}	ζ_8	ζ_8^{-1}	ζ_8	ζ_8^{-1}

Let $j \in \{1, 3, 5, 7\}$. Then

$$\lambda_s([\omega^j]) = \frac{\omega^j(\alpha)\alpha + \omega^j(\alpha^{-1})\alpha^{-1}}{\sqrt{2}} = \frac{\zeta^{-j}\alpha^{-1}\alpha + \zeta^j\alpha\alpha^{-1}}{\sqrt{2}} = \frac{\zeta_8^j + \zeta_8^{-j}}{\sqrt{2}}$$

is an element of $\{+1, -1\}$. Let β be a zero of f_s. Then β equals $\zeta_8^i\alpha^{\pm 1}$ for some $i \in \mathbb{Z}/8\mathbb{Z}$ and choice of sign. Since

$$\omega^j(\beta)\beta = \omega^j(\zeta_8^i\alpha^{\pm 1})\zeta_8^i\alpha^{\pm 1} = \zeta_8^{-i}\omega^j(\alpha^{\pm 1})\zeta_8^i\alpha^{\pm 1} = \omega^j(\alpha^{\pm 1})\alpha^{\pm 1},$$

we also see that λ_s is independent of the choice of α. By definition of ζ_8 we have $\zeta_8 + \zeta_8^{-1} = \sqrt{2} = \zeta_8^7 + \zeta_8^{-7}$. Multiplying the equation by ζ_8^4 we see $\zeta_8^3 + \zeta_8^{-3} = -\sqrt{2} = \zeta_8^5 + \zeta_8^{-5}$. Hence $\lambda_s([\omega]) = \lambda_s([\omega^7]) = +1$ and $\lambda_s([\omega^3]) = \lambda_s([\omega^5]) = -1$. Since $[\omega] \subset \{\omega, \omega^{-1}\}$ (see end of the proof of Proposition 4.3), we see that λ_s is well-defined. □

Let s be a potential starting value. The following proposition will be used in Chapter 9. It describes the intermediate fields of L_s'/K_s'.

Proposition 4.11. *Let s be a potential starting value. Then we have the inclusions*

$$K_s' \subsetneq K_s'(\sqrt{2+s}) \subsetneq K_s'\Big(\sqrt{2+\sqrt{2+s}}\Big) \subsetneq K_s'\Big(\sqrt{2+\sqrt{2+\sqrt{2+s}}}\Big) = L_s'.$$

Moreover these fields are all the intermediate fields of the extension L_s'/K_s'.

Proof. Since α is a zero of $f = x^{16} - sx^8 + 1$, it follows that $\alpha^8 + \alpha^{-8} = s$. Hence $(((\alpha + \alpha^{-1})^2 - 2)^2 - 2)^2$ equals $2 + s$. By Proposition 4.1 the field L_s' is Galois over K_s. Hence we have

$$K_s'\Big(\sqrt{2+\sqrt{2+\sqrt{2+s}}}\Big) = L_s'.$$

By Proposition 4.3 the Galois group of L_s'/K_s' is cyclic of order 8. From this Proposition 4.11 follows. □

Chapter 5

The Lehmer symbol

In this chapter we state an observation made by Lehmer giving rise to what we will call the *Lehmer symbol* (see [4, §A3, page 9]), which is the main object of study in this thesis. After we have introduced this symbol, we will relate it to the so-called *Frobenius symbol.* In Chapters 7 and 9 properties of the Frobenius symbol will be used to prove properties of the Lehmer symbol.

Lehmer's observation and the Frobenius symbol

We start with stating Lehmer's observation. Let $p \in \mathbb{Z}_{>2}$ be such that $M_p = 2^p - 1$ is prime, so in particular p is an odd prime. Let $s \in K$ be a starting value for p (see Definition 2.5). Let $(s \bmod M_p)$ be as in Definition 2.4. Define s_i for $i \in \{1, 2, \ldots, p-1\}$ by $s_1 = (s \bmod M_p)$ and $s_{i+1} = s_i^2 - 2$.

Proposition 5.1. *Let the assumptions be as above. Then we have* $s_{p-2} = \epsilon(s,p)2^{(p+1)/2}$ *for a unique* $\epsilon(s,p) \in \{-1,+1\}$.

In order to see this, note that by Theorem 2.1 we have $s_{p-1} = 0$. So Proposition 5.1 follows from

$$0 = s_{p-1} = s_{p-2}^2 - 2 = s_{p-2}^2 - 2^{p+1} = (s_{p-2} - 2^{(p+1)/2})(s_{p-2} + 2^{(p+1)/2})$$

and the fact that M_p is prime.

Now we will define $\epsilon(s,p)$ for s in the field $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ of characteristic zero. Take $s \in K$. Define $P(s)$ by

$$P(s) = \{p \in \mathbb{Z}_{>2} : M_p \text{ is prime and } s \text{ is a starting value for } p\}.$$

Definition 5.2. *Let* $s \in K$ *and* $p \in P(s)$. *We define the Lehmer symbol* $\epsilon(s,p)$ *by*

$$\epsilon(s,p) = \epsilon(s \bmod M_p, p).$$

Next we define the Frobenius symbol. Let F/E be a finite Galois extension of number fields with Galois group G. Let $\mathfrak{m}$ be a non-zero prime ideal of the ring of integers $\mathcal{O}_E$ of E that is unramified in F. Let $\mathfrak{M}$ be a prime ideal of the ring of integers $\mathcal{O}_F$ of F above $\mathfrak{m}$, i.e. $\mathcal{O}_E \cap \mathfrak{M} = \mathfrak{m}$. Let H be a subgroup of G. We denote the fixed field of H by L.

Theorem 5.3. *There is a unique element* $\mathrm{Frob}_{\mathfrak{M}}$ *in* G *with the property*

$$\forall x \in \mathcal{O}_F\colon \quad \mathrm{Frob}_{\mathfrak{M}}(x) \equiv x^{\#(\mathcal{O}_E/\mathfrak{m})} \bmod \mathfrak{M},$$

where $\#(\mathcal{O}_E/\mathfrak{m})$ *is the number of elements of* $\mathcal{O}_E/\mathfrak{m}$*. Furthermore the inertia degree of* $\mathcal{O}_L \cap \mathfrak{M}$ *over* $\mathfrak{m}$ *is* 1 *if and only if* $\mathrm{Frob}_{\mathfrak{M}} \in H$*.*

For a proof of Theorem 5.3 see the next section. We call the unique element $\mathrm{Frob}_{\mathfrak{M}}$ of Theorem 5.3 the *Frobenius symbol* of $\mathfrak{M}$ over E. If we want to make the extension F/E explicit, then we denote $\mathrm{Frob}_{\mathfrak{M}}$ by

$$(\mathfrak{M}, F/E) \text{ or } \left(\frac{\mathfrak{M}}{F/E}\right).$$

The Galois group G acts transitively on the set of prime ideals of $\mathcal{O}_F$ above $\mathfrak{m}$ and $(\sigma(\mathfrak{M}), F/E) = \sigma(\mathfrak{M}, F/E)\sigma^{-1}$ for any $\sigma \in G$ (see [7, Chapter I, §5]). Therefore the conjugacy class of $(\mathfrak{M}, F/E)$ in G does not depend on the choice of a prime $\mathfrak{M}$ above $\mathfrak{m}$. Hence we can define $(\mathfrak{m}, F/E)$ to be the conjugacy class of $(\mathfrak{M}, F/E)$ in G. When it is clear in which extension we work we will denote $(\mathfrak{m}, F/E)$ by $\mathrm{Frob}_{\mathfrak{m}}$.

We will also use the so-called consistency property of the Frobenius symbol. We will state this property in the next proposition. Let F' be a number field such that $E \subset F' \subset F$ and F'/E Galois. Let $\mathfrak{M}'$ be the prime below $\mathfrak{M}$ in F', i.e. $\mathfrak{M}' = \mathfrak{M} \cap F'$.

Proposition 5.4. *We have* $(\mathfrak{M}, F/E)|_{F'} = (\mathfrak{M}', F'/E)$*, where* $(\mathfrak{M}, F/E)|_{F'}$ *is the restriction of* $(\mathfrak{M}, F/E)$ *to the field* F'*.*

For a proof of Proposition 5.4 see [7, Chapter X, §1].

Now we relate the Lehmer symbol and the Frobenius symbol. First we recall some notation of Chapter 4. Let $s \in K$ be a potential starting value, let $f_s = x^{16} - sx^8 + 1$ and let L_s be the splitting field of f_s over $\mathbb{Q}(s)$. Define K_s by $K_s = L_s \cap K$ and let $n \in \mathbb{Z}_{>0}$ be such that $K_s = \mathbb{Q}(\sqrt[n]{2})$. Define $K_s'' = K_s(\sqrt{s-2}, \sqrt{-s-2})$. As in Chapter 4 let $G_s = \mathrm{Gal}(L_s/K_s)$ be the Galois group of L_s over K_s. Recall that the equivalence relation $\sim$ on G_s is defined by conjugation. Note that the set $\mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}$ of elements of order 8 in $\mathrm{Gal}(L_s/K_s'')$ is closed under $\sim$.

Proposition 5.5. *Let* $s \in K$ *and let* $p \in P(s)$*. Then the ideal* $(\sqrt[n]{2}^p - 1)$ *in* $\mathcal{O}_{K_s}$ *is prime and unramified in* L_s*. Furthermore we have* $\mathrm{Frob}((\sqrt[n]{2}^p - 1), L_s/K_s) \in \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim}$*.*

We prove Proposition 5.5 in the last section of this chapter. Recall the map

$$\lambda_s : \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim} \to \{+1,-1\}$$

of Chapter 4. We define the map

$$\epsilon_s : P(s) \to \{+1,-1\}$$

by $\epsilon_s : p \mapsto \epsilon(s,p)$ and we define a map

$$\mathrm{Frob} : P(s) \to \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}$$

by $p \mapsto \mathrm{Frob}((\sqrt[n]{2}^p - 1), L_s/K_s)$. Note that this map is well-defined by Proposition 5.5.

The following theorem relates the Lehmer symbol to the Frobenius symbol.

Theorem 5.6. *Let $s \in K$ be a potential starting value. Then the diagram*

$$\begin{tikzcd}
P(s) \arrow[r, "\epsilon_s"] \arrow[dr, "\mathrm{Frob}"'] & \{+1,-1\} \\
 & \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim} \arrow[u, "\lambda_s"']
\end{tikzcd}$$

commutes.

A proof of Theorem 5.6 can be found in the last section of this chapter.

We finish this section with a corollary of Theorem 5.6. First we recall some notation of Chapter 4. The map $r : \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim} \to \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim}$ induced by the restriction map $\mathrm{Gal}(L_s/K_s) \to \mathrm{Gal}(L_s'/K_s)$ is bijective. We define the map $\mathrm{Frob}' = r \circ \mathrm{Frob}$ from $P(s)$ to $\mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim}$. Note that the consistency property implies $\mathrm{Frob}'(p) = \mathrm{Frob}((\sqrt[n]{2}^p - 1), L_s'/K_s)$. Recall the map $\lambda_s' : \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim} \to \{+1,-1\}$ (see Definition 4.6). Now Theorem 5.6 and the definition of λ_s' yield the following corollary.

Corollary 5.7. *Let $s \in K$ be a potential starting value. Then the diagram*

$$\begin{tikzcd}
P(s) \arrow[r, "\epsilon_s"] \arrow[dr, "\mathrm{Frob}'"'] & \{+1,-1\} \\
 & \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim} \arrow[u, "\lambda_s'"']
\end{tikzcd}$$

commutes.

Corollary 5.7 implies that if $p, q \in P(s)$ and $\mathrm{Frob}'(p) = \mathrm{Frob}'(q)$ then p and q have the same Lehmer symbol.

In the next chapter we state well-known properties of the Frobenius symbol. In the case $\mathrm{Gal}(L_s'/K_s)$ is abelian these properties allow us to calculate the Lehmer symbol more efficiently than by direct calculation of $\epsilon_s(p)$.

Ramification and ramification groups

In this section we introduce decomposition groups and ramification groups. The proposition that we state about these groups will imply Theorem 5.3.

Let F/E be a Galois extension of number fields with Galois group G. Let $\mathfrak{M}$ be a non-zero prime ideal of $\mathcal{O}_F$, let $\mathfrak{m} = \mathcal{O}_E \cap \mathfrak{M}$ and let $p \in \mathbb{Z}$ be the prime number below $\mathfrak{M}$, i.e. $(p) = \mathbb{Z} \cap \mathfrak{M}$. We define the decomposition group $G_{\mathfrak{M}}$ of $\mathfrak{M}$ by

$$G_{\mathfrak{M}} = \{\sigma \in G : \sigma(\mathfrak{M}) = \mathfrak{M}\}.$$

Since $\sigma \in G_{\mathfrak{M}}$ leaves $\mathfrak{M}$ fixed and is the identity on $\mathcal{O}_E$, the element σ induces an element $\overline{\sigma}$ of $\overline{G}_{\mathfrak{M}} = \mathrm{Gal}((\mathcal{O}_F/\mathfrak{M})/(\mathcal{O}_E/\mathfrak{m}))$. Hence we have a group homomorphism

$$r : G_{\mathfrak{M}} \to \overline{G}_{\mathfrak{M}}.$$

For $n \in \mathbb{Z}_{\geq 0}$ we define the n-th ramification group $V_{\mathfrak{M},n}$ of $\mathfrak{M}$ by

$$V_{\mathfrak{M},n} = \{\sigma \in G : \text{for all } x \in \mathcal{O}_F \text{ we have } \sigma(x) \equiv x \bmod \mathfrak{M}^{n+1}\}.$$

Denote the fixed field of $G_{\mathfrak{M}}$ by D and denote the fixed field of $V_{\mathfrak{M},n}$ by T_n. Let L be a number field such that $E \subset L \subset F$. In the following proposition we state well-known results about the decomposition group and the ramification groups that we will use in this thesis (see [14, Chapter 1 §7 and §8, Chapter 4]).

Proposition 5.8. *We have:*

(i) *the map r is surjective and has kernel $V_{\mathfrak{M},0}$,*
(ii) $\forall \sigma \in G\ \forall n \in \mathbb{Z}_{\geq 0} :\ G_{\sigma(\mathfrak{M})} = \sigma G_{\mathfrak{M}} \sigma^{-1}$ *and* $V_{\sigma(\mathfrak{M}),n} = \sigma V_{\mathfrak{M},n} \sigma^{-1}$,
(iii) $e(\mathcal{O}_L \cap \mathfrak{M}/\mathfrak{m}) = f(\mathcal{O}_L \cap \mathfrak{M}/\mathfrak{m}) = 1$ *if and only if* $L \subset D$,
(iv) $e(\mathcal{O}_L \cap \mathfrak{M}/\mathfrak{m}) = 1$ *if and only if* $L \subset T_0$,
(v) *there is an injective group homomorphism* $V_{\mathfrak{M},0}/V_{\mathfrak{M},1} \to (\mathcal{O}_F/\mathfrak{M})^*$,
(vi) $V_{\mathfrak{M},1} = \{\sigma \in V_{\mathfrak{M},0} :$ *order of σ equals p^n for some $n \in \mathbb{Z}_{\geq 0}$*$\}$.

Proof of Theorem 5.3. Let the notation be as in Theorem 5.3. By assumption $\mathfrak{m}$ is unramified in F. Now proposition 5.8(iv) implies $T_0 = F$, so V_0 is the trivial group. Hence by Proposition 5.8(i) the map r is an isomorphism. We know by the theory of finite fields that there exists a unique element $\overline{\sigma} \in \overline{G}_{\mathfrak{M}}$ defined by $\overline{\sigma} : x \mapsto x^{\#(\mathcal{O}_E/\mathfrak{m})}$ that generates $\overline{G}_{\mathfrak{M}}$. Hence there exists an element $\mathrm{Frob}_{\mathfrak{M}} \in G$ that has the property described in Theorem 5.3. To prove uniqueness we have to show that every $\sigma \in G$ with the property as described in Theorem 5.3 belongs to $G_{\mathfrak{M}}$. Let $\sigma \in G$ be an element with the property described in Theorem 5.3. Suppose $x \in \mathfrak{M}$. Then we have $\sigma(x) \equiv x^{\#(\mathcal{O}_E/\mathfrak{m})} \equiv 0 \bmod \mathfrak{M}$, so $\sigma(\mathfrak{M}) \subset \mathfrak{M}$. Since σ has finite order, we see that $\sigma(\mathfrak{M}) = \mathfrak{M}$. Hence we have $\sigma \in G_{\mathfrak{M}}$. Therefore we conclude that the element $\mathrm{Frob}_{\mathfrak{M}}$ is unique. The second part of Theorem 5.3 follows directly from (iii). □

We finish this section with a proposition that controls the ramification in L_s/K_s. Let $\mathfrak{d}_s = \{x \in \mathcal{O}_{K_s} : x \cdot s \in \mathcal{O}_{K_s}\}$ be the denominator ideal of $s \in K$.

Proposition 5.9. *Let $s \in K$. If a non-zero prime ideal $\mathfrak{m}$ of $\mathcal{O}_{K_s}$ ramifies in L_s then $\mathfrak{m} \mid 2\mathfrak{d}_s$ or $\mathfrak{m}$ ramifies in $K_s(\sqrt{4-s^2})$.*

Proof of Proposition 5.9. We recall from the first section of Chapter 4 that $L_s = K_s(\alpha, \zeta_8)$. If a non-zero prime ideal $\mathfrak{m}$ of $\mathcal{O}_{K_s}$ ramifies then it ramifies in $K_s(\alpha^8, \zeta_8)/K_s$ or in $L_s/K_s(\alpha^8, \zeta_8)$.

By definition of α the element α^8 is a zero of the polynomial $x^2 - sx + 1$, hence $K_s(\alpha^8, \zeta_8) = K_s(\sqrt{4-s^2}, \zeta_8)$. In the extension $K_s(\zeta_8)/K_s$ only the prime ideal $(\sqrt[n]{2})$ can ramify, hence if $\mathfrak{m}$ ramifies in $K_s(\alpha^8, \zeta_8)/K_s$ then $\mathfrak{m}|2$ or $\mathfrak{m}$ ramifies in $K_s(\sqrt{4-s^2})/K_s$.

Let $d \in \mathfrak{d}_s$. Then $d \cdot s$ is an element of $\mathcal{O}_K$, so $g = x^2 - dsx + d^2 \in \mathcal{O}_K[x]$. Both $d\alpha^8$ and $d\alpha^{-8}$ are zeros of g. Hence it follows that $d\alpha^8, d\alpha^{-8} \in \mathcal{O}_K$. Therefore the zero $d\alpha$ of the polynomial $x^8 - (d\alpha)^8$ is an algebraic integer. Hence if $\mathfrak{m}$ ramifies in $L_s/K_s(\alpha^8, \zeta_8)$ then $\mathfrak{m}|8(d\alpha)^8$ (see [7, Chapter II, §2]). Similarly if $\mathfrak{m}$ ramifies in $L_s/K_s(\alpha^8, \zeta_8)$ then $\mathfrak{m}|8(d\alpha^{-1})^8$. Therefore $\mathfrak{m}$ divides $8(d\alpha)^8 \cdot 8(d\alpha^{-1})^8 = 64d^{16}$, so $\mathfrak{m}|2d$. Hence if $\mathfrak{m}$ ramifies in $L_s/K_s(\alpha^8, \zeta_8)$ then $\mathfrak{m}|2\mathfrak{d}_s$. □

Relating the symbols

In this section we prove Proposition 5.5 (actually we prove a stronger result, namely Proposition 5.10 below) and Theorem 5.6. Let $s \in K$. Recall the definitions of L_s, L'_s, K''_s, K'_s and K_s of Chapter 4.

Proposition 5.10. *Let $s \in K$, take $p \in P(s)$ and set $n = [K_s : \mathbb{Q}]$. Define $\mathfrak{m}_p$ to be the ideal $(\sqrt[n]{2}^p - 1)$ of $\mathcal{O}_{K_s}$. Then we have:*

(i) *s is a potential starting value,*
(ii) *$\mathfrak{m}_p$ is a prime ideal of $\mathcal{O}_{K_s}$ of degree one over $\mathbb{Q}$ unramified in L_s,*
(iii) *$\mathrm{Frob}_{\mathfrak{M}_p}$ generates the group $\mathrm{Gal}(L_s/K''_s)$,*
(iv) *$\mathrm{Frob}_{\mathfrak{M}'_p}$ generates the group $\mathrm{Gal}(L'_s/K'_s)$,*

where $\mathfrak{M}_p$ and $\mathfrak{M}'_p$ are prime ideals of $\mathcal{O}_{L_s}$ and $\mathcal{O}_{L'_s}$ above $\mathfrak{m}_p$ respectively.

Proof. (i) The assumption $p \in P(s)$ implies by definition that s is a starting value for p and that p is odd. Hence s is by Theorem 3.2 a potential starting value.

(ii) By Proposition 4.4 the integer $[K_s : \mathbb{Q}(s)]$ equals 1 or 2. Since $p \in P(s)$, we have $\gcd(p, [\mathbb{Q}(s) : \mathbb{Q}]) = 1$ and p is odd. Hence we have $\gcd(p, [K_s : \mathbb{Q}]) = 1$. Since n is even, we see that the absolute norm of $\sqrt[n]{2}^p - 1$ is $(-1)^n \cdot -M_p = -M_p$. Hence $\mathfrak{m}_p$ is a prime of degree one and the fields $\mathcal{O}_{K_s}/\mathfrak{m}_p$ and $\mathbb{Z}/M_p\mathbb{Z}$ are isomorphic. Since $p \in P(s)$, we can write $s = r/t$ with $r \in R_p$ and $t \in S_p$ (see Definition 2.5). By definition of R_p and S_p there is a positive integer $m \in n\mathbb{Z}$ such that $r, t \in \mathbb{Z}[\sqrt[m]{2}]$ and $p \nmid m$. The prime $\mathfrak{M}_p = (\sqrt[m]{2}^p - 1)$ of $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$ lies above $\mathfrak{m}_p$. Since $t \in S_p$ and S_p is the inverse image of $(\mathbb{Z}/M_p\mathbb{Z})^*$ under the map $\varphi_p : R_p \to \mathbb{Z}/M_p\mathbb{Z}$ (see Chapter 2), the prime $\mathfrak{M}_p$ does not divide the ideal (t)

of $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$. Hence we have $\operatorname{ord}_{\mathfrak{m}_p}(s) \geq 0$, so $4 - s^2$ maps naturally to $\mathcal{O}_{K_s}/\mathfrak{m}_p$ and $\mathfrak{m}_p$ does not divide the denominator ideal $\mathfrak{d}_s$ of s.

Since s is a starting value for p, it follows that $4 - s^2$ is a nonzero square in $\mathbb{Z}/M_p\mathbb{Z}$. Therefore $4 - s^2$ is a nonzero square in $\mathcal{O}_{K_s}/\mathfrak{m}_p$, so $\mathfrak{m}_p$ splits completely in $K_s(\sqrt{4 - s^2})$. Now Proposition 5.9 implies (ii).

(iii) From (ii) it follows that $\mathfrak{m}_p$ is unramified in L_s. In the proof of (ii) we showed that $\operatorname{ord}_{\mathfrak{m}_p}(s) \geq 0$. Since s is a starting value for p, the elements $s - 2$ and $-s - 2$ are nonzero squares in $\mathbb{Z}/M_p\mathbb{Z}$. Hence the natural images of $s - 2$ and $-s - 2$ are nonzero squares in $\mathcal{O}_{K_s}/\mathfrak{m}_p$. From this it follows that $\mathfrak{m}_p$ splits completely in $K''_s = K_s(\sqrt{s-2}, \sqrt{-s-2})$. The primes above $\mathfrak{m}_p$ in K''_s are inert in the extension $K''_s(\alpha^4 + \alpha^{-4}) = K''_s(\mathrm{i})$ over K''_s since $\left(\frac{-1}{M_p}\right) = -1$. Now Theorem 5.3 implies that $(\mathfrak{m}''_p, K''_s(\mathrm{i})/K''_s)$ generates $\operatorname{Gal}(K''_s(\mathrm{i})/K''_s)$, where $\mathfrak{m}''_p$ is the prime of K''_s below $\mathfrak{M}_p$. By Proposition 4.2 the extension L_s/K''_s is cyclic of order 8. By Proposition 5.4 the element $(\mathfrak{m}''_p, L_s/K''_s)$ generates $\operatorname{Gal}(L_s/K''_s)$. Since $\operatorname{Gal}(L_s/K''_s)$ is abelian and $\mathfrak{M}_p$ lies above $\mathfrak{m}''_p$, the element $(\mathfrak{m}''_p, L_s/K''_s)$ equals $\operatorname{Frob}_{\mathfrak{M}_p}$. This completes the proof of (iii).

(iv) Take $\mathfrak{M}_p$ above $\mathfrak{M}'_p$. By (iii) we know that $(\mathfrak{M}_p, L_s/K_s)$ generates $\operatorname{Gal}(L_s/K''_s)$. Using Proposition 4.2 and Proposition 5.4 for the extension $K_s \subset L'_s \subset L_s$ yields that $(\mathfrak{M}'_p, L'_s/K_s)$ generates $\operatorname{Gal}(L'_s/K'_s)$. □

Proof of Proposition 5.5. Directly from Proposition 5.10(ii) and (iii). □

Proof of Theorem 5.6. Let $\mathcal{O}_{L_s}$ be the ring of integers of L_s. Since ring morphisms respect inverting, it follows that Theorem 5.3 can also be applied to elements x in the local ring $(\mathcal{O}_{L_s})_{\mathfrak{M}_p}$, where $\mathfrak{M}_p$ is as above.

Let $p \in P(s)$. Then $(s \bmod M_p) \in \mathbb{Z}/M_p\mathbb{Z}$ is defined. Hence α, a root of the polynomial $x^{16} - sx^8 + 1$, is an element of $(\mathcal{O}_{L_s})_{\mathfrak{M}_p}$. By Theorem 5.3 we have

$$\operatorname{Frob}_{\mathfrak{M}_p}(\alpha)\alpha + \operatorname{Frob}_{\mathfrak{M}_p}(\alpha^{-1})\alpha^{-1} = \alpha^{M_p+1} + \alpha^{-(M_p+1)} = (\alpha^8)^{2^{p-3}} + (\alpha^{-8})^{2^{p-3}}$$

in the field $\mathcal{O}_{L_s}/\mathfrak{M}_p$. Recall that

$$s_{i+1} = s_i^2 - 2.$$

From $s_1 = s = \alpha^8 + \alpha^{-8}$ we get $s_{p-2} = (\alpha^8)^{2^{p-3}} + (\alpha^{-8})^{2^{p-3}}$. Note $\zeta_8 \in L_s$ implies that n is even. Hence $\sqrt{2} - 2^{(p+1)/2} = \sqrt{2}(1 - \sqrt{2}^p)$ and $\mathfrak{M}_p \mid (1 - \sqrt[n]{2}^p) \mid (1 - \sqrt{2}^p)$ imply

$$(\alpha^8)^{2^{p-3}} + (\alpha^{-8})^{2^{p-3}} = s_{p-2} = \epsilon(s,p)2^{(p+1)/2} = \epsilon(s,p)\sqrt{2}$$

in the field $\mathcal{O}_{L_s}/\mathfrak{M}_p$. This means that the equality

$$(\operatorname{Frob}_{\mathfrak{M}_p}(\alpha)\alpha + \operatorname{Frob}_{\mathfrak{M}_p}(\alpha^{-1})\alpha^{-1})/\sqrt{2} = \epsilon(s,p)$$

holds in the field $\mathcal{O}_{L_s}/\mathfrak{M}_p$. By Proposition 5.10(iii) the element $[\operatorname{Frob}_{\mathfrak{m}_p}]$ is in the domain of λ_s. Applying Proposition 4.5 we see that

$$\epsilon_s = \lambda_s \circ \operatorname{Frob}.$$

□

Chapter 6

Class field theory

Theorem 5.6 relates the Lehmer symbol to the Frobenius symbol. For abelian extensions of number fields one can calculate the Frobenius symbol using the Artin map of class field theory. In this chapter we will introduce class field theory. In the next chapter we will apply class field theory to prove properties of the Lehmer symbol.

The Artin map

In this section we will briefly explain the Artin map. We also state the theorems of class field theory concerning the Artin map that we apply in the next chapter.

Let F/E be a finite abelian extension of number fields with Galois group G and discriminant Δ. Let $\mathfrak{p} \neq 0$ be a prime of E relatively prime to Δ, so that $\mathfrak{p}$ is unramified in F/E. Let $\mathfrak{P}$ be a prime ideal of the ring of integers of F such that $\mathfrak{P} \cap \mathcal{O}_E = \mathfrak{p}$, i.e. $\mathfrak{P}$ lies above $\mathfrak{p}$. In the previous chapter we introduced the Frobenius symbol. The Frobenius symbol has the property $\sigma(\mathfrak{P}, F/E)\sigma^{-1} = (\sigma(\mathfrak{P}), F/E)$ for any $\sigma \in G$. The extension F/E is abelian, so the Frobenius symbol does not depend on the choice of the prime $\mathfrak{P}$. Hence we can define $\mathrm{Frob}_{\mathfrak{p}}$ by $(\mathfrak{P}, F/E)$.

Let $I = I_E(\Delta)$ be the group of fractional ideals generated by the prime ideals $\mathfrak{p} \nmid \Delta$ of $\mathcal{O}_E$. The group I is a free abelian group generated by the set of primes of E relatively prime to Δ. The *Artin map* is the group homomorphism

$$I \to G$$

defined on the generators $\mathfrak{p}$ of I by

$$\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}.$$

From class field theory it follows that the Artin map is surjective. This theory also gives a description of the kernel of the Artin map.

In order to describe the kernel of the Artin map we will use the notion of a totally positive element. A real embedding of E is a ring homomorphism from

E to the field of real numbers $\mathbb{R}$. An element $x \in E$ is called *totally positive* in F/E if for every real embedding σ of E which is not induced by a real embedding of F we have $\sigma(x) > 0$.

Theorem 6.1. *Let F/E be a finite abelian extension of number fields. Let $\mathcal{O}_E$ be the ring of integers of E. Then there exists a non-zero ideal $\mathfrak{f}$ in $\mathcal{O}_E$, which is divisible by all ramified primes in F/E, such that for each $x \in E^*$ with*

(i) $\operatorname{ord}_{\mathfrak{p}}(x-1) \geq \operatorname{ord}_{\mathfrak{p}}(\mathfrak{f})$ *for all prime ideals* $\mathfrak{p} \mid \mathfrak{f}$,
(ii) x *is totally positive in* F/E,

the ideal $(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(x)}$ is in the kernel of the Artin map, where the product runs over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_E$. Furthermore, the Artin map is surjective.

For a proof of Theorem 6.1 see [7, Chapter X, §1, Theorem 1] and [7, Chapter X, §2, Theorem 2]. We call an ideal $\mathfrak{f}$ for which the conclusion of Theorem 6.1 holds a *modulus* for F/E.

Theorem 6.2. *If $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are two moduli for F/E then their greatest common divisor* $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ *is also a modulus.*

For a proof of Theorem 6.2 see [5, Chapter V, §6]. From Theorem 6.2 it follows that for every extension F/E of number fields, we have a unique modulus $\mathfrak{f}$ for F/E such that every modulus of F/E is divisible by $\mathfrak{f}$. We call this modulus $\mathfrak{f}$ the *conductor* of F/E. (Readers already familiar with class field theory should note that we give a different definition of modulus here than one would find in the literature, since our definition of modulus does not allow the modulus to "contain" the so-called infinite primes.) The following theorem gives an upper bound for the conductor.

Theorem 6.3. *Let F/E be a finite abelian extension of number fields. Let Δ be the discriminant of F/E. Let $\mathfrak{f}$ be the conductor of the extension. Then*

$$\mathfrak{f} \mid \gcd(\Delta, [F:E] \cdot \Big(\prod_{p \mid [F:E]} p \Big) \prod_{\mathfrak{p} \mid \Delta} \mathfrak{p}),$$

where the first product runs over all primes of $\mathbb{Z}$ which divide $[F:E]$ and the second product runs over all primes $\mathfrak{p}$ of E which divide Δ.

We will prove Theorem 6.3 in the next section, assuming the well-known fact that $\mathfrak{f}$ divides Δ (see [11, Chapter 5, §3, Theorem 3.27]).

The following corollary gives an upper-bound of the 2-part of the conductor in a special case.

Corollary 6.4. *Let $n \in \mathbb{Z}_{>0}$, let $L/\mathbb{Q}(\sqrt[n]{2})$ be an abelian extension of degree 8, let $\mathfrak{f}$ be the conductor of $L/\mathbb{Q}(\sqrt[n]{2})$, and let $m \in \mathbb{Z}_{\geq 0}$ be such that $\sqrt[n]{2}^m \parallel \mathfrak{f}$. Then we have $m \leq 4n+1$.*

Corollary 6.4 follows directly from Theorem 6.3. Indeed by Theorem 6.3 we have $(\sqrt[n]{2})^m \mid 8 \cdot 2 \cdot (\sqrt[n]{2}) = (\sqrt[n]{2})^{4n+1}$ where $m = \operatorname{ord}_{(\sqrt[n]{2})}(\mathfrak{f})$.

An example: primes of the form $x^2 + 23y^2$

To illustrate how one can apply class field theory we will prove that we can write a prime p as $p = x^2 + 23y^2$ with $x, y \in \mathbb{Z}$ if and only if $x^3 - x + 1$ has three zeros in $\mathbb{F}_p$ or $p = 23$ (for more examples see [1]).

The statement above is clear for $p = 23$. For the remaining part of this section assume $p \neq 23$.

Let L be the splitting field of the polynomial $f = x^3 - x + 1$. The polynomial f has no zeros in $\mathbb{F}_2$, hence f is irreducible over $\mathbb{Q}$. The discriminant of f is -23. Therefore $\sqrt{-23} \in L$. Hence $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the full symmetric group of degree 3. Let $F = \mathbb{Q}(\sqrt{-23})$. Now we show that the conductor of L/F is 1. The only primes that ramify in $L/\mathbb{Q}$ divide the discriminant of f, so only the prime $(\sqrt{-23})$ can ramify in L/F. Suppose for a contradiction that $(\sqrt{-23})$ ramifies in L/F. Then 23 is totally ramified in $L/\mathbb{Q}$, since $L/\mathbb{Q}$ is Galois. Hence the inertia group of 23 in L/F is $\mathrm{Gal}(L/\mathbb{Q})$. However by Proposition 5.8(v) and (vi) the inertia group of a tamely ramified prime is cyclic, hence we have a contradiction. Therefore no prime ramifies in the extension L/F.

By Theorem 6.3 the conductor of L/F is 1. Note that F cannot be embedded in the field of real numbers, so every element of F is totally positive. Now the Artin Reciprocity Law implies that all principal ideals of F are in the kernel of the (surjective) Artin map $I_F \to \mathrm{Gal}(L/F)$. Let Cl_F be the class group of F. The class number of F is 3. Hence the Artin map induces a isomorphism from Cl_F to $\mathrm{Gal}(L/F)$. This isomorphism implies that the Frobenius symbol of every principal ideal in F in the extension L/F is trivial. Therefore every principal prime ideal of F splits completely in L. Let $p \in \mathbb{Z}$ be a prime number. Then p splits in F completely into principal ideals if and only if p splits completely in L. Proposition 5.8(iii) implies: p splits completely in L if and only if f has three zeros in $\mathbb{F}_p$. Hence p splits in principal ideals in F if and only if f has three zeros in $\mathbb{F}_p$.

Let $\alpha = (1 + \sqrt{-23})/2$ and $\overline{\alpha} = (1 - \sqrt{-23})/2$. The ring of integers $\mathcal{O}_F$ is $\mathbb{Z}[\alpha]$. Suppose $p = x^2 + 23y^2$. Then (p) is the product of the principal ideals $(x + \sqrt{-23}y)$ and $(x - \sqrt{-23}y)$ of $\mathcal{O}_F$. Now suppose that p splits into principal ideals in $\mathcal{O}_F$. Then we have $p = (a + b\alpha)(a + b\overline{\alpha}) = a^2 + ab + 6b^2$. If b is odd, then p is divisible by 2. Since p is an odd prime, b is even. Therefore we get $a + b\alpha \in \mathbb{Z}[\sqrt{-23}]$, so p can be written in the form $x^2 + 23y^2$. Hence p can be written as $x^2 + 23y^2$ if and only if p splits into principal ideals in F.

Now we can conclude that p can be written as $x^2 + 23y^2$ if and only if f has three zeros in $\mathbb{F}_p$.

Estimating conductors

In this section we give a proof of Theorem 6.3 based on well-known theorems of local class field theory and Newton polygons.

Let F/E be an abelian extension of number fields. Let $\mathfrak{f}$ be the conductor of F/E and let Δ be the discriminant of F/E. A rough approximation of the conductor is given by the following theorem.

Theorem 6.5. *We have* $\mathfrak{f} \mid \Delta$.

Proof. See [14, Chapter VI, §3, Corollary 2] or [11, Chapter 5, §3, Theorem 3.27]. □

The next theorem we state enables us to calculate the conductor.

Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_E$ and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_F$ above $\mathfrak{p}$. Let $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ be the corresponding abelian extension of local fields. Let $\mathcal{O}_{E_{\mathfrak{p}}}$ be the ring of integers of $E_{\mathfrak{p}}$. For $i \in \mathbb{Z}_{>0}$ we define the multiplicative group U_i by $1 + \mathfrak{p}^i$ and we let $U_0 = \mathcal{O}^*_{E_{\mathfrak{p}}}$. Denote the norm map from $F^*_{\mathfrak{P}}$ to $E^*_{\mathfrak{p}}$ by $\mathrm{N}_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}$. Denote the subgroup $\mathrm{N}_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(F^*_{\mathfrak{P}})$ of $E^*_{\mathfrak{p}}$ by N, so

$$N = \mathrm{N}_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(F^*_{\mathfrak{P}}).$$

Theorem 6.6. *Let* $i \in \mathbb{Z}_{\geq 0}$ *be the smallest integer such that* $U_i \subset N$. *Then we have* $\mathfrak{p}^i \parallel \mathfrak{f}$.

Proof. See [14, Chapter XV, §2, Corollary 2]. □

In order to apply Theorem 6.6 efficiently we will use one of the main theorems of local class field theory.

Let G be the Galois group of F/E. Since F/E is abelian, Proposition 5.8(ii) implies that the decomposition group $G_{\mathfrak{P}}$ does not depend on the prime $\mathfrak{P}$ above $\mathfrak{p}$. Hence we can denote the decomposition group by $G_{\mathfrak{p}}$. Similarly we denote the ramification groups by $V_{\mathfrak{p},i}$. An element σ of the Galois group of $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ can be restricted to F. Since $E \subset E_{\mathfrak{p}}$, the element σ acts as the identity on E. Therefore we have a restriction map $r : \mathrm{Gal}(F_{\mathfrak{P}}/E_{\mathfrak{p}}) \to G$. This map is injective and the image of r is $G_{\mathfrak{p}}$ (see [14, Chapter II, §3, Corollary 4]). Hence we can identify $\mathrm{Gal}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$ with $G_{\mathfrak{p}}$.

Theorem 6.7. *We have a group isomorphism* $E^*_{\mathfrak{p}}/N \to G_{\mathfrak{p}}$ *that for* $n \in \{0, 1\}$ *maps* U_nN/N *bijectively to* $V_{\mathfrak{p},n}$.

Proof. For $n = 0$ see [14, Chapter IV, §3] and [14, Chapter XV, §2]. Suppose $n = 1$. Then U_1N/N is the Sylow p-subgroup of U_0N/N (see [7, Chapter 2, §3]). By Proposition 5.8(vi) the group $V_{\mathfrak{p},1}$ is a Sylow p-subgroup of $V_{\mathfrak{p},0}$. Hence for $n = 1$ the theorem also holds. □

Theorem 6.8. *The prime ideal* $\mathfrak{p}$ *is unramified in* F *if and only if* $\mathfrak{p} \nmid \mathfrak{f}$. *Suppose* $\mathfrak{p}$ *is ramified in* F. *Then* $\mathfrak{p}$ *is tamely ramified in* F *if and only if* $\mathfrak{p} \parallel \mathfrak{f}$.

Proof. Assume $\mathfrak{p}$ is unramified in F/E. Then Proposition 5.8(iv) implies that $V_{\mathfrak{p},0}$ is the trivial group. Hence the group isomorphism of Theorem 6.7 maps U_0N/N to the identity element of $G_{\mathfrak{p}}$. Therefore $U_0 \subset N$. Now Theorem 6.6 implies $\mathfrak{p} \nmid \mathfrak{f}$.

Assume $\mathfrak{p} \nmid \mathfrak{f}$. Then Theorem 6.6 implies $U_0 \subset N$. Therefore U_0N/N is the trivial group. By Theorem 6.7 the group $V_{\mathfrak{p},0}$ is trivial. Hence Proposition 5.8(iv) implies $\mathfrak{p}$ is unramified.

Assume $\mathfrak{p}$ is tamely ramified in F. Then Proposition 5.8(vi) implies that $V_{\mathfrak{p},1}$ is the trivial group. Hence the group isomorphism of Theorem 6.7 maps $U_1 N/N$ to the identity element of $G_{\mathfrak{p}}$. Therefore $U_1 \subset N$. Since $\mathfrak{p}$ is ramified, Proposition 5.8(iv) implies that $V_{\mathfrak{p},0}$ is a non-trivial group. From Theorem 6.7 we get that the group U_0 is not contained in N. Now Theorem 6.6 implies $\mathfrak{p} \parallel \mathfrak{f}$.

Assume $\mathfrak{p} \parallel \mathfrak{f}$. Then Theorem 6.6 implies $U_1 \subset N$. Therefore $U_1 N/N$ is the trivial group, so Theorem 6.7 implies that $V_{\mathfrak{p},1}$ is the trivial group. Now Proposition 5.8(vi) implies that $\mathfrak{p}$ is tamely ramified. □

Let $p \in \mathbb{Z}$ be the prime under $\mathfrak{p}$. Let $e = e(\mathfrak{p}/p) = \operatorname{ord}_{\mathfrak{p}}(p)$ be the ramification index of $\mathfrak{p}$ in $E/\mathbb{Q}$. Let $\lfloor \frac{e}{p-1} \rfloor \in \mathbb{Z}$ be such that $0 \leq \frac{e}{p-1} - \lfloor \frac{e}{p-1} \rfloor < 1$.

Lemma 6.9. *Let $i \in \mathbb{Z}_{\geq 0}$. If $i \geq \lfloor \frac{e}{p-1} \rfloor + 1$ then the map $U_i \to U_{i+e}$ defined by $x \mapsto x^p$ is a group isomorphism.*

Proof. Let $\mathcal{O} = \mathcal{O}_{E_{\mathfrak{p}}}$ be the ring of integers of $E_{\mathfrak{p}}$. Let $\pi \in \mathcal{O}$ be such that $(\pi) = \mathfrak{p}$. Note that $i \geq \lfloor \frac{e}{p-1} \rfloor + 1$ implies $i(p-1) \geq e+1$. Hence $p \cdot i \geq i+e+1$. Therefore $\pi^{i+e+1} \mid \pi^{ip}$. We will use this result in order to apply Hensel's Lemma.

Since $(p) = (\pi)^e$ and $\pi^{i+e+1} \mid \pi^{ip}$, the coefficients of the polynomial $(1 + \pi^i y)^p - 1 = p\pi^i y + \ldots + \pi^{p \cdot i} y^p \in \mathcal{O}[y]$ are elements of $(\pi)^{i+e} \cdot \mathcal{O}$. Hence for all $x \in U_i$ we have $x^p \in U_{i+e}$, so the map $\phi : x \mapsto x^p$ from U_i to U_{i+e} is well-defined.

To show that ϕ is a group isomorphism it suffices to prove that ϕ is a bijection. First we show that ϕ is surjective. Let $u \in U_{i+e}$. Then we see $g(y) = (1 + \pi^i y)^p - u \in (\pi)^{i+e} \cdot \mathcal{O}[y]$, so $f(y) = g(y)/\pi^{i+e} \in \mathcal{O}[y]$. Let $a \in \mathcal{O}$ be such that $u = 1 + p\pi^i a$. Since $\pi^{i+e+1} \mid \pi^{pi}$, we have $g(a) = \frac{1}{2}p(p-1)\pi^{2i}a^2 + \ldots + \pi^{pi}a^p \in \pi^{i+e+1} \cdot \mathcal{O}$. Hence we have $\pi | f(a)$. The derivative of $f(y)$ equals $f'(y) = p \cdot (1+\pi^i y)^{p-1} \cdot \pi^i \cdot \pi^{-i-e} \in (1+\pi^i y)^{p-1} \cdot \mathcal{O}^*$, so $\pi \nmid f'(a)$. Therefore Hensel's Lemma implies that there exists an element $\alpha \in \mathcal{O}$ such that $f(\alpha) = 0$. By definition of $f(y)$ we see that $g(y)$ also has a zero in $\mathcal{O}$. This proves that ϕ is surjective.

Let ζ_p be a primitive p-th root of unity. To show that ϕ is injective it suffices to prove that $\zeta_p \notin U_i$. From above we know $i(p-1) \geq e+1$. Hence we have $(\pi)^{i(p-1)} \nmid (\pi)^e = (p) = (1-\zeta_p)^{p-1}$. This implies $1 - \zeta_p \notin \pi^i \cdot \mathcal{O}$. Therefore we can conclude that $\zeta_p \notin U_i$. This finishes the proof of Lemma 6.9. □

Proof of Theorem 6.3. By Theorem 6.8 only primes $\mathfrak{p}$ that ramify in F/E can divide the conductor $\mathfrak{f}$ of F/E. We recall from Proposition 5.8(vi) that $V_{\mathfrak{p},1}$ is the p-part of the inertia group $V_{\mathfrak{p},0}$ in F/E. We define ϵ by $\epsilon = \epsilon(\mathfrak{p}) = \operatorname{ord}_p(\text{exponent of } V_{\mathfrak{p},1})$, where p is the prime of $\mathbb{Q}$ below $\mathfrak{p}$. Now we prove that

$$U_{\lfloor \frac{e}{p-1} \rfloor + 1 + e\epsilon} = U_{\lfloor \frac{e}{p-1} \rfloor + 1}^{p^\epsilon} \subset U_1^{p^\epsilon} \subset N$$

hold (see just above Theorem 6.6 for the definition of N). The equality follows from applying Lemma 6.9 precisely ϵ times starting with $i = \lfloor \frac{e}{p-1} \rfloor + 1$. The first inclusion follows from $U_{\lfloor \frac{e}{p-1} \rfloor + 1} \subset U_1$. Now we prove the second inclusion.

By definition of ϵ we have that p^ϵ annihilates $V_{\mathfrak{p},1}$. Hence by Theorem 6.7 the integer p^ϵ annihilates U_1N/N. Therefore we have $U_1^{p^\epsilon} \subset N$.

From Theorem 6.6 we get $\mathrm{ord}_\mathfrak{p}(\mathfrak{f}) \leq \lfloor \frac{e}{p-1} \rfloor + 1 + e\epsilon$. Hence together with Theorem 6.5 we have

$$\mathfrak{f} \mid \gcd(\Delta, \prod_{\mathfrak{p}|\Delta} \mathfrak{p}^{\lfloor \frac{e(\mathfrak{p})}{p-1} \rfloor + 1 + e(\mathfrak{p})\epsilon(\mathfrak{p})}).$$

Now we prove that this result implies Theorem 6.3.

Assume that $\mathfrak{p}$ is wildly ramified. Then $\mathfrak{p} \mid \Delta$ implies $\mathfrak{p} \mid [F:E]$. Hence we have

$$\prod_{\mathfrak{p}|\Delta} \mathfrak{p}^{\lfloor \frac{e(\mathfrak{p})}{p-1} \rfloor} \Big| \prod_{p|[F:E]} \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p})} \Big| \prod_{p|[F:E]} p.$$

Let $m(p)$ be the maximum of the set $\{\epsilon(\mathfrak{p}) : \mathfrak{p} \mid p\}$. The order of $V_{\mathfrak{p},1}$ divides the order of G, so

$$m(p) \leq \mathrm{ord}_p([F:E]).$$

Hence we have

$$\prod_{\mathfrak{p}|\Delta} \mathfrak{p}^{\epsilon(\mathfrak{p})e(\mathfrak{p})} \Big| \prod_{p|[F:E]} \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p})\epsilon(\mathfrak{p})} \Big| \prod_{p|[F:E]} (\prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p})})^{m(p)} \Big| \prod_{p|[F:E]} p^{m(p)} \mid [F:E].$$

Theorem 6.8 implies $\mathfrak{f}$ divides $\prod_{p|[F:E]} p \cdot \prod_{\mathfrak{p}|\Delta} \mathfrak{p} \cdot [F:E]$. □

Chapter 7

Periodicity

In this chapter we combine the results of the previous chapters to prove the main theorem of this thesis, that is: for a fixed well-chosen value $s \in K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ the Lehmer symbol $\epsilon(s, p)$ is "periodic in the variable p".

Main theorem for rational starting values

The first example of a starting value for which the Lehmer symbol $\epsilon(s, p)$ is periodic in p is given by the following theorem of S.Y. Gebre-Egziabher.

Theorem 7.1. *Let $p \in \mathbb{Z}_{>2}$ and let $M = 2^p - 1$ be prime. Then*

$$\epsilon(2/3, p) = 1 \Leftrightarrow p \equiv 1 \bmod 4 \quad \textit{and} \quad p \neq 5.$$

This theorem of Gebre-Egziabher follows almost immediately from Theorem 7.2 below. For this theorem we recall that $P(s)$ is the set of $p \in \mathbb{Z}_{>2}$ such that $2^p - 1$ is prime and s is a starting value for p (see just before Definition 5.2). Let $s \in \mathbb{Q}$ and write $s = \frac{c_s}{d_s}$ with $c_s, d_s \in \mathbb{Z}$ and $\gcd(c_s, d_s) = 1$. Let $r_s = \prod_{q | d_s} q$ where the product is taken over all prime numbers $q \neq 2$ that divide d_s. Define w_s to be the multiplicative order of $(2 \bmod r_s)$ in $(\mathbb{Z}/r_s\mathbb{Z})^*$.

Theorem 7.2. *Let $s \in \mathbb{Q}$ such that $4 - s^2$ is a square in $\mathbb{Q}(\sqrt{2})^*$. Then for all $p, q \in P(s)$ we have*

$$\epsilon(s, p) = \epsilon(s, q) \textit{ if } p, q \geq 13 \textit{ and } p \equiv q \bmod (2 \cdot w_s).$$

To see how Theorem 7.2 implies Theorem 7.1, take $s = \frac{2}{3}$. Then

$$4 - s^2 = 32/9 = (4\sqrt{2}/3)^2,$$

so Theorem 7.2 applies to $s = \frac{2}{3}$. We have $r_s = 3$ and $w_s = 2$. Hence by Theorem 7.2 above for all $p, q \in P(s)$ such that $p, q \geq 13$ we have $\epsilon(s, p) = \epsilon(s, q)$ if $p \equiv q$ mod 4. After we calculate $\epsilon(2/3, p)$ for $p = 3, 5, 7, 13, 19$, Theorem 7.1 follows.

Another example that illustrates Theorem 7.2, is the following corollary. Recall the definition of bad prime of Chapter 2.

Corollary 7.3. *Let $s = \frac{626}{363}$. Then s is a universal starting value with the set of bad primes equal to $\{2\}$. Furthermore we have*

$$\epsilon(s,p) = 1 \textit{ if and only if } p \equiv 1, 7, 9 \textit{ or } 13 \bmod 20.$$

Proof. Let $s = \frac{626}{363}$. The elements $s-2 = 10^2 \cdot 11^{-2} \cdot -3^{-1}$ and $-s-2 = (2\sqrt{2} \cdot 13)^2 \cdot 11^{-2} \cdot -3^{-1}$ equal -3 in the multiplicative group $\mathbb{Q}(\sqrt{2})^*/\mathbb{Q}(\sqrt{2})^{*^2}$. For $u = 3, 5, 11$ and 13 the order of $(2 \bmod p)$ is even, so for odd $q \in \mathbb{Z}_{>1}$ we have $s-2, -s-2 \in (\mathbb{Z}/M_q\mathbb{Z})^*$. Hence for each odd $q \in \mathbb{Z}_{>1}$ the Jacobi symbols $\left(\frac{s-2}{M_q}\right)$ and $\left(\frac{-s-2}{M_q}\right)$ equal $\left(\frac{-3}{M_q}\right) = 1$. Therefore s is a universal starting value with bad prime 2. The element $4 - s^2 = 2^5 \cdot 5^2 \cdot 13^2 \cdot 3^{-2} \cdot 11^{-4}$ is a square in the multiplicative group $\mathbb{Q}(\sqrt{2})^*$. The denominator d_s equals $363 = 3 \cdot 11^2$, so $r_s = 33$. The order w_s of $(2 \bmod 33)$ in $(\mathbb{Z}/r_s\mathbb{Z})^*$ is 10. Hence by Theorem 7.2 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 13$ and $p \equiv q \bmod 20$. After we calculate $\epsilon(\frac{626}{363}, p)$ for $p = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 2203$ the above corollary follows. □

Main theorem

To state the main theorem concisely we first define periodicity for Lehmer symbols. Let $s \in K$. In Chapter 5 we defined the map

$$\epsilon_s : P(s) \to \{\pm 1\}$$

by $p \mapsto \epsilon(s,p)$.

Definition 7.4. *We call a function ϵ defined on a set P of prime numbers periodic if there exist positive integers l, m such that for all $p, q \in P$ we have*

$$\epsilon(p) = \epsilon(q) \textit{ if } p, q \geq l \textit{ and } p \equiv q \bmod m.$$

For example if we take $s = \frac{2}{3}$ and apply Theorem 7.1 then we see that ϵ_s is periodic, since we can set $l = 6$ and $m = 4$.

Let $K_s = K \cap \mathbb{Q}(s, \sqrt{2}, \sqrt{s-2}, \sqrt{-s-2})$ (by Proposition 4.4 this definition agrees with the definition of K_s in Chapter 4). Let $\mathcal{O}_s = \mathcal{O}_{K_s}$ be the ring of integers of K_s, let $\mathfrak{d}_s = \{x \in \mathcal{O}_s : \ x \cdot s \in \mathcal{O}_s\}$ and let $n = [K_s : \mathbb{Q}]$, so that $K_s = \mathbb{Q}(\sqrt[n]{2})$. Let $\mathfrak{r}_s$ be the ideal $\prod_{\mathfrak{p}|\mathfrak{d}_s} \mathfrak{p}$ of $\mathcal{O}_s$ where the product is taken over all prime ideals $\mathfrak{p} \neq (\sqrt[n]{2})$ of $\mathcal{O}_s$ that divide $\mathfrak{d}_s$. Define $\omega_s = \mathrm{ord}(\sqrt[n]{2} \bmod \mathfrak{r}_s)$ to be the multiplicative order of the element $(\sqrt[n]{2} \bmod \mathfrak{r}_s)$ in $(\mathcal{O}_s/\mathfrak{r}_s)^*$.

Theorem 7.5. *Let $s \in K$ be such that $4 - s^2$ is a square in K^*. Then ϵ_s is periodic. Furthermore we can take $l = 4 \cdot n + 1$ and $m = \omega_s$ in Definition 7.4.*

For a proof of Theorem 7.5 see the next section of this chapter.

In the remainder of this section we give some corollaries of the main theorem. Recall the definition of bad prime of Chapter 2.

Corollary 7.6. *Let $s = -\frac{14}{75} + \frac{32}{25}\sqrt{2}$. Then s is a universal starting value with the set of bad primes equal to $\{2\}$. Furthermore we have*

$$\epsilon(s,p) = -1 \textit{ if and only if } p \neq 3, 5.$$

Proof. Note that $-3\cdot(s-2) = (\frac{6}{5} - \frac{8}{5}\sqrt{2})^2$ and $-3\cdot(-s-2) = (\frac{8}{5} + \frac{6}{5}\sqrt{2})^2$. Hence s is a universal starting value with bad prime 2 and in the group $K^*/{K^*}^2$ the identity $4 - s^2 = -3\cdot(s-2)\cdot -3\cdot(-s-2) = 1$ holds. By Theorem 7.5 we conclude that ϵ_s is periodic. Next we calculate l and m. From the identities for $-3\cdot(s-2)$ and $-3\cdot(-s-2)$ it follows that $K_s = \mathbb{Q}(\sqrt{2})$. This yields $n = [K_s : \mathbb{Q}] = 2$, the ideal $\mathfrak{d}_s$ equals (75) and the ideal $\mathfrak{r}_s$ equals (15). The order of $(\sqrt{2} \bmod (15))$ in $(\mathbb{Z}[\sqrt{2}]/(15))^*$ equals 8. We conclude that we can set $l = 4\cdot n + 1 = 9$ and $m = \omega_s = 8$. Hence by Theorem 7.5 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 9$ and $p \equiv q \bmod 8$. After we calculate $\epsilon(s,p)$ for $p = 3, 5, 7, 13, 17, 19, 31$ the above corollary follows. □

Corollary 7.7. *Let $s = \frac{238}{507} + \frac{160}{169}\sqrt{2}$. Then s is a universal starting value with the set of bad primes equal to $\{2\}$. Furthermore we have*

$$\epsilon(s,p) = 1 \textit{ if and only if } p \equiv 5 \bmod 6 \textit{ and } p \neq 5.$$

Proof. Note that $-3\cdot(s-2) = (-\frac{24}{13} + \frac{10}{13}\sqrt{2})^2$ and $-3\cdot(-s-2) = (\frac{10}{13} + \frac{24}{13}\sqrt{2})^2$. Hence s is a universal starting value with bad prime 2 and in the group $K^*/{K^*}^2$ the identity $4 - s^2 = -3\cdot(s-2)\cdot -3\cdot(-s-2) = 1$ holds. By Theorem 7.5 we conclude that ϵ_s is periodic. Next we calculate l and m. From the identities for $-3\cdot(s-2)$ and $-3\cdot(-s-2)$ it follows that $K_s = \mathbb{Q}(\sqrt{2})$. This yields $n = [K_s : \mathbb{Q}] = 2$, the ideal $\mathfrak{d}_s$ equals (507) and the ideal $\mathfrak{r}_s$ equals (39). The order of $(\sqrt{2} \bmod (39))$ in $(\mathbb{Z}[\sqrt{2}]/(39))^*$ equals 24. We conclude that we can set $l = 4\cdot n + 1 = 9$ and $m = \omega_s = 24$. Hence by Theorem 7.5 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 9$ and $p \equiv q \bmod 24$. After we calculate $\epsilon(s,p)$ for $p = 3, 5, 7, 13, 17, 19, 31, 107, 2281, 4253, 756839$ the above corollary follows. □

Corollary 7.8. *Let $s = \frac{118}{49} - \frac{800}{147}\sqrt[4]{2} - \frac{96}{49}\sqrt[4]{2}^2 + \frac{704}{147}\sqrt[4]{2}^3$. Then s is a universal starting value with the set of bad primes equal to $\{2, 3\}$. Furthermore we have*

$$\epsilon(s,p) = 1 \textit{ if and only if } p \equiv 5, 7 \bmod 12.$$

Proof. Note that $-3\cdot(s-2) = (\frac{18}{7} + \frac{8}{7}\sqrt[4]{2} - \frac{8}{7}\sqrt[4]{2}^2 - \frac{16}{7}\sqrt[4]{2}^3)^2$ and $-3\cdot(-s-2) = (-\frac{16}{7} + \frac{16}{7}\sqrt[4]{2} + \frac{18}{7}\sqrt[4]{2}^2 - \frac{4}{7}\sqrt[4]{2}^3)^2$. Hence s is a universal starting value with bad primes 2 and 3, and in the group $K^*/{K^*}^2$ the identity $4 - s^2 = -3\cdot(s-2)\cdot -3\cdot(-s-2) = 1$ holds. By Theorem 7.5 we conclude that ϵ_s is periodic. Next we calculate l and m. From the identities for $-3\cdot(s-2)$ and $-3\cdot(-s-2)$ it follows that $K_s = \mathbb{Q}(\sqrt[4]{2})$. This yields $n = [K_s : \mathbb{Q}] = 4$, the ideal $\mathfrak{d}_s$ divides (147) and the ideal $\mathfrak{r}_s$ divides (21). The order of $(\sqrt[4]{2} \bmod (21))$ in $(\mathbb{Z}[\sqrt[4]{2}]/(21))^*$ equals 24. We conclude that we can set $l = 4\cdot n + 1 = 17$ and $m = \omega_s = 24$. Hence by Theorem 7.5 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 17$ and $p \equiv q \bmod 24$. After we calculate $\epsilon(s,p)$ for $p = 5, 7, 13, 17, 19, 31, 61, 107, 2281, 4253, 756839$ the above corollary follows. □

Proof of the main theorem

We recall the notation of Chapters 4 and 5. Let $s \in K$ be a potential starting value, let $\alpha \in \overline{\mathbb{Q}}$ be a zero of $f_s = x^{16} - sx^8 + 1$, let L_s be the splitting field of f_s over $\mathbb{Q}(s)$ and let $n \in \mathbb{Z}_{>0}$ be such that $K_s = L_s \cap K = \mathbb{Q}(\sqrt[n]{2})$. Let $L'_s = K_s(\sqrt{4-s^2}, \alpha + \alpha^{-1})$ (by Proposition 4.1 the field L'_s is well-defined and Galois over K_s) and let G'_s be the Galois group of L'_s over K_s.

Lemma 7.9. *Let $s \in K$. Suppose $4 - s^2$ is a square in K^*. Then $4 - s^2$ is a square in K_s^*.*

Proof. Clearly $\sqrt{4-s^2} \in K^*$ and by Proposition 4.1 we have $\sqrt{4-s^2} \in L_s$, so $\sqrt{4-s^2} \in K^* \cap L_s = K_s^*$. Hence $4 - s^2$ is a square in K_s^*. □

Proof of Theorem 7.5. If $P(s) \subset \{2\}$ then the theorem follows immediately. Suppose $P(s) \not\subset \{2\}$. Then $P(s)$ contains an odd prime. By Theorem 3.2 the value s is a potential starting value. Lemma 7.9 yields $4 - s^2 \in (K_s^*)^2$. Hence K'_s, defined by $K'_s = K_s(\sqrt{4-s^2})$, equals the field K_s, so by Proposition 4.3 the group G'_s is cyclic of order 8.

Next we describe a modulus for L'_s/K_s. Let $\mathfrak{f}$ be the conductor of L'_s/K_s. Write $\mathfrak{f}$ as the product $(\sqrt[n]{2})^i \cdot \mathfrak{f}_{\text{odd}}$ where $i \in \mathbb{Z}_{\geq 0}$ and $\mathfrak{f}_{\text{odd}}$ is not divisible by the prime $(\sqrt[n]{2})$. By Proposition 5.9 we know that all primes $\neq (\sqrt[n]{2})$ that ramify in L'_s/K_s divide $\mathfrak{d}_s$ and hence $\mathfrak{r}_s$. By Theorem 6.3 and $[L'_s : K_s] = 8$, the ideal $\mathfrak{f}_{\text{odd}}$ equals the product of the primes $\neq (\sqrt[n]{2})$ that ramify in L'_s/K_s. Hence $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{r}_s$. By Corollary 6.4 we have $i \leq 4n + 1$. Hence $\mathfrak{m} = (\sqrt[n]{2})^{4n+1} \cdot \mathfrak{r}_s$ is a modulus for L'_s/K_s.

Suppose $p, q \in P(s)$ satisfy $p \equiv q \bmod \omega_s$ and $p, q \geq 4n+1$. Let $m_p = \sqrt[n]{2}^p - 1$ and let $m_q = \sqrt[n]{2}^q - 1$. By definition ω_s is the order of $\sqrt[n]{2}$ in $(\mathcal{O}_s/\mathfrak{r}_s)^*$, so $p \equiv q \bmod \omega_s$ implies $m_p \equiv m_q \bmod \mathfrak{r}_s$. The assumption $p, q \geq 4n + 1$ implies $m_p \equiv m_q \bmod (\sqrt[n]{2})^{4n+1}$. Hence we have $m_p \equiv m_q \bmod \mathfrak{m}$. Let $x = m_p \cdot m_q^{-1}$. The ideal $\mathfrak{m}$ is a modulus for L'_s/K_s, so $\operatorname{ord}_{\mathfrak{p}}(x-1) \geq \operatorname{ord}_{\mathfrak{p}}(\mathfrak{f})$ for all prime ideals $\mathfrak{p} \mid \mathfrak{f}$. The field K_s has two real embeddings, namely σ defined by $\sigma(\sqrt[n]{2}) = \sqrt[n]{2}$ and τ defined by $\tau(\sqrt[n]{2}) = -\sqrt[n]{2}$. Since both p and q are odd, we see that $\sigma(x) > 0$ and $\tau(x) > 0$, i.e. x is totally positive in L'_s/K_s. Now conditions (i) and (ii) of Theorem 6.1 are satisfied, therefore we conclude that the ideal (x) is in the kernel of the Artin map. Hence $((x), L'_s/K_s)$ is the trivial element of G'_s, so $((m_p), L'_s/K_s) = ((m_q), L'_s/K_s)$. By Corollary 5.7 it follows that $\epsilon_s(p) = \epsilon_s(q)$. □

Proof of Theorem 7.2. Let $s \in \mathbb{Q}$ be such that $4 - s^2$ is a square in $\mathbb{Q}(\sqrt{2})^*$. By Proposition 4.4 we have $n = [K_s : \mathbb{Q}(s)] = 2$. From Theorem 7.5 it follows that ϵ_s is periodic. Since $s \in \mathbb{Q}$, we have $\mathfrak{d}_s = (d_s)$, the ideal $\mathfrak{r}_s$ equals (r_s) and hence ω_s divides $2 \cdot w_s$. Hence we can take $l \geq 4 \cdot 2 + 1 = 9$ and $m = \omega_s = 2 \cdot w_s$. Since $p, q \in P(s)$ and $p, q \geq 9$ imply $p, q \geq 13$, we set $l = 13$. □

Chapter 8

Composing auxiliary fields

In this chapter we construct for certain pairs of potential starting values a Galois extension by composing two auxiliary fields of Chapter 4. We also relate certain elements of this Galois extension to a sign (see Theorem 8.10 below).

Potential starting values and Galois groups

In this section we define pairs of potential starting values for which we construct a Galois extension. Recall from Definition 3.1 the definition of a potential starting value.

Definition 8.1. *We call $s, t \in K$ a related pair of potential starting values if s is a potential starting value, neither $4 - s^2$ nor $4 - t^2$ is a square in K^*, and $(4-s^2)(4-t^2)$ and $(s+2)(t+2)$ are squares in K^* and $K(\sqrt{4-s^2})^*$ respectively.*

For example if we take $s = 4$ and $t = 10$, then s and t form a related pair of potential starting values. Indeed $(4 - 4^2) \cdot (4 - 10^2) = -12 \cdot -96 = (24\sqrt{2})^2$ and $(4 + 2)(10 + 2) = 2 \cdot 6^2$.

Proposition 8.2. *If $s, t \in K$ is a related pair of potential starting values, then both s and t are potential starting values.*

We prove this proposition in the last section of this chapter.

Let $s \in K$ be a potential starting value. We recall some notation of Chapter 4. Let $f_s = x^{16} - sx^8 + 1$, let $\alpha = \alpha_s \in \overline{\mathbb{Q}}$ be a zero of f_s and let L_s be the splitting field of f_s over $\mathbb{Q}(s)$. Let $K_s = L_s \cap K$ and let $L'_s = K_s(\sqrt{4-s^2}, \alpha_s + \alpha_s^{-1})$.

Let $t \in K$ be a potential starting value. Define $K_{s,t}$ by $K_{s,t} = (L_s L_t) \cap K$. The next proposition, which we prove in last section of this chapter, is useful for calculating the field $K_{s,t}$.

Proposition 8.3. *Let $s, t \in K$ be a related pair of potential starting values. Then we have $[K_{s,t} : \mathbb{Q}(s, t)] = 1, 2$ or 4.*

Define $F_s = K_{s,t}L'_s = K_{s,t}(\sqrt{4-s^2}, \alpha_s + \alpha_s^{-1})$. From Proposition 4.1 it follows that L'_s/K_s is Galois. Hence F_s over $K_{s,t}$ is Galois. In the last section of this chapter we prove the next proposition.

Proposition 8.4. *Let s, t be potential starting values. Then the restriction map from $\mathrm{Gal}(F_s/K_{s,t})$ to $\mathrm{Gal}(L'_s/K_s)$ is a group isomorphism.*

Define $F = F_{s,t}$ to be the compositum of F_s and F_t. Both F_s and F_t are Galois over $K_{s,t}$, so F is Galois over $K_{s,t}$. For a related pair of potential starting values $s, t \in K$ we will study the Galois group G of F over $K_{s,t}$. We prove the following lemma in the last section of this chapter.

Lemma 8.5. *Let $s, t \in K$ be a related pair of potential starting values. Then $(4-s^2)(4-t^2)$ and $(s+2)(t+2)$ are squares in $K^*_{s,t}$ and $K_{s,t}(\sqrt{4-s^2})^*$ respectively.*

Let $E = E_{s,t} = F_s \cap F_t$. Define $E' = E'_{s,t} = K_{s,t}(\sqrt{4-s^2}) = K_{s,t}(\sqrt{4-t^2})$; note that by Lemma 8.5 the last equality sign holds. By Definition 8.1 we have $[E' : K_{s,t}] = 2$. Define the subgroup H of G by $H = \mathrm{Gal}(F/E')$.

Proposition 8.6. *Let $s, t \in K$ be a related pair of potential starting values and let $n = [E : E']$. Then the exact sequence $1 \to H \to G \to \mathrm{Gal}(E'/K_{s,t}) \to 1$ splits, where the action of the non-trivial element of $\mathrm{Gal}(E'/K_{s,t})$ on H sends any group element to its inverse. Moreover H is isomorphic to the additive group $\{(a, b) \in (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) : a \equiv b \bmod n\}$, the commutator subgroup of G is H^2 and n equals 2, 4 or 8.*

Proposition 8.6 will be proved in the last section of this chapter.

Galois groups and signs

Let $s, t \in K$ be a related pair of potential starting values. Let F, E' and G be as above. By Lemma 8.5 we can define E'' by $E'' = E''_{s,t} = E'(\sqrt{s+2}) = E'(\sqrt{t+2})$. Later we prove $[E'' : E'] = 2$ (see Lemma 8.15). For convenience we give an overview of some fields defined so far. In the right diagram one can read (at the corresponding places) the definitions of the fields in the left diagram.

$$\begin{tikzcd}
 & F \arrow[dl, dash] \arrow[dr, dash] & \\
F_s \arrow[dr, dash] \arrow[ddd, dash, bend right, "C_8"'] & & F_t \arrow[dl, dash] \arrow[ddd, dash, bend left, "C_8"] \\
 & E \arrow[d, dash] & \\
 & E'' \arrow[d, dash] & \\
 & E' \arrow[d, dash, "C_2"] & \\
 & K_{s,t} &
\end{tikzcd}$$

$$\begin{tikzcd}
 & F_sF_t \arrow[dl, dash] \arrow[dr, dash] & \\
E'(\alpha_s + \alpha_s^{-1}) \arrow[dr, dash] & & E'(\alpha_t + \alpha_t^{-1}) \arrow[dl, dash] \\
 & F_s \cap F_t \arrow[d, dash] & \\
 & E'(\sqrt{s+2}) \arrow[d, dash] & \\
 & K_{s,t}(\sqrt{4-s^2}) \arrow[d, dash] & \\
 & K_{s,t} &
\end{tikzcd}$$

Let $\mathrm{Gal}(F/E')^{\mathrm{gen}}$ be the set of all elements of order 8 of $\mathrm{Gal}(F/E')$. Proposition 8.6 implies $\mathrm{Gal}(F/E')^{\mathrm{gen}} = \{\sigma \in \mathrm{Gal}(F/E') : \mathrm{ord}(\sigma|F_s) = \mathrm{ord}(\sigma|F_t) = 8\}$. Now we define the equivalence relation $\sim$ on G by $\sigma \sim \tau$ if σ is conjugate to τ in G. We denote the equivalence class of $\sigma \in G$ by $[\sigma]$. Since $\mathrm{Gal}(F/E')$ is a normal subgroup of G and conjugate elements have the same order, the set $\mathrm{Gal}(F/E')^{\mathrm{gen}}$ is a union of conjugacy classes. Recall from Chapter 4 the definition of the set $\mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim$. Note that K'_s is a subfield of E' and that $[K'_s : K_s]$ equals $[E' : K_{s,t}]$. Therefore by Proposition 8.4 we have a surjective restriction map $r_s : \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \,\to \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim$. Recall from Definition 4.6 the map $\lambda'_s : \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim \,\to \{\pm 1\}$.

Definition 8.7. *For $s, t \in K$ a related pair of potential starting values we define the map*

$$\lambda'_{s,t} : \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \,\to \{\pm 1\}$$

by: $\lambda'_{s,t}([\sigma])$ equals the product of $(\lambda'_s \circ r_s)([\sigma])$ and $(\lambda'_t \circ r_t)([\sigma])$.

Proposition 8.8. *The map $\lambda'_{s,t}$ is surjective if and only if $[E : E'] = 2$ or 4.*

We prove Proposition 8.8 in the last section of this chapter. Next we state when and how the map $\lambda'_{s,t}$ factors via the Galois group of an abelian extension of $K_{s,t}$.

Proposition 8.9. *Let $s, t \in K$ be a related pair of potential starting values. Then there exists an intermediate field T in the extension $F/K_{s,t}$ such that TE'' is the maximal abelian extension of $K_{s,t}$ in F and $T \cap E''$ equals $K_{s,t}$. Moreover for each such T we are in one of the following two cases:*

$$\begin{array}{ll} \text{(i)} & [T : K_{s,t}] = 1 \text{ and } [E : E'] = 8, \\ \text{(ii)} & [T : K_{s,t}] = 2 \text{ and } [E : E'] = 2 \text{ or } 4. \end{array}$$

We prove Proposition 8.9 in the last section of this chapter. Let $r_{s,t}$ be the restriction map $r_{s,t} : \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \,\to \mathrm{Gal}(T/K_{s,t})$. The following theorem will be proved in the last section of this chapter.

Theorem 8.10. *Let $s, t \in K$ be a related pair of potential starting values and let T be as in Proposition 8.9. Then there exists an injective map $\mu_{s,t}$: $\mathrm{Gal}(T/K_{s,t}) \to \{\pm 1\}$ together with a commutative diagram*

$$\begin{tikzcd}
\mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \arrow[d, "r_{s,t}"'] \arrow[dr, "\lambda'_{s,t}"] & \\
\mathrm{Gal}(T/K_{s,t}) \arrow[r, "\mu_{s,t}"'] & \{\pm 1\}
\end{tikzcd}$$

if and only if $[E : E']$ equals 4 or 8.

Proofs

In this section we prove the propositions, lemmas and theorems stated in this chapter.

Inspired by the definition of a potential starting value (see Definition 3.1) and Proposition 3.3 we give the following definition for a potential starting pair.

Definition 8.11. *We call $s, t \in K$ a potential starting pair if*

$$\mathrm{i} \notin K(\sqrt{s-2}, \sqrt{-s-2}, \sqrt{t-2}, \sqrt{-t-2}).$$

Proposition 8.12. *If $s, t \in K$ is a related pair of potential starting values then $s, t \in K$ is a potential starting pair.*

Proof. Suppose $s, t \in K$ is a related pair of potential starting values. By Definition 8.1 the element $(4-s^2)(4-t^2)$ is a square in K^*, so $K(\sqrt{4-s^2}) = K(\sqrt{4-t^2})$. Also by Definition 8.1 the element $(s+2)(t+2)$ is a square in $K(\sqrt{4-s^2})^*$, so $(-s-2)(-t-2)$ is a square in $K(\sqrt{4-s^2})^*$. Hence we have $K(\sqrt{4-s^2}, \sqrt{-s-2}) = K(\sqrt{4-t^2}, \sqrt{-t-2})$. Definition 8.1 yields that s is a potential starting value, so by Proposition 3.3 we have $\mathrm{i} \notin K(\sqrt{s-2}, \sqrt{-s-2}) = K(\sqrt{4-s^2}, \sqrt{-s-2})$. Therefore $\mathrm{i} \notin K(\sqrt{s-2}, \sqrt{-s-2}, \sqrt{t-2}, \sqrt{-t-2})$. By definition of potential starting pair the proposition follows. □

Proof of Proposition 8.2. Proposition 8.12 implies s, t is a potential starting pair. Definition 8.11 and Proposition 3.3 imply that both s and t are potential starting values. □

Proposition 8.13. *Let $s, t \in K$ be a potential starting pair. Then we have $[K_{s,t} : \mathbb{Q}(s,t)] = 1, 2$ or 4.*

Proof. Let $s, t \in K$ be a potential starting pair. Recall the definition of $\mathbb{Q}''_s$ and $\mathbb{Q}''_t$ in the last section of Chapter 4. We recall that L_s is the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}(s)$. Let $L = L_s L_t$ and $M = \mathbb{Q}''_s \mathbb{Q}''_t$. The definitions of $\mathbb{Q}''_s$ and $\mathbb{Q}''_t$ imply that $M/\mathbb{Q}(s,t)$ is Galois with $\mathrm{Gal}(M/\mathbb{Q}(s,t))$ abelian. By Corollary 3.6 we get $[M \cap K : \mathbb{Q}(s,t)] \leq 2$. Proposition 4.9 implies that L/M is Galois with $\mathrm{Gal}(L/M)$ an abelian 2-group. Since s, t is a potential starting pair, we have $\mathrm{i} \notin MK$. Hence Proposition 3.7 implies $[L \cap K : M \cap K] \leq 2$. By definition one has $K_{s,t} = L \cap K$. Therefore we have $[K_{s,t} : \mathbb{Q}(s,t)] = 1, 2$ or 4. □

Proof of Proposition 8.3. Proposition 8.3 follows directly from Proposition 8.12 and Proposition 8.13. □

Proof of Proposition 8.4. We have a restriction map from $\mathrm{Gal}(F_s/K_{s,t})$ to $\mathrm{Gal}(L'_s/K_s)$. By the definitions of the fields K_s and $K_{s,t}$ it is clear that $K_{s,t}$ is an extension of K_s, the intersection $L'_s \cap K_{s,t}$ equals K_s and L'_s/K_s is Galois. Since $F_s = K_{s,t} L'_s$, the proposition follows from Theorem 3.12. □

For $n \in \mathbb{Z}_{>0}$ write C_n for a cyclic group of order n.

Lemma 8.14. *Let H be a finite abelian group. Let the non-trivial element of C_2 act on H by sending an element of G to its inverse. Then the commutator subgroup of $C_2 \ltimes H$ is H^2.*

Proof. Define $G = C_2 \ltimes H$. Let c be the non-trivial element of C_2 and let $h \in H$. The identity $chc^{-1}h^{-1} = h^{-2}$ implies $H^2 \subset [G, G]$.

Clearly H is a normal subgroup of G. Note that H^2 is a characteristic subgroup of H, i.e. every automorphism of H leaves H^2 invariant. Hence H^2 is a normal subgroup of G. The group $G/H^2 = C_2 \ltimes (H/H^2) = C_2 \times (H/H^2)$ is abelian, so $[G, G] \subset H^2$. Hence we have $[G, G] = H^2$. □

Proof of Lemma 8.5. From Definition 8.1 it follows that $\sqrt{(4-s^2)(4-t^2)} \in K^*$ and $\sqrt{(s+2)(t+2)} \in K(\sqrt{4-s^2})^*$. By Proposition 4.1 we have $\sqrt{4-s^2}$, $\sqrt{s+2} \in L_s$ and $\sqrt{4-t^2}, \sqrt{t+2} \in L_t$. This implies that both elements $\sqrt{(4-s^2)(4-t^2)}$ and $\sqrt{(s+2)(t+2)}$ lie in L_sL_t. Therefore we obtain that the element $\sqrt{(4-s^2)(4-t^2)}$ lies in $K^* \cap (L_sL_t) = K^*_{s,t}$ and that $\sqrt{(s+2)(t+2)}$ lies in $K(\sqrt{4-s^2}) \cap (L_sL_t) = K_{s,t}(\sqrt{4-s^2})^*$, so $(4-s^2)(4-t^2)$ and $(s+2)(t+2)$ are squares in $K_{s,t}(\sqrt{4-s^2})^*$ and $K^*_{s,t}$ respectively. □

Lemma 8.15. *Let $s, t \in K$ be a related pair of potential starting values. Then we have $[E'' : E'] = 2$.*

Proof. By Proposition 4.11 we have $[K'_s(\sqrt{s+2}) : K'_s] = 2$. Recall that $K'_s = K_s(\sqrt{4-s^2})$. Since $E' = K_{s,t}(\sqrt{4-s^2})$ and $E'' = K_{s,t}(\sqrt{4-s^2}, \sqrt{s+2})$, Proposition 8.4 implies $[E'' : E'] = 2$. □

Lemma 8.16. *Let $s, t \in K$ be a related pair of potential starting values. Then we have $[E : E'] = 2, 4$ or 8.*

Proof. The definition of related pair of potential starting values, the definition of E', the definition of E'' and Lemma 8.5 imply $E' \subset E'' \subset E \subset F_s$. By Proposition 4.2 we have $[F_s : E'] = 8$. Since $E' \neq E''$ (see Lemma 8.15), we have $[E : E'] = 2, 4$ or 8. □

Let $n \in \mathbb{Z}_{>0}$ with $n \mid 8$. Let $H'_n = \{(a, b) \in (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) : a \equiv b \bmod n\}$.

Proof of Proposition 8.6. By assumption $s, t \in K$ is a related pair of potential starting values. From the definition of related pair of potential starting values and Lemma 8.5 it follows that $[E' : K_{s,t}] = 2$ and $E' \subset E$. By Proposition 8.4 the restriction map $\mathrm{Gal}(F_s/K_{s,t}) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism. Now Proposition 4.3 implies $\mathrm{Gal}(F_s/E')$ is isomorphic to C_8. Hence by Proposition 3.13 the group H is isomorphic to H'_n where $n = [E : E']$. (In the case $n \neq 2$ choose two elements $\sigma \in \mathrm{Gal}(F_s/E')$ and $\tau \in \mathrm{Gal}(F_t/E')$ of order 8 such that $\sigma|_E = \tau|_E$ and send (σ, τ) to $(1, 1)$.)

By Proposition 4.3 it follows that $\mathrm{Gal}(F_s/K_{s,t})$ is isomorphic to the group $\mathrm{Gal}(F_s/E') \rtimes \mathrm{Gal}(E'/K_{s,t})$ where the non-trivial element of $\mathrm{Gal}(E'/K_{s,t})$ acts as -1 on $\mathrm{Gal}(F_s/E')$. This result we also get for t, namely $\mathrm{Gal}(F_t/K_{s,t})$ is isomorphic to $\mathrm{Gal}(F_t/E') \rtimes \mathrm{Gal}(E'/K_{s,t})$ where the non-trivial element of $\mathrm{Gal}(E'/K_{s,t})$

acts as -1 on $\mathrm{Gal}(F_t/E')$. By Proposition 3.13 the group $G = \mathrm{Gal}(F/K_{s,t})$ is isomorphic to $\mathrm{Gal}(F_s/K_{s,t}) \times_{\mathrm{Gal}(E/K_{s,t})} \mathrm{Gal}(F_t/K_{s,t})$. Let σ be any element of G such that $\sigma|E'$ is the non-trivial element of $\mathrm{Gal}(E'/K_{s,t})$. Since $\mathrm{Gal}(F_s/K_{s,t})$ is a dihedral group, the order of $\sigma|F_s$ equals two (same for t). Hence the order of $(\sigma|F_s, \sigma|F_t) \in \mathrm{Gal}(F_s/K_{s,t}) \times_{\mathrm{Gal}(E/K_{s,t})} \mathrm{Gal}(F_t/K_{s,t})$ equals 2. By the isomorphism above the order of σ equals two. Therefore the exact sequence $1 \to \mathrm{Gal}(F/E') \to G \to \mathrm{Gal}(E'/K_{s,t}) \to 1$ splits. Since $\mathrm{Gal}(F_s/K_{s,t})$ is a dihedral group, the action of $\sigma|E'$ on $\mathrm{Gal}(F_s/E')$ sends a group element to its inverse. We get a similar result for t. By the isomorphism above the action of $\sigma|E'$ on $\mathrm{Gal}(F/E')$ sends a group element to its inverse. By Lemma 8.14 it follows that $[G,G]$ is H^2. From Lemma 8.16 we get $[E : E'] = 2, 4$ or 8. □

Lemma 8.17. *Let $s, t \in K$ be a related pair of potential starting values and let $[\sigma] \in \mathrm{Gal}(F/E')^{\mathrm{gen}}/\!\sim$. Then $\lambda'_{s,t}([\sigma])$ equals $\lambda'_{s,t}([\sigma^i])$ for any odd $i \in \mathbb{Z}$.*

Proof. By definition $\mathrm{Gal}(F/E')^{\mathrm{gen}}$ is the set of elements of order 8 of $\mathrm{Gal}(F/E')$. Hence for $i \equiv 1$ or $7 \bmod 8$ Proposition 8.6 implies $[\sigma] = [\sigma^i]$. Therefore in the case $i \equiv 1$ or $7 \bmod 8$ Lemma 8.17 holds.

Let $i \equiv 3$ or $5 \bmod 8$. Recall the map r_s of the previous section. Also recall the map λ'_s of Definition 4.6. The definition of λ'_s and Proposition 4.5 imply $(\lambda'_s \circ r_s)([\sigma]) = -(\lambda'_s \circ r_s)([\sigma^i])$. We get a similar result for t. Hence the product of $(\lambda'_s \circ r_s)([\sigma])$ and $(\lambda'_t \circ r_t)([\sigma])$ equals the product of $(\lambda'_s \circ r_s)([\sigma^i])$ and $(\lambda'_t \circ r_t)([\sigma^i])$. By definition of $\lambda'_{s,t}$ Lemma 8.17 follows. □

Proof of Proposition 8.8. From Lemma 8.16 we get $[E : E'] = 2, 4$ or 8. Suppose $[E : E'] = 8$. Then Proposition 8.6 implies that the group $\mathrm{Gal}(F/E')$ is isomorphic to C_8 and hence $\mathrm{Gal}(F/E')^{\mathrm{gen}}$ equals $\{[\sigma], [\sigma^3]\}$ where σ is a generator of $\mathrm{Gal}(F/E')$. Now Lemma 8.17 implies $\lambda'_{s,t}$ is constant.

Suppose $[E : E'] = 2$ or 4. Then by Proposition 8.6 there exist $\sigma, \tau \in \mathrm{Gal}(F/E')^{\mathrm{gen}}$ such that $\sigma|F_s = \tau|F_s$ and $\sigma|F_t = (\tau|F_t)^{[E:E']+1}$. Clearly we have $(\lambda'_s \circ r_s)([\sigma]) = (\lambda'_s \circ r_s)([\tau])$. By definition of λ'_t and Proposition 4.5 we have $(\lambda'_t \circ r_t)([\sigma]) = -(\lambda'_t \circ r_t)([\tau])$. Now the definition of $\lambda'_{s,t}$ implies $\lambda'_{s,t}([\sigma]) \neq \lambda'_{s,t}([\tau])$. Hence $\lambda'_{s,t}$ is surjective. □

Proposition 8.18. *Let s, t be a related pair of potential starting values. Let $G = \mathrm{Gal}(F/K_{s,t})$. Let $[G,G]$ be the commutator subgroup of G. Then $G/[G,G]$ is isomorphic to $C_2 \times C_2 \times C_2$ if $[E : E']$ equals 2 or 4. Moreover $G/[G,G]$ is isomorphic to $C_2 \times C_2$ if $[E : E']$ equals 8.*

Proof. By Proposition 8.6 the group $G/[G,G]$ is isomorphic to $(H/H^2) \rtimes C_2$, where H is isomorphic to $C_8 \times_{C_{[E:E']}} C_8$. Lemma 8.16 yields $[E : E'] = 2, 4$ or 8. Suppose $[E : E'] = 4$ or 2. Then H/H^2 is isomorphic to $C_2 \times C_2$, so $G/[G,G]$ is isomorphic to $C_2 \times C_2 \times C_2$. Suppose $[E : E'] = 8$. Then H/H^2 is isomorphic to C_2, so $G/[G,G]$ is isomorphic to $C_2 \times C_2$. □

Proof of Proposition 8.9. Let D be the maximal abelian extension of $K_{s,t}$ in F. Then $\mathrm{Gal}(D/K_{s,t})$ is isomorphic to $G/[G,G]$. We will use the structure of $G/[G,G]$ to prove Proposition 8.9. The definition of E'' implies that E'' is a subfield of D and that $\mathrm{Gal}(E''/K_{s,t})$ is isomorphic to $C_2 \times C_2$. Lemma 8.16 yields $[E : E'] = 2, 4$ or 8. Suppose $[E : E'] = 8$. Proposition 8.18 implies that $G/[G, G]$ is isomorphic to $C_2 \times C_2$. Therefore we can take $T = K_{s,t}$ in Proposition 8.9.

Suppose $[E : E'] = 4$ or 2. Proposition 8.18 implies that $G/[G, G]$ is isomorphic to $C_2 \times C_2 \times C_2$. Hence there exist four different quadratic extensions T of $K_{s,t}$ such that $E'' \cap T = K_{s,t}$ and $TE'' = D$. □

Lemma 8.19. *Let $s, t \in K$ be a related pair of potential starting values. Then the restriction map $r_{s,t} : \mathrm{Gal}(F/E')^{\mathrm{gen}}/{\sim} \to \mathrm{Gal}(T/K_{s,t})$ is surjective.*

Proof. Suppose for a contradiction that $r_{s,t}$ is not surjective. Then we have $T \neq K_{s,t}$, so Proposition 8.9 implies $[T : K_{s,t}] = 2$ and $T \cap E'' = K_{s,t}$. Hence the restriction map $\mathrm{Gal}(F/E'') \to \mathrm{Gal}(T/K_{s,t})$ is surjective. Recall that $H = \mathrm{Gal}(F/E')$. The Galois group $\mathrm{Gal}(F/E'')$ is $H[4] = \{x \in H : x^4 = 1\}$, so the restriction map $H[4] \to \mathrm{Gal}(T/K_{s,t})$ is surjective. Since $[E'' : E'] = 2$, the index $(H : H[4])$ equals 2. Let $g \in \mathrm{Gal}(F/E')^{\mathrm{gen}}$, so that g has order 8. Then we have $\mathrm{Gal}(F/E')^{\mathrm{gen}} = gH[4]$. Since the map $H[4] \to \mathrm{Gal}(T/K_{s,t})$ is surjective, the map $gH[4] \to \mathrm{Gal}(T/K_{s,t})$ is surjective as well. Therefore $r_{s,t}$ is surjective. □

Lemma 8.20. *Let $s, t \in K$ be a related pair of potential starting values and let $n = [E : E']$. Then $\mathrm{Gal}(F/E')$ has precisely $8/n$ cyclic subgroups of order 8.*

Proof. Lemma 8.16 implies $n = 2, 4$ or 8. Let $H = \mathrm{Gal}(F/E')$. From Proposition 8.6 we get H is isomorphic to $C_8 \times_{C_n} C_8$. Hence H has $32/n$ elements of order 8. Every cyclic group of order 8 has precisely 4 elements of order 8. Therefore H has precisely $(32/n)/4$ cyclic subgroups of order 8. Since $(32/n)/4$ equals $8/n$, Lemma 8.20 follows. □

Let $s, t \in K$ be a related pair of potential starting values, let $[E : E'] = 2$ or 4 and let D be the maximal abelian extension in $F/K_{s,t}$. Then Proposition 8.9 implies that $\mathrm{Gal}(D/E')$ is isomorphic to $C_2 \times C_2$. Hence there are three quadratic extension of E' which are subfields of D. Two of these quadratic extensions are E'' and TE'. We define T' to be the remaining quadratic extension of E'. For convenience we give the following diagram.

$$\begin{tikzcd}
& & D = TE'' \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
& TE' \arrow[dl, dash] \arrow[dr, dash] & T' \arrow[d, dash] & E'' \arrow[dl, dash] \\
T \arrow[dr, dash] & & E' \arrow[dl, dash] & \\
& K_{s,t} = T \cap E' & &
\end{tikzcd}$$

Lemma 8.21. *Let $s, t \in K$ be a related pair of potential starting values. Let $\sigma \in \mathrm{Gal}(F/E')^{\mathrm{gen}}$, let T be as in Proposition 8.9 and let $[E : E'] = 2$ or 4. Then the fixed field of $\langle\sigma\rangle$ contains either TE' or T'.*

Proof. The definition of $\mathrm{Gal}(F/E')^{\mathrm{gen}}$ implies that σ acts trivially on E' and non-trivially on E''. Hence either σ acts trivially on TE' or σ acts trivially on T'. Therefore Lemma 8.21 follows. □

We recall the restriction map $r_{s,t} : \mathrm{Gal}(F/E')^{\mathrm{gen}}/{\sim} \to \mathrm{Gal}(T/K_{s,t})$. Let $r = r_{s,t}$.

Corollary 8.22. *Let $s, t \in K$ be a related pair of potential starting values. Let $\sigma \in \mathrm{Gal}(F/E')^{\mathrm{gen}}$. Then $r([\sigma])$ equals $r([\sigma^i])$ for any odd $i \in \mathbb{Z}$.*

Proof. By definition all elements in $\mathrm{Gal}(F/E')^{gen}$ have order 8, so $\langle\sigma\rangle = \langle\sigma^i\rangle$ for any odd $i \in \mathbb{Z}$. By Proposition 8.9 the order of $\mathrm{Gal}(T/K_{s,t})$ equals 1 or 2. Hence Corollary 8.22 follows. □

Proof of Theorem 8.10. Lemma 8.16 implies $[E : E'] = 2, 4$ or 8. Suppose $[E : E'] = 8$. Then Proposition 8.8 implies that $\lambda'_{s,t}$ is not surjective. From Proposition 8.9 we get $\mathrm{Gal}(T/K_{s,t})$ has precisely one element. Therefore there exists a map $\mu_{s,t}$ such that the diagram in Theorem 8.10 commutes.

Suppose $[E : E'] = 4$ and let $\sigma, \tau \in \mathrm{Gal}(F/E')^{\mathrm{gen}}$. Then by Lemma 8.20 the group $\mathrm{Gal}(F/E')$ has precisely two cyclic subgroups of order 8. By Proposition 8.8 the map $\lambda'_{s,t}$ is surjective. Now Lemma 8.17 yields: $\lambda'_{s,t}([\sigma]) = \lambda'_{s,t}([\tau]) \iff \langle\sigma\rangle = \langle\tau\rangle$. By Lemma 8.19 the map $r : \mathrm{Gal}(F/E')^{\mathrm{gen}}/{\sim} \to \mathrm{Gal}(T/K_{s,t})$ is surjective. Corollary 8.22 implies $r([\sigma]) = r([\sigma^i])$ for any odd $i \in \mathbb{Z}$. Since $\mathrm{Gal}(F/E')$ has precisely two cyclic subgroups of order 8, we get: $r([\sigma]) = r([\tau]) \iff \langle\sigma\rangle = \langle\tau\rangle$. Hence we have: $r([\sigma]) = r([\tau]) \iff \lambda'_{s,t}([\sigma]) = \lambda'_{s,t}([\tau])$. Hence there exists a map $\mu_{s,t}$ such that the diagram in Theorem 8.10 commutes.

Suppose $[E : E'] = 2$. Then Proposition 8.6 implies that $\mathrm{Gal}(F/E')$ is isomorphic to $\{(a, b) \in (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) : a \equiv b \bmod 2\}$. Hence there exist $\sigma, \tau \in \mathrm{Gal}(F/E')^{\mathrm{gen}}$ such that $\sigma|F_s = \tau|F_s$ and $\sigma|F_t = (\tau|F_t)^7$. By definition of λ'_t and Proposition 4.5 we have $(\lambda'_t \circ r_t)([\sigma]) = (\lambda'_t \circ r_t)([\tau])$. The equation $\sigma|F_s = \tau|F_s$ implies $(\lambda'_s \circ r_s)([\sigma]) = (\lambda'_s \circ r_s)([\tau])$. Hence by definition of $\lambda'_{s,t}$ we have $\lambda'_{s,t}([\sigma]) = \lambda'_{s,t}([\tau])$. To prove Theorem 8.10, it suffices to show that $r([\sigma]) \neq r([\tau])$. The equation $\sigma|F_t = (\tau|F_t)^7$ implies that $(\sigma|F_t)^2 \neq (\tau|F_t)^2$ and $(\sigma|F_t)^4 = (\tau|F_t)^4$. Therefore $\langle\sigma\rangle \cap \langle\tau\rangle$ has precisely 2 elements, so the order of $\langle\sigma, \tau\rangle$ is 32. Hence we have $\mathrm{Gal}(F/E') = \langle\sigma, \tau\rangle$. From Lemma 8.21 we get that the fixed field of $\langle\sigma\rangle$ contains either TE' or T'. We get the same result for τ. Since $\mathrm{Gal}(F/E') = \langle\sigma, \tau\rangle$, we have: the fixed field of $\langle\sigma\rangle$ contains TE' if and only if the fixed field of $\langle\tau\rangle$ contains T'. Therefore $\sigma|_T \neq \tau|_T$, so we have $r([\sigma]) \neq r([\tau])$. Hence there does not exist a map $\mu_{s,t}$ such that the diagram in Theorem 8.10 commutes. □

Chapter 9

Relating Lehmer symbols

In this chapter we show that for certain well-chosen related pairs of potential starting values $s, t \in K$ (see Definition 8.1) the product of the corresponding Lehmer symbols $\epsilon(s,p)$ and $\epsilon(t,p)$ is "periodic in the variable p". Below we make this precise.

Woltman's conjecture

The following theorem, proved by S.Y. Gebre-Egziabher in 2000, was first stated in 1996 by G. Woltman as a conjecture (see [8, Chapter 2, §4]).

Theorem 9.1. *Let $p \in \mathbb{Z}_{>2}$ and suppose that $M = 2^p - 1$ is prime. Then*

$$\epsilon(4,p) \cdot \epsilon(10,p) = 1 \Leftrightarrow p \equiv 5 \textit{ or } 7 \bmod 8 \quad \textit{and} \quad p \neq 5.$$

A proof of Theorem 9.1 can be found at the end of this section.

In this chapter we generalize Theorem 9.1. To state this generalization concisely we will use the definition of periodic functions (see Definition 7.4). Let $s, t \in K$. In Chapter 5 we defined the map $\epsilon_s : P(s) \to \{\pm 1\}$ by $p \mapsto \epsilon(s,p)$. This map yields a map $\epsilon_{s,t} : P(s) \cap P(t) \to \{\pm 1\}$ defined by $p \mapsto \epsilon(s,p) \cdot \epsilon(t,p)$. For well-chosen values of s and t the map $\epsilon_{s,t}$ is periodic. If we take $s = 4$ and $t = 10$, and apply Theorem 9.1, then we see that $\epsilon_{s,t}$ is periodic, since we can take $l = 5$ and $m = 8$ (see Definition 7.4).

Next we state a first version of the main theorem of this chapter. First we recall some notation of Chapters 4 and 8. Let $s, t \in K$ be a related pair of potential starting values. Define L_s as the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}(s)$. Let $K_{s,t} = (L_s L_t) \cap K$, let $E' = K_{s,t}(\sqrt{4 - s^2})$, let $F_s = E'(\alpha_s + \alpha_s^{-1})$ and let $E = F_s \cap F_t$. Note that Lemma 8.16 implies $[E : E'] = 2, 4$ or 8.

Proposition 9.2. *Let s, t be a related pair of potential starting values. Then $\epsilon_{s,t}$ is periodic if $[E : E']$ equals 4 or 8. Moreover if $[E : E']$ equals 8, then $\epsilon_{s,t}$ is a constant function.*

We prove Proposition 9.2 in the last section of this chapter.

Suppose $[E : E'] = 8$. Then Proposition 9.2 implies that we can set $l = 0$ and $m = 1$ in Definition 7.4. Next we state a theorem on the possible values for l and m in Definition 7.4 in the case $[E : E'] = 4$.

Let $s, t \in K$ be a related pair of potential starting values. Let T be as in Proposition 8.9. Proposition 8.9 implies $[T : K_{s,t}] \leq 2$. Let $n = [K_{s,t} : \mathbb{Q}]$, so that $K_{s,t}$ equals $\mathbb{Q}(\sqrt[n]{2})$. Denote a modulus for $T/K_{s,t}$ by $\mathfrak{t}$. Write $\mathfrak{t}_{\text{odd}}$ for the odd part of $\mathfrak{t}$, i.e. $\mathfrak{t} = \mathfrak{t}_{\text{odd}} \cdot (\sqrt[n]{2})^i$ for some $i \in \mathbb{Z}_{\geq 0}$ and $(\sqrt[n]{2}) \nmid \mathfrak{t}_{\text{odd}}$. Let $\mathcal{O}_{K_{s,t}}$ be the ring of integers of $K_{s,t}$. Write ω for the order of $(\sqrt[n]{2} \bmod \mathfrak{t}_{\text{odd}})$ in $(\mathcal{O}_{K_{s,t}}/\mathfrak{t}_{\text{odd}})^*$.

Theorem 9.3. *Let $s, t \in K$ be a related pair of potential starting values. Suppose $[E : E'] = 4$ or 8. Then $\epsilon_{s,t}$ is periodic and we can set $l = 2n + 1$ and $m = \omega$ in Definition 7.4. Moreover we have $n \mid 4 \cdot [\mathbb{Q}(s, t) : \mathbb{Q}]$.*

For a proof of Theorem 9.3 see the last section of this chapter.

To verify if the conditions of Theorem 9.3 hold, one has to do some computations. Moreover to find a suitable m one also has to do computations. Next we state a corollary of Theorem 9.3 that makes these computations easier.

Let s, t be a related pair of potential starting values. Set $d = [\mathbb{Q}(s, t) : \mathbb{Q}]$. Let $\mathfrak{d}_s = \{x \in \mathbb{Z}[\sqrt[d]{2}] : x \cdot s \in \mathbb{Z}[\sqrt[d]{2}]\}$ be the denominator ideal of s. Similarly we define $\mathfrak{d}_t$. Let $\mathfrak{d} = \mathfrak{d}_{s,t} = \mathfrak{d}_s\mathfrak{d}_t$, which is an ideal of $\mathbb{Z}[\sqrt[d]{2}]$. Let $\mathfrak{e}$ be the product of all prime ideals $\mathfrak{p}$ of $\mathbb{Z}[\sqrt[d]{2}]$ for which $\text{ord}_{\mathfrak{p}}(4 - s^2)$ is odd. Let $\mathfrak{r} = \mathfrak{r}_{s,t}$ be the product of all prime ideals $\mathfrak{p} \neq (\sqrt[d]{2})$ of $\mathbb{Z}[\sqrt[d]{2}]$ which divide $\mathfrak{d}\mathfrak{e}$. Define $w_{s,t} = \text{ord}(\sqrt[d]{2} \bmod \mathfrak{r})$ to be the multiplicative order of $(\sqrt[d]{2} \bmod \mathfrak{r})$ in $(\mathbb{Z}[\sqrt[d]{2}]/\mathfrak{r})^*$.

Corollary 9.4. *Let $s, t \in K$ be a related pair of potential starting values. Suppose $(2 + \sqrt{2 + s})(2 + \sqrt{2 + t})$ is a square in $K(\sqrt{2 + s}, \sqrt{2 - s})^*$. Then $\epsilon_{s,t}$ is periodic and we can take $l = 8 \cdot d + 1$ and $m = 4 \cdot w_{s,t}$ in Definition 7.4. If in addition to the assumptions above*

$$\left(2 + \sqrt{2 + \sqrt{2 + s}}\right)\left(2 + \sqrt{2 + \sqrt{2 + t}}\right)$$

is a square in $K(\sqrt{2 + s}, \sqrt{2 - s}, \sqrt{2 + \sqrt{2 + s}})^*$, then $\epsilon_{s,t}$ is constant.

We prove Corollary 9.4 in the last section of this chapter.

Now we state two more examples of a periodic $\epsilon_{s,t}$. The starting values in these examples are universal starting values. Only the starting value in the first corollary has a bad prime (see just below Definition 2.5), which is 11.

Corollary 9.5. *Let $s = \frac{1108}{529}$ and let $t = \frac{5476}{529}$. Then both s and t are universal starting values, each with the set of bad primes equal to $\{11\}$. Furthermore for all $p \in P(s) \cap P(t)$ we have*

$$\epsilon(s, p) \cdot \epsilon(t, p) = 1 \textit{ if and only if } p \equiv 3, 4, 6, 9 \textit{ or } 10 \bmod 11.$$

Corollary 9.6. *Let $s = \frac{1492}{121}$ and let $t = \frac{1924}{121}$. Then both s and t are universal starting values with no bad primes. Furthermore for all $p \in P(s) \cap P(t)$ we have*

$$\epsilon(s, p) \cdot \epsilon(t, p) = -1.$$

In the last section of this chapter we prove these two corollaries.

Proof of Woltman's Conjecture. Let $s = 4$ and $t = 10$. We recall from the first section of Chapter 8 that s, t is a related pair of potential starting values. Note the following idenity

$$(2+\sqrt{2+4})(2+\sqrt{2+10}) = (\sqrt[4]{2}(1+\sqrt{2}+\sqrt{3}))^2 \in K(\sqrt{6},\sqrt{-2})^{*^2}.$$

Now Corollary 9.4 implies that $\epsilon_{s,t}$ is periodic. Clearly we have $d = 1$, $\mathfrak{d} = (1)$ and $\mathfrak{c} = (3)$. Therefore we have $\mathfrak{r} = 3$. The multiplicative order $w_{s,t}$ of $(2 \bmod \mathfrak{r})$ is 2. Hence by Corollary 9.4 we can set $l = 8 \cdot d + 1 = 9$ and $m = 4 \cdot w_{s,t} = 8$ in Definition 7.4. After calculating $\epsilon_{s,t}(p)$ for $p = 3, 5, 7, 13, 17, 19$ and 31 Theorem 9.1 follows. □

Relating Lehmer symbols via Frobenius symbols

In this section we relate a product of Lehmer symbols with a Frobenius symbol. We start with recalling (from Chapter 8) and defining the maps in the diagram below.

$$\begin{tikzcd}
P(s)\cap P(t) \arrow[r, "\mathrm{Frob}_1"] \arrow[rr, bend left, "\epsilon_{s,t}"] \arrow[dr, "\mathrm{Frob}_2"] \arrow[ddr, "\mathrm{Frob}_3"'] & \mathrm{Gal}(T/K_{s,t}) \arrow[r, dashed, "\mu_{s,t}"] & \{\pm1\} \\
& \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \arrow[u, "r_{s,t}"'] \arrow[ur, "\lambda'_{s,t}"] \arrow[d, "r"] & \\
& \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim \times \mathrm{Gal}(L'_t/K'_t)^{\mathrm{gen}}/\sim \arrow[uur, "\lambda'_s\times\lambda'_t"'] &
\end{tikzcd}$$

Let $s, t \in K$ be a related pair of potential starting values. By Proposition 8.2 both s and t are potential starting values. Recall the definition $\epsilon_{s,t}$ from the first section of this chapter. Let T be as in Proposition 8.9. The maps $r_{s,t}$, $\lambda'_{s,t}$ and $r_s : \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \to \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim$ are defined in the second section of Chapter 8. The map $\mu_{s,t}$ exists if and only if $[E : E'] = 4$ or 8 (see Theorem 8.10). We define the map r in the diagram above by $r : [\sigma] \mapsto (r_s([\sigma]), r_t([\sigma]))$. From Definition 4.6 of Chapter 4 we recall the map $\lambda'_s : \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim \to \{\pm1\}$. Define the map $\lambda'_s \times \lambda'_t$ in the diagram above by $\lambda'_s \times \lambda'_t : ([\sigma], [\tau]) \mapsto \lambda'_s([\sigma]) \cdot \lambda'_t([\tau])$. The following proposition will be used to define the maps Frob_1, Frob_2 and Frob_3.

Proposition 9.7. *Let $s, t \in K$, take $p \in P(s) \cap P(t)$ and set $n = [K_{s,t} : \mathbb{Q}]$. Then $(\sqrt[n]{2}^p - 1)$ is a prime ideal of $\mathcal{O}_{K_{s,T}}$ of degree one over $\mathbb{Q}$ unramified in F.*

We prove this proposition at the end of this section.

Next we define the three remaining maps in the diagram above, namely the Frobenius maps Frob_1, Frob_2 and Frob_3. Let $n = [K_{s,t} : \mathbb{Q}]$. We define the map Frob_1 by $\mathrm{Frob}_1 : p \mapsto ((\sqrt[n]{2}^p - 1), T/K_{s,t})$. Note that by Proposition 9.7 this map is well-defined.

Proposition 9.8. *Let $s, t \in K$ be a related pair of potential starting values and let $n = [K_{s,t} : \mathbb{Q}]$. Suppose $p \in P(s) \cap P(t)$. Then $((\sqrt[n]{2}^p - 1), F/K_{s,t})$ is an element of $\mathrm{Gal}(F/E')^{\mathrm{gen}}/\!\sim$.*

We prove Proposition 9.8 at the end of this section. Define the map Frob_2 by $\mathrm{Frob}_2 : p \mapsto ((\sqrt[n]{2}^p - 1), F/K_{s,t})$. Let $n_s = [K_s : \mathbb{Q}]$ and let $n_t = [K_t : \mathbb{Q}]$. Define the map Frob_3 by

$$\mathrm{Frob}_3 : p \mapsto (((\sqrt[n_s]{2}^p - 1), L'_s/K_s), ((\sqrt[n_t]{2}^p - 1), L'_t/K_t)).$$

Note that by Proposition 9.7 these two maps are well-defined.

Theorem 9.9. *Let $s, t \in K$ be a related pair of potential starting values. Then the diagram without $\mu_{s,t}$ above commutes. Moreover if $[E : E']$ equals 4 or 8, then the entire diagram exists and commutes.*

A proof of Theorem 9.9 can be found at the end of this section. The following corollary, which follows directly from Theorem 9.9, can be seen as an analog of Corollary 5.7.

Corollary 9.10. *Let $s, t \in K$ be a related pair of potential starting values. Then the diagram*

$$\begin{tikzcd}
P(s) \cap P(t) \arrow[rr, "\epsilon_{s,t}"] \arrow[drr, "\mathrm{Frob}_2"'] & & \{+1, -1\} \\
 & & \mathrm{Gal}(F/E')^{\mathrm{gen}}/\!\sim \arrow[u, "\lambda'_{s,t}"']
\end{tikzcd}$$

commutes.

To prove that ϵ_s is periodic if $[K'_s : K_s]$ equals 1, we used the fact that the Frobenius map in Corollary 5.7 becomes the Artin map if the Galois group $\mathrm{Gal}(L'_s/K_s)$ is abelian. We cannot apply this method to $\epsilon_{s,t}$ with Corollary 9.10, since the Galois group $\mathrm{Gal}(F/K_{s,t})$ is not abelian. However we can use the following corollary, which follows directly from Theorem 9.9, to prove that $\epsilon_{s,t}$ is periodic if $[E : E']$ equals 4 or 8.

Corollary 9.11. *Let $s, t \in K$ be a related pair of potential starting values. Suppose $[E : E']$ equals 4 or 8. Then the diagram*

$$\begin{tikzcd}
P(s) \cap P(t) \arrow[r, "\epsilon_{s,t}"] \arrow[dr, "\mathrm{Frob}_1"'] & \{+1, -1\} \\
 & \mathrm{Gal}(T/K_{s,t}) \arrow[u, "\mu_{s,t}"']
\end{tikzcd}$$

commutes.

Proof of Proposition 9.7. Let $p \in P(s) \cap P(t)$. Then Proposition 5.10(ii) implies $p \nmid [K_s : \mathbb{Q}]$ and $p \nmid [K_t : \mathbb{Q}]$. By Proposition 8.3 we have $[K_{s,t} : \mathbb{Q}(s,t)] \mid 4$. Since p is odd, the inclusions $\mathbb{Q}(s,t) \subset K_s K_t \subset K_{s,t}$ imply $p \nmid [K_{s,t} : \mathbb{Q}] = n$. Since $2 \mid n$, the absolute norm of $\sqrt[n]{2}^p - 1$ equals $-(2^p - 1)$. By definition of $P(s)$ the integer $2^p - 1$ is a prime number, so the ideal $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$ is a prime ideal of degree 1 over $\mathbb{Q}$.

By Proposition 5.10(ii) the prime ideal $\mathfrak{m}_p \cap K_s$ of K_s is unramified in L_s. This implies that $\mathfrak{m}_p$ is unramified in $L_s K_{s,t}$ (see [7, Chapter II, §4]). Similarly we derive that $\mathfrak{m}_p$ is unramified in $L_t K_{s,t}$. We recall $K_{s,t} = (L_s L_t) \cap K$, so $K_{s,t} \subset L_s L_t$. Hence $\mathfrak{m}_p$ is unramified in $F \subset L_s L_t$ (see [7, Chapter II, §4]). □

Proof of Proposition 9.8. Let $p \in P(s) \cap P(t)$ and let $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$. By Proposition 9.7 the ideal $\mathfrak{m}_p$ is a prime ideal of degree 1 over $\mathbb{Q}$. Let $\mathfrak{m}'_p = \mathfrak{m}_p \cap K_s$. The consistency property implies $(\mathfrak{m}_p, F_s/K_{s,t})|L_s = (\mathfrak{m}'_p, L_s/K_s)$. We recall the notation $K'_s = K_s(\sqrt{4 - s^2})$. Further we recall from Proposition 5.10(iv) that every element of the conjugacy class $(\mathfrak{m}'_p, L_s/'K_s)$ generates the group $\mathrm{Gal}(L'_s/K'_s)$. By Proposition 8.4 the restriction map $\mathrm{Gal}(F_s/K_{s,t}) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism. Since K'_s is a subfield of $E' = K_{s,t}(\sqrt{4 - s^2})$, the restriction map $\mathrm{Gal}(F_s/E') \to \mathrm{Gal}(L'_s/K'_s)$ is an isomorphism. Hence every element of the conjugacy class $(\mathfrak{m}_p, F_s/K_{s,t})$ generates the group $\mathrm{Gal}(F_s/E')$. Similarly for t we get: every element of the conjugacy class $(\mathfrak{m}_p, F_t/K_{s,t})$ generates the group $\mathrm{Gal}(F_t/E')$. Hence by Proposition 8.6 we have $(\mathfrak{m}_p, F/K_{s,t}) \in \mathrm{Gal}(F/E')^{\mathrm{gen}}/\!\sim$. □

Proof of Theorem 9.9. Suppose $s, t \in K$ is a related pair of potential starting values. Then the maps Frob_1, Frob_2, $\mu_{s,t}$, $\lambda'_{s,t}$ and $r_{s,t}$ are defined. By Proposition 8.2 both s and t are potential starting values. Hence also the maps Frob_3, r and $\lambda'_s \times \lambda'_t$ are defined. The identity $\lambda'_{s,t} = (\lambda'_s \times \lambda'_t) \circ r$ follows directly from the definition of $\lambda'_{s,t}$ (see Definition 8.7). The identities $\mathrm{Frob}_3 = r \circ \mathrm{Frob}_2$ and $\mathrm{Frob}_1 = r_{s,t} \circ \mathrm{Frob}_2$ follow from the consistency property (see Proposition 5.4). The identity $\epsilon_{s,t} = (\lambda'_s \times \lambda'_t) \circ \mathrm{Frob}_3$ follows from Corollary 5.7 and the definitions of the maps $\epsilon_{s,t}$ and $\lambda'_s \times \lambda'_t$. From the identities that we just proved we get

$$\epsilon_{s,t} = (\lambda'_s \times \lambda'_t) \circ \mathrm{Frob}_3 = (\lambda'_s \times \lambda'_t) \circ (r \circ \mathrm{Frob}_2) = ((\lambda'_s \times \lambda'_t) \circ r) \circ \mathrm{Frob}_2 = \lambda'_{s,t} \circ \mathrm{Frob}_2.$$

Hence $\epsilon_{s,t}$ equals $\lambda'_{s,t} \circ \mathrm{Frob}_2$. This proves the first part of Theorem 9.9. Now assume $[E : E'] = 4$ or 8. From Theorem 8.10 we get $\lambda'_{s,t} = \mu_{s,t} \circ r_{s,t}$. From the identities that we proved so far we get

$$\epsilon_{s,t} = \lambda'_{s,t} \circ \mathrm{Frob}_2 = (\mu_{s,t} \circ r_{s,t}) \circ \mathrm{Frob}_2 = \mu_{s,t} \circ (r_{s,t} \circ \mathrm{Frob}_2) = \mu_{s,t} \circ \mathrm{Frob}_1.$$

Hence $\epsilon_{s,t}$ equals $\mu_{s,t} \circ \mathrm{Frob}_1$. □

Proofs

In this section we prove Proposition 9.2, Theorem 9.3, Corollary 9.4, Corollary 9.5 and Corollary 9.6.

We recall some notation from the first section of Chapter 9. Let $s, t \in K$ be a related pair of potential starting values. Let T be as in Proposition 8.9. Let $n = [K_{s,t} : \mathbb{Q}]$. Denote a modulus for $T/K_{s,t}$ by $\mathfrak{t}$. Write $\mathfrak{t} = \mathfrak{t}_{\text{odd}} \cdot (\sqrt[n]{2})^i$ for some $i \in \mathbb{Z}_{\geq 0}$ and $(\sqrt[n]{2}) \nmid \mathfrak{t}_{\text{odd}}$. Let $\mathcal{O}_{K_{s,t}}$ be the ring of integers of $K_{s,t}$. Write ω for the order of $(\sqrt[n]{2} \bmod \mathfrak{t}_{\text{odd}})$ in $(\mathcal{O}_{K_{s,t}}/\mathfrak{t}_{\text{odd}})^*$.

Proof of Theorem 9.3. Let $\mathfrak{f}$ be the conductor of $T/K_{s,t}$. Write $\mathfrak{f}$ as the product $(\sqrt[n]{2})^j \cdot \mathfrak{f}_{\text{odd}}$ where $j \in \mathbb{Z}_{\geq 0}$ and $\mathfrak{f}_{\text{odd}}$ is not divisible by the prime $(\sqrt[n]{2})$. By Theorem 6.3 we have $(\sqrt[n]{2})^j \mid 2 \cdot 2 \cdot \sqrt[n]{2}$. Hence $\mathfrak{m} = (\sqrt[n]{2})^{2n+1} \cdot \mathfrak{f}_{\text{odd}}$ is a modulus for $T/K_{s,t}$.

Suppose $p, q \in P(s) \cap P(t)$ satisfy $p \equiv q \bmod \omega$ and $p, q \geq 2n + 1$. Let $m_p = \sqrt[n]{2}^p - 1$ and let $m_q = \sqrt[n]{2}^q - 1$. By definition ω is the order of $\sqrt[n]{2}$ in $(\mathcal{O}_{K_{s,t}}/\mathfrak{t}_{\text{odd}})^*$, so $p \equiv q \bmod \omega$ implies $m_p \equiv m_q \bmod \mathfrak{t}_{\text{odd}}$. Note that $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{t}_{\text{odd}}$, so $p \equiv q \bmod \omega$ implies $m_p \equiv m_q \bmod \mathfrak{f}_{\text{odd}}$. The assumption $p, q \geq 2n+1$ implies $m_p \equiv m_q \bmod (\sqrt[n]{2})^{2n+1}$. Hence we have $m_p \equiv m_q \bmod \mathfrak{m}$. Let $x = m_p \cdot m_q^{-1}$. The ideal $\mathfrak{m}$ is a modulus for T/K_s, so $\text{ord}_{\mathfrak{p}}(x - 1) \geq \text{ord}_{\mathfrak{p}}(\mathfrak{f})$ for all prime ideals $\mathfrak{p} \mid \mathfrak{f}$. The field $K_{s,t}$ has two real embeddings, namely σ defined by $\sigma(\sqrt[n]{2}) = \sqrt[n]{2}$ and τ defined by $\tau(\sqrt[n]{2}) = -\sqrt[n]{2}$. Since both p and q are odd, we see that $\sigma(x) > 0$ and $\tau(x) > 0$, i.e. the element x is totally positive in $T/K_{s,t}$. Now conditions (i) and (ii) of Theorem 6.1 are satisfied, therefore we conclude that the ideal (x) is in the kernel of the Artin map. Hence $((x), T/K_{s,t})$ is the trivial element of $\text{Gal}(T/K_{s,t})$, so $((m_p), T/K_{s,t})$ equals $((m_q), T/K_{s,t})$. Therefore the definition of Frob_1 implies $\text{Frob}_1(p) = \text{Frob}_1(q)$. Note that the assumptions of Theorem 9.3 are the same as the assumptions of Corollary 9.11. By Corollary 9.11 it follows that $\epsilon_{s,t}(p)$ equals $\epsilon_{s,t}(q)$. By Proposition 8.3 we have $n \leq 4 \cdot [\mathbb{Q}(s,t) : \mathbb{Q}]$. □

Proof of Proposition 9.2. The first part of Proposition 9.2 follows directly from Theorem 9.3. Since $[E : E'] = 8$, Proposition 8.8 implies that $\lambda'_{s,t}$ is not surjective. Hence from Corollary 9.10 the map $\epsilon_{s,t}$ is constant. □

Let $s, t \in K$ be a related pair of potential starting values. Recall $E' = K_{s,t}(\sqrt{4 - s^2})$ and $E'' = E'(\sqrt{2 + s})$. Define $e'' = (2 + \sqrt{2 + s})(2 + \sqrt{2 + t})$, $E''' = E''(\sqrt{2 + \sqrt{2 + s}})$ and

$$e = \left(2 + \sqrt{2 + \sqrt{2 + s}}\right)\left(2 + \sqrt{2 + \sqrt{2 + t}}\right).$$

Lemma 9.12. *Assume e'' is a square in $(E''K)^*$. Then e'' is a square in E''^*. Moreover if e'' and e are squares in $(E''K)^*$ and $(E'''K)^*$ respectively, then e is a square in E'''^*.*

Proof. By assumption e'' is a square in $(E''K)^*$. Proposition 4.11 implies that e'' is a square in $(L_sL_t)^*$. Hence e'' is a square in $(E''K)^* \cap (L_sL_t)^* = E''^*$. By assumption e is a square in $(E'''K)^*$. Proposition 4.11 implies that e is a square in $(L_sL_t)^*$. Hence e is a square in $(E'''K)^* \cap (L_sL_t)^* = E'''^*$. □

Lemma 9.13. *The element e'' is a square in E''^* if and only if $[E : E']$ equals 4 or 8. Moreover if e'' and e are squares in E''^* and E'''^* respectively, then $[E : E']$ equals 8.*

Proof. Lemma 8.16 implies $[E : E'] = 2, 4$ or 8. Suppose e'' is a square in E''^*. Then Proposition 4.11 implies $[E : E'] = 4$ or 8. If e is also a square in E'''^*, then Proposition 4.11 yields $[E : E'] = 8$. Suppose e'' is not a square in E''^*. Then Proposition 4.11 and Kummer theory imply $[E : E'] = 2$. □

Recall the definition of $\mathfrak{f}_{\text{odd}}$ (see proof of Theorem 9.3) and $\mathfrak{r}$ (see just above Corollary 9.4).

Proposition 9.14. *Let s, t be a pair of potential starting values. Then $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{r}$.*

Proof. Recall the definition of $\mathfrak{d}_s$, $\mathfrak{d}_t$ and $\mathfrak{e}$. Proposition 5.9 implies that if a prime ideal $\mathfrak{p} \neq (\sqrt[n]{2})$ of the ring of integers of $K_{s,t}$ ramifies in $K_{s,t}L_s$, then $\mathfrak{p}$ divides $\mathfrak{d}_s\mathfrak{e}$ (see [7, Chapter II, §5]). We get a similar result for $K_{s,t}L_t/K_{s,t}$. Hence if a prime ideal $\mathfrak{p} \neq (\sqrt[n]{2})$ of the ring of integers of $K_{s,t}$ ramifies in L_sL_t, then $\mathfrak{p}$ divides $\mathfrak{d}_s\mathfrak{d}_t\mathfrak{e} = \mathfrak{d}_{s,t}\mathfrak{e}$. From the definition of F we get $F \subset L_sL_t$. By Proposition 8.6 we have $[F : K_{s,t}] \mid 64$. Hence only the prime $(\sqrt[n]{2})$ is wildly ramified in $F/K_{s,t}$. Therefore Theorem 6.8 implies $\mathfrak{f}_{\text{odd}} \mid \mathfrak{r}$. □

Proof of Corollary 9.4. Let $s, t \in K$ be a related pair of potential starting values. Assume that $(2+\sqrt{2+s})(2+\sqrt{2+t})$ is a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$. Then Lemma 9.12 and Lemma 9.13 imply $[E : E'] = 4$ or 8. Hence Theorem 9.3 implies that $\epsilon_{s,t}$ is periodic. From Theorem 9.3 it follows that $l = 2n + 1 \leq 2 \cdot 4 \cdot [\mathbb{Q}(s,t) : \mathbb{Q}] + 1 = 8 \cdot d + 1$. By Proposition 9.14 the ideal $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{r}$. By Proposition 8.3 we have $n/d = 1, 2$ or 4. Therefore the multiplicative order of $(\sqrt[n]{2} \bmod \mathfrak{f}_{\text{odd}})$ divides four times the multiplicative order of $(\sqrt[d]{2} \bmod \mathfrak{r})$. Hence by Theorem 9.3 we can set $m = 4 \cdot w_{s,t}$. Suppose the extra assumption of Corollary 9.4 holds. Then Lemma 9.12 and Lemma 9.13 imply $[E : E'] = 8$. Hence by Proposition 9.2 the function $\epsilon_{s,t}$ is constant. □

Proof of Corollary 9.6. Taking the variable of Example 2.7 equal to $-\frac{2}{3}\sqrt{2}$ and $-\frac{1}{6}\sqrt{2}$ yields $s = \frac{1492}{121}$ and $t = \frac{1924}{121}$ respectively. Let α_s be a zero of $f_s = x^{16} - sx^8 + 1$. We recall $L_s = \mathbb{Q}(\zeta_8, \alpha_s)$ is the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}$. By equations 4.2 and 4.3 of the proof of Proposition 4.8 we can write $\alpha_s^4 = \frac{\sqrt{s-2}+\sqrt{s+2}}{2}$. From the two equalities below Example 2.7 it follows that $s - 2, t - 2 \in \mathbb{Q}(\sqrt{2})^{*^2}$ and $s + 2, t + 2 \in 3 \cdot \mathbb{Q}(\sqrt{2})^{*^2}$. Hence we have $\mathbb{Q}(\zeta_8, \alpha_s^4) = \mathbb{Q}(\zeta_8, \alpha_t^4)$. Note that in the field $\mathbb{Q}(\zeta_8, \alpha_s^4)$ we have

$$\alpha_s^4 \cdot \alpha_t^4 = \frac{1}{4}\Big(\frac{25}{11}\sqrt{2} + \frac{17}{11}\sqrt{6}\Big)\Big(\frac{29}{11}\sqrt{2} + \frac{19}{11}\sqrt{6}\Big) = 7 + 4\sqrt{3} = \Big(\frac{1}{\sqrt{2}}(1+\sqrt{3})\Big)^4.$$

Hence by Kummer theory the fields L_s and L_t are the same. By Theorem 5.6 it follows that $\epsilon_{s,t}$ is constant.

Next we show $\epsilon_{s,t}(p) = \epsilon(s,p) \cdot \epsilon(t,p) = -1$. Note that we have $s_{3-2} = s_1 = \frac{1492}{121} \equiv \frac{1}{2} \equiv -3 \equiv 2^{(3+1)/2} \bmod 7$, so $\epsilon_s(3)$ equals 1. Note that we have $t_{3-2} = t_1 = \frac{1924}{121} \equiv \frac{-1}{2} \equiv 3 \equiv -2^{(3+1)/2} \bmod 7$, so $\epsilon_t(3)$ equals -1. Hence $\epsilon_{s,t}(3)$ equals -1. Since $\epsilon_{s,t}$ is constant, we have $\epsilon_{s,t}(p) = \epsilon(s,p) \cdot \epsilon(t,p) = -1$. □

Let $s = \frac{1108}{529}$ and $t = \frac{5476}{529}$. The next table will be used in the proof of Corollary 9.5.

p	$\epsilon_s(p)$	$\epsilon_t(p)$	$\epsilon_{s,t}(p)$	p mod 11
3	+	+	+	3
5	+	−	−	5
7	−	+	−	7
13	−	+	−	2
17	−	−	+	6
19	−	+	−	8
31	−	−	+	9
61	−	−	+	6
89	+	−	−	1
107	+	−	−	8
127	−	−	+	6
521	+	+	+	4
607	−	+	−	2
1279	+	+	+	3
2203	−	−	+	3
2281	−	−	+	4
3217	−	+	−	5
4253	−	+	−	7
4423	−	+	−	1
9689	−	−	+	9
9941	+	−	−	8
11213	−	−	+	4
19937	−	+	−	5
21701	+	+	+	9
23209	−	−	+	10

Proof of Corollary 9.5. Taking the variable of Example 2.7 equal to $\frac{2}{7}\sqrt{2}$ and $-\frac{1}{8}\sqrt{2}$ yields $s = \frac{1108}{529}$ and $t = \frac{5476}{529}$ respectively. From the first equality below Example 2.7 it follows that both $s-2$ and $t-2$ are squares in $\mathbb{Q}(\sqrt{2})^*$. From the second equality below Example 2.7 it follows that both $-s-2$ and $-t-2$ can be written as -3 times a square of $\mathbb{Q}(\sqrt{2})^*$. Hence $K(\sqrt{2+s}, \sqrt{2-s})$ equals $K(\sqrt{3}, \sqrt{-1})$. Moreover neither $4-s^2$ nor $4-t^2$ is a square in K^*, and $(4-s^2)(4-t^2)$ and $(s+2)(t+2)$ are squares in K^* and $K(\sqrt{4-s^2})^*$ respectively. Definition 8.1 implies that s, t is a related pair of potential starting values.

Note the relation $(2+\sqrt{2+s})\cdot(2+\sqrt{2+t}) = \frac{1}{23^2}(46+19\sqrt{6})\cdot(46+33\sqrt{6}) = \frac{1}{23^2}\Big((2+\sqrt{6})(2\sqrt{2}+\sqrt{3})^2\Big)\cdot\Big((2+\sqrt{6})(5\sqrt{2}-\sqrt{3})^2\Big) \in K(\sqrt{3},\sqrt{-1})^{*^2}$. By Corollary 9.4 it follows that $\epsilon_{s,t}$ is periodic.

Next we calculate possible l and m as in Definition 7.4. In this and the next three paragraphs we show that $K_{s,t} = \mathbb{Q}(\sqrt{2})$. Recall that $L_s = \mathbb{Q}(\zeta_8, \alpha_s)$, $K_s = L_s \cap K$ and $K''_s = K_s(\sqrt{s-2}, \sqrt{-s-2})$. We want to apply Proposition 3.7 to the extensions $K_s \subset K''_s \subset L_s$. First we show that the assumptions of Proposition 3.7 hold. By Proposition 8.2 we get s is a potential starting value. Proposition 4.4 implies $K''_s = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and $K_s = \mathbb{Q}(\sqrt{2})$. From Proposition 4.2 we get $\mathrm{Gal}(L_s/K''_s)$ is cyclic of order 8. Clearly K''_s/K_s is Galois and $\mathrm{i} \in L_s$. Now Proposition 3.7 implies $L_s \cap K = K''_s \cap K = \mathbb{Q}(\sqrt{2})$. Hence we have $\sqrt[4]{2} \notin L_s$. Similarly we get $\sqrt[4]{2} \notin L_t$.

We recall $K'_s = K_s(\sqrt{4-s^2})$ and $L'_s = K'_s(\alpha_s + \alpha_s^{-1})$. Since $s-2 \in K_s^{*2}$, we have $K'_s = K''_s$. Proposition 4.2 implies $L_s = L'_s$. Similarly we have $L_t = L'_t$. Hence $K_{s,t}$ equals $(L'_sL'_t) \cap K$, so we have $F = L'_sL'_t$.

Suppose for a contradiction $L'_s = L'_t$. Then the fields $F_s = L'_sK_{s,t}$ and $F_t = L'_tK_{s,t}$ are equal. Now Proposition 9.2 implies that $\epsilon_{s,t}$ is constant. This contradicts the table above, so we conclude that $L'_s \neq L'_t$.

Proposition 4.11 and the relation $(2+\sqrt{2+s})\cdot(2+\sqrt{2+t}) \in K'_s(\sqrt{2+s})^{*^2} = K'_t(\sqrt{2+t})^{*^2}$ imply $[F : L'_s \cap L'_t] = 1$ or 4. From $L'_s \neq L'_t$ we get $[F : L'_s \cap L'_t] = 4$. Suppose for a contradiction that $\sqrt[4]{2} \in F$. Then the three intermediate fields of the extension $F/(L'_s \cap L'_t)$ are L'_s, L'_t and $(L'_s \cap L'_t)(\sqrt[4]{2})$. Therefore we have $L'_s(\sqrt[4]{2}) = F = L'_t(\sqrt[4]{2})$. The assumption $\sqrt[4]{2} \in F$ implies $\sqrt[4]{2} \in K_{s,t} = F \cap K$. By definition of F_s and F_t we have $\sqrt[4]{2} \in K_{s,t} \subset F_s$ and $\sqrt[4]{2} \in K_{s,t} \subset F_t$. Therefore we have $F_s = L'_s(\sqrt[4]{2})$ and $F_t = L'_t(\sqrt[4]{2})$, so $F_s = F = F_t$. Now Proposition 9.2 implies that $\epsilon_{s,t}$ is constant. This contradicts the table above, so we conclude that $\sqrt[4]{2} \notin F$. Hence we have $K_{s,t} = F \cap K = \mathbb{Q}(\sqrt{2})$.

By Theorem 9.3 we can set $l = 2 \cdot [K_{s,t} : \mathbb{Q}] + 1 = 5$. In the next three paragraphs we will calculate a possible m.

Recall the notation just above Corollary 9.4. Clearly we have $\mathfrak{d} = (529)^2 = (23)^4$ and $529^2 \cdot (4 - s^2) = 4 \cdot 529^2 - 1108^2 = -(2^2 \cdot 3 \cdot 5^2 \cdot 19^2)$. Therefore $\mathfrak{e}$ equals (3), so that $\mathfrak{r}$ equals $(3) \cdot (23)$.

Note that Lemma 9.13 implies $[E : E'] = 4$ or 8. The table above shows that $\epsilon_{s,t}$ is surjective. Hence by Proposition 9.2 the degree $[E : E']$ equals 4. By Proposition 8.9 and Proposition 8.18 there are 4 different extensions T such that $[T : K_{s,t}] = 2$, the intersection $T \cap E'' = K_{s,t}$ and $T \subset F$. We can choose two, T_1 and T_2, such that T_1T_2 contains the field $E' = K_{s,t}(\sqrt{4-s^2}) = K_{s,t}(\sqrt{-3})$.

$$\begin{tikzcd}
 & T_1T_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
T_1 \arrow[dr, dash] & T_2 \arrow[d, dash] & E' \arrow[dl, dash, "\text{(3) ramifies}"] \\
 & K_{s,t} &
\end{tikzcd}$$

Note that (3) is inert in the extension $K_{s,t}/\mathbb{Q}$. Since 3 does not divide

$[L_sL_t : \mathbb{Q}]$, Proposition 5.8(vi) implies that $V_{(3),1}$ is the trivial group. Hence by Proposition 5.8(v) the group $V_{(3),0}$ is cyclic. Note that the prime ideal (3) ramifies in $E'/K_{s,t}$. Since $V_{(3),0}$ is cyclic, the prime ideal (3) cannot ramify in both extensions $T_i/K_{s,t}$ with $i \in \{1, 2\}$. Hence we can choose a field T_i such that (3) does not divide the conductor of $T_i/K_{s,t}$. By Proposition 9.14 we have $\mathfrak{f}_{\mathrm{odd}} \mid \mathfrak{r}$. Since $\mathfrak{r}$ equals $3 \cdot 23$, we can conclude that $\mathfrak{f}_{\mathrm{odd}}$ divides 23. Therefore $\mathfrak{t} = (23)$ is a modulus for $T_i/K_{s,t}$. Note that $\sqrt{2}^{22} \equiv 1 \bmod 23$, so the order ω of $(\sqrt{2} \bmod 23)$ is 22. Now Theorem 9.3 (and the definition of m) implies $m \mid 22$. Since p is odd, we see that we can set $m = 11$.

The table above shows the signs for s and t. This proves Corollary 9.5. □

Chapter 10

Mersenne primes in arithmetic progressions

We know that there exist at least 47 Mersenne primes, and it is a conjecture that there are infinitely many. Dirichlet's theorem says for each $a, b \in \mathbb{Z}_{>0}$ with a and b relatively prime there are infinitely many primes p such that $p \equiv a \bmod b$ (see [11, Chapter 8, §7, Corollary 7.3]). Since there are no Mersenne primes that are 1 modulo 4, Dirichlet's theorem is not true if we replace primes by Mersenne primes. However for the exponents of Mersenne primes one might wonder if for each $a, b \in \mathbb{Z}_{>0}$ with a and b relatively prime there are infinitely many primes p with $p \equiv a \bmod b$ such that $2^p - 1$ is prime.

In this chapter we will speculate on Mersenne primes in arithmetic progression and reformulate these speculations in terms of Artin symbols (see Theorem 10.6 below). With this reformulation we prepare ourselves for the next chapter, where we will speculate on Frobenius symbols of Mersenne primes and generalise Theorem 10.6 (see Theorem 11.7 below).

Exponents in arithmetic progressions

Let $\mathcal{E}_{2012}$ be the set of currently known exponents p such that 2^p-1 is a Mersenne prime, i.e.

$$\begin{aligned}\mathcal{E}_{2012} \;=\; &\{2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,\\ &3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243,\\ &110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221,\\ &3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457,\\ &32582657, 37156667, 42643801, 43112609\}.\end{aligned}$$

In the table below we see the frequency of the last digit of $p \in \mathcal{E}_{2012} \backslash \{2, 5\}$.

i	1	3	7	9
$\#\{p \in \mathcal{E}_{2012} : p \equiv i \bmod 10\}$	11	11	14	9

The following table shows the frequency of $p \in \mathcal{E}_{2012} \backslash \{3\}$ in residue classes modulo 3.

i	1	2
$\#\{p \in \mathcal{E}_{2012} : p \equiv i \bmod 3\}$	23	23

The last table shows the frequency of $p \in \mathcal{E}_{2012} \backslash \{3, 5\}$ in residue classes modulo 15.

i	1	2	4	7	8	11	13	14
$\#\{p \in \mathcal{E}_{2012} : p \equiv i \bmod 15\}$	6	7	4	8	5	5	5	5

The distribution of the exponents over the different residue classes modulo 10, 3 and 15, make it reasonable to expect that for every $a, b \in \mathbb{Z}_{>0}$ with a and b relatively prime there are infinitely many exponents $p \equiv a \bmod b$ such that $2^p - 1$ is prime. In this chapter we will reformulate this expectation in two ways using Artin symbols.

Artin symbols of Mersenne primes

Let L be a finite abelian extension of $\mathbb{Q}$.

Definition 10.1. *We define* Mer_L *to be the set of all* $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ *such that there are infinitely many Mersenne primes* M *with* $\sigma = ((M), L/\mathbb{Q})$.

Examples. From Definition 10.1 it is clear that Mer_L is empty if and only if there are only finitely many Mersenne primes. We have $\mathrm{Mer}_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$ if there are infinitely Mersenne primes. Let $n \in \mathbb{Z}_{>0}$ and let ζ_{2^n} be a primitive 2^n-th root of unity. If there are infinitely many Mersenne primes then the set $\mathrm{Mer}_{\mathbb{Q}(\zeta_{2^n})}$ contains precisely the automorphism induced by complex conjugation.

Next we define the set $W_L \subset \mathrm{Gal}(L/\mathbb{Q})$, which one should think of as the smallest subset of $\mathrm{Gal}(L/\mathbb{Q})$ that we know that contains Mer_L. Let n_L be the conductor of $L/\mathbb{Q}$ and let $n_{L,\mathrm{odd}} \in \mathbb{Z}_{>0}$ be the largest odd integer that divides n_L. Denote by d_L the multiplicative order of $(2 \bmod n_{L,\mathrm{odd}})$ in the group $(\mathbb{Z}/n_{L,\mathrm{odd}}\mathbb{Z})^*$. In order to make the Artin symbols in the next definition well-defined, we note that from Lemma 10.9 we get: if $q \in \mathbb{Z}_{>0}$, $q \geq \mathrm{ord}_2(n_L)$ and $\gcd(q, d_L) = 1$ then $\gcd(2^q - 1, n_L) = 1$.

Definition 10.2. *We define* W_L *to be the set of all Artin symbols* $((2^q - 1), L/\mathbb{Q})$ *with* $q \in \mathbb{Z}_{>0}$, $q \geq \mathrm{ord}_2(n_L)$ *and* $\gcd(q, d_L) = 1$.

Proposition 10.3. *We have* $\mathrm{Mer}_L \subset W_L$.

We prove Proposition 10.3 in the last section of this chapter.

Examples. We have $W_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$. For $n \in \mathbb{Z}_{>0}$ let ζ_n be a primitive n-th root of unity. Then for $k \in \mathbb{Z}_{>0}$ the set $W_{\mathbb{Q}(\zeta_{2^k})}$ contains only the automorphism induced by complex conjugation.

Suppose $n = 2^{10} - 1$. Define $L = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Then one easily sees $n_L = (n)$, $d_L = 10$ and $W_L = \{\sigma_1, \sigma_7, \sigma_{127}, \sigma_{511}\}$, where $\sigma_i : \zeta_n + \zeta_n^{-1} \mapsto \zeta_n^i + \zeta_n^{-i}$. The table below is similar to the first table of this chapter, but from an Artin symbol point of view.

i	1	3	7	9
$\#\{p \in \mathcal{E}_{2012} : (2^p - 1, L/\mathbb{Q}) = \sigma_{2^i-1}\}$	11	11	14	9

There are $\varphi(2^{10} - 1) = 600$ different Artin symbols of non-ramified primes in $L/\mathbb{Q}$, but only four different Artin symbols come from Mersenne primes.

The following theorem, which we prove in the last section of this chapter, suggests that one may reasonably conjecture $\mathrm{Mer}_L = W_L$.

Theorem 10.4. *The following two statements are equivalent:*

(i) *For every $a, b \in \mathbb{Z}_{>0}$ relatively prime there are infinitely many integers $p \equiv a \bmod b$ such that $2^p - 1$ is a Mersenne prime.*

(ii) *For each finite abelian extension L of $\mathbb{Q}$ we have $\mathrm{Mer}_L = W_L$.*

Profinite groups

In this section we define the notion of a profinite group (and set and ring) and we will give some examples which will be applied in the next section.

A topological group G is a set together with a group structure and a topological structure such that the multiplication map $G \times G \to G$, defined by $(g_1, g_2) \mapsto g_1 g_2$, and inverse map $G \to G$, defined by $g \mapsto g^{-1}$, are continuous. A topological ring R is a set together with a ring structure and a topological structure such that the multiplication map $R \times R \to R$, defined by $(r_1, r_2) \mapsto r_1 r_2$, and addition map $R \times R \to R$, defined by $(r_1, r_2) \mapsto r_1 + r_2$, are continuous. Every finite group (or set or ring) is a topological group (or set or ring) if we give the finite group (or set or ring) the discrete topology.

Next we need the notion of a directed partially ordered set. This is a set I with a partial order $\geq$ such that for every $i, j \in I$ there is an element $k \in I$ such that $k \geq i$ and $k \geq j$.

Now we can define a projective system. Let I be a partially ordered set. A projective system of groups (or sets or rings) is a collection of groups (or sets or rings) G_i for $i \in I$ with a group (or set or ring) homomorphism $f_i^j : G_j \to G_i$ for all $i, j \in I$ with $j \geq i$ such that $f_i^j \circ f_j^k = f_i^k$ for $k \geq j \geq i$ and f_i^i is the identity on G_i.

A projective system has a projective limit, namely

$$G = \varprojlim_i G_i = \{(\alpha_i)_{i \in I} \in \prod_{i \in I} G_i : \text{for all } i, j \in I \text{ with } j \geq i \text{ we have } f_i^j(\alpha_j) = \alpha_i\}.$$

We put a topology on G: we give G_i the discrete topology, $\prod_{i \in I} G_i$ the product topology and $\varprojlim_i G_i$ the subspace topology. We call G a profinite group (or set or ring) if G is a topological group (or set or ring) which is isomorphic (as a topological group (or set or ring)) to a projective limit of finite groups (or sets or rings). For each $i \in I$ we have a projection map $G \to G_i$ such that for all $j \geq i$ the diagram

$$\begin{tikzcd}
 & G \arrow[dl] \arrow[dr] & \\
G_j \arrow[rr] & & G_i
\end{tikzcd}$$

commutes.

Next we describe two examples of projective limits that we use below. Let $\mathbb{N}$ be the set of positive integers, which we partially order by divisibility. The collection of rings $\mathbb{Z}/n\mathbb{Z}$ (with $n \in \mathbb{N}$) and the maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $(a \bmod n) \mapsto (a \bmod m)$ for $n, m \in \mathbb{N}$ with $m \mid n$, is a projective system. We denote the projective limit $\varprojlim_{n\in\mathbb{N}}(\mathbb{Z}/n\mathbb{Z})$ by $\hat{\mathbb{Z}}$. Let $\mathbb{Z}_2$ be the projective limit of the rings $(\mathbb{Z}/2^i\mathbb{Z})$, where i runs over the positive integers. Let $\mathbb{Z}_{\text{odd}}$ be the projective limit of the rings $(\mathbb{Z}/n_{\text{odd}}\mathbb{Z})$, where n_{odd} runs over the odd positive integers. Write $n \in \mathbb{Z}_{>0}$ as $2^i \cdot n_{\text{odd}}$, where $i \in \mathbb{Z}_{\geq 0}$ and n_{odd} is an odd positive integer. By the Chinese remainder theorem the map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/n_{\text{odd}}\mathbb{Z}$ defined by $(a \bmod n) \mapsto (a \bmod 2^i, a \bmod n_{\text{odd}})$ is a ring isomorphism. This isomorphism induces an isomorphism between the profinite rings $\hat{\mathbb{Z}}$ and $\mathbb{Z}_2 \times \mathbb{Z}_{\text{odd}}$. We denote the group of units of $\hat{\mathbb{Z}}$ by $\hat{\mathbb{Z}}^*$. Note that $\hat{\mathbb{Z}}^*$ is a profinite group.

We have an action of $\hat{\mathbb{Z}}^*$ on the set G as follows. For $i \in I$ and $x \in \hat{\mathbb{Z}}^*$ let $e_i(x) \in \mathbb{Z}$ be such that for $n = n(i)$, the order of G_i, we have $x_n = (e_i(x) \bmod n)$. For $g \in G$ and $x \in \hat{\mathbb{Z}}^*$ let $g^x = (g_i^{e_i(x)})$. This action $\hat{\mathbb{Z}}^* \times G \to G$ is continuous (see [19, Chapter 1, §5, Proposition 1.5.3]).

Let I be the set of finite abelian extensions of $\mathbb{Q}$ inside a chosen algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The collection of groups $\text{Gal}(L/\mathbb{Q})$ (with $L \in I$) and the restriction maps $\text{Gal}(L'/\mathbb{Q}) \to \text{Gal}(L/\mathbb{Q})$ for $L \subset L'$ is a projective system. We denote the projective limit $\varprojlim_{L\in I} \text{Gal}(L/\mathbb{Q})$ by $G_{\mathbb{Q}}^{\text{ab}}$.

The group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. Now from the Kronecker-Weber Theorem it follows that $G_{\mathbb{Q}}^{\text{ab}} = \varprojlim_{n\in\mathbb{Z}_{>0}} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \hat{\mathbb{Z}}^*$.

A profinite reformulation

In this section we will reformulate Theorem 10.4(ii) in terms of projective limits.

Proposition 10.5. *Let L, L' be finite abelian extensions of $\mathbb{Q}$. Suppose $L \subset L'$. Then the restriction map* $\text{Gal}(L'/\mathbb{Q}) \to \text{Gal}(L/\mathbb{Q})$ *induces surjective maps* $\text{Mer}_{L'} \to \text{Mer}_L$ *and* $W_{L'} \to W_L$.

Proposition 10.5 will be proved in the next section. Now we can define Mer_{ab} and W_{ab} to be the projective limit of all Mer_L and W_L respectively, where $L \subset \overline{\mathbb{Q}}$ runs over all finite abelian extensions of $\mathbb{Q}$. The inclusions $\text{Mer}_L \subset$

$W_L \subset \mathrm{Gal}(L/\mathbb{Q})$ yield the inclusions $\mathrm{Mer}_{\mathrm{ab}} \subset W_{\mathrm{ab}} \subset G_{\mathbb{Q}}^{\mathrm{ab}}$. Now we can extend Theorem 10.4.

Theorem 10.6. *The following three statements are equivalent:*

(i) *For every $a, b \in \mathbb{Z}_{>0}$ relatively prime there are infinitely many integers $p \equiv a \bmod b$ such that $2^p - 1$ is a Mersenne prime.*

(ii) *For each finite abelian extension L of $\mathbb{Q}$ we have $\mathrm{Mer}_L = W_L$.*

(iii) *We have $\mathrm{Mer}_{\mathrm{ab}} = W_{\mathrm{ab}}$.*

A proof of Theorem 10.6 can be found in the next section.

Next we describe W_{ab} by means of class field theory. Let the notation be as above. That is, L is an abelian extension of $\mathbb{Q}$ with conductor n_L, and d_L is the multiplicative order of $(2 \bmod n_{L,\mathrm{odd}})$ in the group $(\mathbb{Z}/n_{L,\mathrm{odd}}\mathbb{Z})^*$. Let $x \in \mathbb{Z}_{>0}$ such that $\gcd(x, d_L) = 1$. Then Lemma 10.9 implies $\gcd(2^x - 1, n_L) = 1$. Hence we have a well-defined map

$$\tau_{d_L} : (\mathbb{Z}/d_L\mathbb{Z})^* \to \mathrm{Gal}(L/\mathbb{Q})$$

defined by

$$u \bmod d_L \mapsto ((2^x - 1), L/\mathbb{Q}),$$

where $x \in \mathbb{Z}_{>0}$ is such that $x \equiv u \bmod d_L$ and $x \geq \mathrm{ord}_2(n_L)$. Let $m_L \in \mathbb{Z}_{>0}$ be the smallest divisor of d_L such that τ_{d_L} factors via the natural map $r : (\mathbb{Z}/d_L\mathbb{Z})^* \to (\mathbb{Z}/m_L\mathbb{Z})^*$. Define $\tau_L : (\mathbb{Z}/m_L\mathbb{Z})^* \to \mathrm{Gal}(L/\mathbb{Q})$ by $\tau_{d_L} = \tau_L \circ r$. Note that the image of τ_L is W_L.

Proposition 10.7. *The maps τ_L induce a map τ_{ab} from $\hat{\mathbb{Z}}^*$ to $G_{\mathbb{Q}}^{\mathrm{ab}}$. Moreover τ_{ab} is continuous.*

We prove Proposition 10.7 in the next section.

Now we describe the image of τ_{ab} more explicitly. We recall that we can identify $\hat{\mathbb{Z}}^*$ with $\mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$ and $G_{\mathbb{Q}}^{\mathrm{ab}}$ with $\hat{\mathbb{Z}}^*$. For $g \in \mathbb{Z}_{\mathrm{odd}}^*$ and $x \in \hat{\mathbb{Z}}^*$ recall the definition of g^x (see previous section).

Theorem 10.8. *We have $\tau_{\mathrm{ab}}(\hat{\mathbb{Z}}^*) = W_{\mathrm{ab}}$. By identifying $G_{\mathbb{Q}}^{\mathrm{ab}}$ with $\mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$, the set W_{ab} can be described as*

$$\{-1\} \times \{2^x - 1 : x \in \hat{\mathbb{Z}}^*\} \subset \mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*.$$

Furthermore the map τ_{ab} is injective.

We prove Theorem 10.8 in the next section.

Justifying the reformulations

In this section we prove Proposition 10.3, Theorem 10.4, Proposition 10.5, Theorem 10.6, Proposition 10.7, and Theorem 10.8.

Proof of Proposition 10.3. Suppose $\sigma \in \mathrm{Mer}_L$. Recall that n_L is the conductor of $L/\mathbb{Q}$. Recall the definition of $n_{L,\mathrm{odd}}$ and d_L (see just below Definition 10.1). By assumption there are infinitely many Mersenne primes $M_p = 2^p - 1$ with $\sigma = ((M_p), L/\mathbb{Q})$, so we can choose one M_p such that $p \geq \mathrm{ord}_2(n_L)$, $\gcd(p, d_L) = 1$. The definition of W_L implies $((M_p), L/\mathbb{Q}) = \sigma \in W_L$. Therefore Mer_L is a subset of W_L. □

Proof of Proposition 10.5. Let $\sigma \in \mathrm{Mer}_L$. Then there exist infinitely many Mersenne primes M with $\sigma = ((M), L/\mathbb{Q})$. Since there are only finitely many $\tau \in \mathrm{Gal}(L'/\mathbb{Q})$ with $\tau|_L = \sigma$, the consistency property (see Proposition 5.4) implies that there exists $\tau \in \mathrm{Gal}(L'/\mathbb{Q})$ with $\tau|_L = \sigma$ such that there are infinitely many Mersenne primes M with $\tau = ((M), L'/\mathbb{Q})$. Hence the restriction map $\mathrm{Mer}_{L'} \to \mathrm{Mer}_L$ is surjective.

Since $L \subset L'$, the Kronecker-Weber Theorem implies $n_L \mid n_{L'}$. Therefore we have $n_{L,\mathrm{odd}} \mid n_{L',\mathrm{odd}}$, so $d_L \mid d_{L'}$. Now the consistency property implies that the map $W_{L'} \to W_L$ is well defined and surjective. □

Proof of Theorem 10.6. (ii)⇒(iii). Direct from the definition of $\mathrm{Mer}_{\mathrm{ab}}$ and W_{ab} as projective limits.

(iii)⇒(ii). For each finite abelian extension L and L' of $\mathbb{Q}$ we have a surjective restriction map $f_L : G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{Gal}(L/\mathbb{Q})$. Proposition 10.5 implies that the restriction maps $W_L \to W_{L'}$ and $\mathrm{Mer}_L \to \mathrm{Mer}_{L'}$ are also surjective. By assumption $W_{\mathrm{ab}} = \mathrm{Mer}_{\mathrm{ab}}$, so

$$W_L = f_L(W_{\mathrm{ab}}) = f_L(\mathrm{Mer}_{\mathrm{ab}}) = \mathrm{Mer}_L.$$

The first and the third equality follow from [19, Chapter 1, §1, Proposition 1.1.6].

(ii)⇒(i). Fix $b \in \mathbb{Z}_{>0}$. Let L be the cyclotomic extension obtained by adjoining a root of unity if order $2^b - 1$ to $\mathbb{Q}$. Then L has conductor $(2^b - 1)$. The multiplicative order of $(2 \bmod 2^b - 1)$ is b. By assumption $\mathrm{Mer}_L = W_L$, so for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$ the element $((2^a - 1), L/\mathbb{Q})$ is contained in Mer_L. By definition of Mer_L this means: there are infinitely many Mersenne primes $M_q = 2^q - 1$ with $((M_q), L/\mathbb{Q}) = ((2^a - 1), L/\mathbb{Q})$. Note that $((M_q), L/\mathbb{Q}) = ((2^a - 1), L/\mathbb{Q})$ implies $M_q \equiv 2^a - 1 \bmod 2^b - 1$. The congruence $M_q \equiv 2^a - 1 \bmod 2^b - 1$ implies $q \equiv a \bmod b$. Hence for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$ there are infinitely many exponents $q \in \mathbb{Z}_{>0}$ with $q \equiv a \bmod b$ such that $2^q - 1$ is prime.

(i)⇒(ii). Let L be a finite abelian extension of $\mathbb{Q}$. Let $n \in \mathbb{Z}_{>0}$ be the conductor of $L/\mathbb{Q}$. By Kronecker-Weber the cyclotomic field $L' = \mathbb{Q}(\zeta_n)$ contains L. We recall the definition of $d_{L'}$. Write n as $2^i \cdot n_{\mathrm{odd}}$ where $i \in \mathbb{Z}_{\geq 0}$ and $n_{\mathrm{odd}} \in \mathbb{Z}_{>0}$ odd. Then $d_{L'}$ is the order of $(2 \bmod n_{\mathrm{odd}})$ in the group

$(\mathbb{Z}/n_{\mathrm{odd}}\mathbb{Z})^*$. By assumption (see (i)): for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, d_{L'}) = 1$ there are infinitely many exponents $p \in \mathbb{Z}_{>0}$ with $p \equiv a \bmod d_{L'}$ such that $2^p - 1$ is prime. Hence for each $a \in \mathbb{Z}_{>0}$ with $\gcd(a, d_{L'}) = 1$ there exists $p \in \mathbb{Z}_{>0}$ with $p \equiv a \bmod d_{L'}$ and $p \geq \mathrm{ord}_2(n)$ such that $((2^p - 1), L'/\mathbb{Q})$ is an element of $\mathrm{Mer}_{L'}$, so $\mathrm{Mer}_{L'} = W_{L'}$. Using the surjective maps $W_{L'} \to W_L$ and $\mathrm{Mer}_{L'} \to \mathrm{Mer}_L$ (see Proposition 10.5) we conclude that $\mathrm{Mer}_L = W_L$. □

Proof of Theorem 10.4. This follows directly from Theorem 10.6. □

Lemma 10.9. *Let $n, d, x \in \mathbb{Z}_{>0}$ and let $\mathfrak{f}$ be an ideal of the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt[n]{2})$. If we have $\sqrt[n]{2}^d \equiv 1 \bmod \mathfrak{f}$ and $\gcd(d, x) = 1$, then we have $(\sqrt[n]{2}^x - 1) + \mathfrak{f} = \mathcal{O}$.*

Proof. Let $\mathfrak{d} = (\sqrt[n]{2}^x - 1) + \mathfrak{f}$ be an ideal of $\mathcal{O}$. Then we have $\sqrt[n]{2}^d \equiv 1 \bmod \mathfrak{d}$ and $\sqrt[n]{2}^x \equiv 1 \bmod \mathfrak{d}$. Since $\gcd(d, x) = 1$, there exist $a, b \in \mathbb{Z}$ such that $ad + bx = 1$. Therefore we get $1 \equiv (\sqrt[n]{2}^d)^a \cdot (\sqrt[n]{2}^x)^b \equiv \sqrt[n]{2}^{ad+bx} \equiv \sqrt[n]{2} \bmod \mathfrak{d}$. Hence $\sqrt[n]{2} - 1 \in \mathfrak{d}$. Note that $\sqrt[n]{2} - 1$ is a root of $f = (y+1)^n - 2$. Since f has constant term -1, we see that $\sqrt[n]{2} - 1$ is a unit of $\mathcal{O}$. Hence we have $\mathfrak{d} = \mathcal{O}$. □

Let $A \subset \mathbb{Z}$ and let $n \in \mathbb{Z}_{>0}$. Note that we have the natural map $A \to \mathbb{Z}/n\mathbb{Z}$. Let X be a set. We call a map $f : A \to X$ periodic modulo n if there exists a map $\bar{f} : \mathbb{Z}/n\mathbb{Z} \to X$ such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr] & & X \\
& \mathbb{Z}/n\mathbb{Z} \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

commutes.

Lemma 10.10. *Let $g, n, m \in \mathbb{Z}_{>0}$. Let $A = \{x \in \mathbb{Z} : \gcd(x, nm) = 1$ and $x \geq g\}$. Suppose $f : A \to X$ is periodic modulo n and modulo m. Then f is periodic modulo $\gcd(n, m)$.*

Proof. Let $c = \gcd(n, m)$. Let $x, y \in A$ such that $x \equiv y \bmod c$. Since $x \equiv y \bmod c$, there exists $z \in \mathbb{Z}$ such that $z \equiv x \bmod n$ and $z \equiv y \bmod m$. Indeed, solve the congruence modulo every highest prime power dividing $\mathrm{lcm}(n, m)$ and apply the Chinese remainder Theorem. Clearly we have $\gcd(z, nm) = 1$. Let $h \in \mathbb{Z}_{>0}$ be such that $z' = z + nm \cdot h \geq g$. Then z' is an element of A and we have $z' \equiv x \bmod n$ and $z' \equiv y \bmod m$. Therefore we get $f(x) = f(z') = f(y)$. Hence f is periodic modulo c. □

Lemma 10.11. *Let L and L' be finite abelian extensions of $\mathbb{Q}$ such that $L \subset L'$. Then m_L divides $m_{L'}$ and the diagram*

$$\begin{tikzcd}
\hat{\mathbb{Z}}^* \arrow[r] \arrow[d, "\mathrm{id}"] & (\mathbb{Z}/m_{L'}\mathbb{Z})^* \arrow[r, "\tau_{L'}"] \arrow[d] & \mathrm{Gal}(L'/\mathbb{Q}) \arrow[d, "\mathrm{res}"] \\
\hat{\mathbb{Z}}^* \arrow[r] & (\mathbb{Z}/m_L\mathbb{Z})^* \arrow[r, "\tau_L"] & \mathrm{Gal}(L/\mathbb{Q})
\end{tikzcd}$$

commutes.

Proof. Set $n = m_L \cdot m_{L'}$ and $g = \mathrm{ord}_2(n_L)$. Let $A = \{x \in \mathbb{Z} : \gcd(x, n) = 1 \text{ and } x \geq g\}$. Let $r : A \to (\mathbb{Z}/m_L\mathbb{Z})^*$ and $r' : A \to (\mathbb{Z}/m'_L\mathbb{Z})^*$ be the natural maps. Note that $\tau_L \circ r$ is periodic modulo m_L. By the consistency property we have $\tau_L \circ r = \mathrm{res} \circ \tau_{L'} \circ r'$, so $\tau_L \circ r$ is periodic modulo m'_L. Hence by Lemma 10.10 the map $\tau_L \circ r$ is periodic modulo $\gcd(m_L, m_{L'})$. The definition of m_L (see just above Proposition 10.7) implies $m_L = \gcd(m_L, m_{L'})$. Hence m_L divides m'_L. Therefore we have a natural the map $(\mathbb{Z}/m'_L\mathbb{Z})^* \to (\mathbb{Z}/m_L\mathbb{Z})^*$. Hence by definition of $\hat{\mathbb{Z}}^*$ the left square of the diagram in Lemma 10.11 commutes (see the diagram in the section on profinite groups). The consistency property implies that the right square of the diagram in Lemma 10.11 commutes. □

Proof of Proposition 10.7. Lemma 10.11 implies that the maps τ_L induce a map $\hat{\mathbb{Z}}^*$ to $G_{\mathbb{Q}}^{\mathrm{ab}}$. Let r_L be the restriction map $G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{Gal}(L/\mathbb{Q})$. The map $r_L \circ \tau_{\mathrm{ab}}$ factors via the continuous maps $\hat{\mathbb{Z}}^* \to (\mathbb{Z}/m_L\mathbb{Z})^*$ and τ_L. Therefore $r_L \circ \tau_{\mathrm{ab}}$ is continuous. Hence we can conclude that τ_{ab} is continuous (see [19, Chapter 1, §1, Proposition 1.1.6(d)]). □

Proof of Theorem 10.8. The condition $x \geq \mathrm{ord}_2(n_L)$ in the definition of the maps τ_L implies that the projection of W_{ab} (seen as a subset of $\mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$) on the first coordinate equals $\{-1\}$. Now the definition of g^x implies $W_{\mathrm{ab}} = \{-1\} \times \{2^x - 1 : x \in \hat{\mathbb{Z}}^*\}$.

Let $(a_m)_m, (b_m)_m \in \hat{\mathbb{Z}}^*$. Suppose $(a_m)_m \neq (b_m)_m$. Then there is an integer $m \in \mathbb{N}$ such that $a_m \neq b_m$. Let $L = \mathbb{Q}(\zeta_{2^m-1})$, so $m_L = m$. Then $((2^{a_m} - 1), L/\mathbb{Q}) \neq ((2^{b_m} - 1), L/\mathbb{Q})$, which yields $\tau_{\mathrm{ab}}(a) \neq \tau_{\mathrm{ab}}(b)$. Hence the map τ_{ab} is injective. □

Chapter 11

Mersenne primes in Galois extensions

Let L be a finite Galois extension of $\mathbb{Q}$. The Chebotarev density theorem implies that for each conjugacy class C of the Galois group of $L/\mathbb{Q}$ there are infinitely many prime numbers having Frobenius symbol equal to C (see [11, Chapter VIII, §7, Theorem 7.4]). Chebotarev's theorem can be seen as a generalization of Dirichlet's theorem about primes in arithmetic progression, which we stated in the previous chapter. Since Dirichlet's theorem is not true for Mersenne primes, it follows that Chebotarev's theorem is not true for Mersenne primes either.

In this chapter we will speculate on Frobenius symbols of Mersenne primes. We will show that some conjugacy classes of a Galois group cannot be the Frobenius symbol of infinitely many Mersenne primes. The statement that the remaining conjugacy classes are the Frobenius symbol of infinitely many Mersenne primes will be reformulated in a more natural and a more compact way (see Theorem 11.7(ii) and (iii) respectively). In the next chapter we will assume the correctness of the statement in Theorem 11.7(iii) in order to partly answer a question of Lehmer. This assumption will be our working hypothesis.

Frobenius symbols of Mersenne primes

Let L be a finite Galois extension of $\mathbb{Q}$. For $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ we denote the conjugacy class of σ by $[\sigma]$.

Definition 11.1. *The set* Mer_L *is the set of all* $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ *such that there are infinitely many Mersenne primes* M *with* $[\sigma] = ((M), L/\mathbb{Q})$.

Clearly Mer_L is a subset of $\mathrm{Gal}(L/\mathbb{Q})$.

Next we define the set $W_L \subset \mathrm{Gal}(L/\mathbb{Q})$, which one should think of as the smallest subset of $\mathrm{Gal}(L/\mathbb{Q})$ that we know that contains Mer_L. Its definition will be an extension of the definition of W_L of the previous chapter to finite

Galois extensions of $\mathbb{Q}$. Hence in the case that L is a finite abelian extension over $\mathbb{Q}$ we know from the previous chapter that W_L is the image of τ_L. In this chapter we will extend the definition of τ_L in order to define W_L. The extension of τ_L is inspired by the fact that the Artin map controls the Frobenius symbols of the primes $(\sqrt[n]{2}^p - 1)$ in finite abelian extensions of $\mathbb{Q}(\sqrt[n]{2})$. The only other restriction for Frobenius symbols of the primes $(\sqrt[n]{2}^p - 1)$ we can think of comes from the consistency property. This is reflected in our definition of W_L (see definition of T_L below). Now we make this precise.

For every positive integer n and every finite abelian extension $F/\mathbb{Q}(\sqrt[n]{2})$ we define $\mathfrak{f}_{F,n}$ to be the conductor of F over $\mathbb{Q}(\sqrt[n]{2})$. Fix such a field extension $F/\mathbb{Q}(\sqrt[n]{2})$. Write $\mathfrak{f}_{F,n} = (\sqrt[n]{2})^{\mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f}_{F,n})} \cdot \mathfrak{f}_{F,n,\mathrm{odd}}$. Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\sqrt[n]{2})$. Denote the multiplicative order of $\sqrt[n]{2}$ modulo $\mathfrak{f}_{F,n,\mathrm{odd}}$ in the group $(\mathcal{O}/\mathfrak{f}_{F,n,\mathrm{odd}})^*$ by $d_{F,n}$. Let $x \in \mathbb{Z}_{>0}$ be such that $\gcd(x, d_{F,n}) = 1$. Then Lemma 10.9 implies $(\sqrt[n]{2}^x - 1) + \mathfrak{f} = \mathcal{O}$. Hence we have a well-defined map

$$\tau_{d_{F,n}} : (\mathbb{Z}/d_{F,n}\mathbb{Z})^* \to \mathrm{Gal}(F/\mathbb{Q}(\sqrt[n]{2}))$$

defined by $u \mapsto ((\sqrt[n]{2}^x - 1), F/\mathbb{Q}(\sqrt[n]{2}))$, where $x \in \mathbb{Z}$ is such that $x \equiv u \bmod d_{F,n}$ and $x \geq \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f}_{F,n})$. Note that this map is independent of the choice of x. Let $k_{F,n} \in \mathbb{Z}_{>0}$ be the smallest divisor of $d_{F,n}$ such that $\tau_{d_{F,n}}$ factors via the restriction map $r : (\mathbb{Z}/d_{F,n}\mathbb{Z})^* \to (\mathbb{Z}/k_{F,n}\mathbb{Z})^*$. Define $\tau_{F,n} : (\mathbb{Z}/k_{F,n}\mathbb{Z})^* \to \mathrm{Gal}(F/\mathbb{Q}(\sqrt[n]{2}))$ by $\tau_{d_{F,n}} = \tau_{F,n} \circ r$.

We recall $K = \bigcup_{i=1}^{\infty} \mathbb{Q}(\sqrt[i]{2})$. Denote the maximal abelian extension of $L \cap K$ in L by L^{ab} and let

$$r : \mathrm{Gal}(L/L \cap K) \to \mathrm{Gal}(L^{\mathrm{ab}}/L \cap K)$$

be the restriction map. Let $T_L = r^{-1}(\text{image of } \tau_{L^{\mathrm{ab}},n})$ where $n = [L \cap K : \mathbb{Q}]$. Since the Frobenius of a prime number is a conjugacy class of $\mathrm{Gal}(L/\mathbb{Q})$, we define W_L as follows.

Definition 11.2. *We define W_L to be the set $\bigcup_\sigma \sigma T_L \sigma^{-1}$ where σ runs over all elements of* $\mathrm{Gal}(L/\mathbb{Q})$.

Note that W_L is the set of all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ which have a conjugate $\psi \in \mathrm{Gal}(L/\mathbb{Q})$ with $\psi|_{L \cap K}$ the identity and $\psi|_{L^{\mathrm{ab}}}$ in the image of $\tau_{L^{\mathrm{ab}},n}$.

Proposition 11.3. *We have* $\mathrm{Mer}_L \subset W_L$.

A proof of Proposition 11.3 can be found in the last section of this chapter. The following proposition, which we prove in the last section of this chapter, relates the sets Mer_L and the sets W_L for finite Galois extensions L of $\mathbb{Q}$.

Proposition 11.4. *Let L be a finite Galois extension of $\mathbb{Q}$. Suppose L' is a finite Galois extension of $\mathbb{Q}$ which contains L. Then the restriction map* $\mathrm{Gal}(L'/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ *induces surjective maps* $\mathrm{Mer}_{L'} \to \mathrm{Mer}_L$, *$T_{L'} \to T_L$ and $W_{L'} \to W_L$.*

Example. Let L be the field $\mathbb{Q}(\sqrt[6]{5}, \zeta_6)$, where ζ_6 is a zero of the polynomial $x^2 - x + 1$ and $\sqrt[6]{5}$ a zero of the polynomial $x^6 - 5$. The Galois group of $L/\mathbb{Q}$ is the dihedral group $G = \langle \sigma, \psi \rangle$ of order 12, where $\sigma(\sqrt[6]{5}) = \zeta_6 \sqrt[6]{5}$ and $\sigma(\zeta_6) = \zeta_6$, and $\psi(\zeta_6) = \zeta_6^{-1}$ and $\psi(\sqrt[6]{5}) = \sqrt[6]{5}$. Recall the definition of $\mathcal{E}_{2012}$ (see first section of Chapter 10). Let $\mathcal{E} = \{p \in \mathcal{E}_{2012} : 3 \leq p \leq 20000\}$. In the table below we state a list of the Frobenius symbols of $2^p - 1$ with $p \in \mathcal{E}$.

conjugacy class	#hits	exponents
$\{\mathrm{id}\}$	5	$13, 89, 4253, 11213, 19937$
$\{\sigma^3\}$	2	$7, 4423$
$\{\sigma^2, \sigma^{-2}\}$	8	$5, 17, 61, 521, 2281, 3217, 9689, 9941$
$\{\sigma^1, \sigma^{-1}\}$	8	$3, 19, 31, 107, 127, 607, 1279, 2203$
$\{\psi, \sigma^2\psi, \sigma^4\psi\}$	0	
$\{\psi\sigma, \sigma^3\psi\}$	0	

The table suggests that only the powers of σ occur as Frobenius symbol of a Mersenne prime, i.e. the table suggests that $\mathrm{Mer}_L \subset \langle \sigma \rangle$. This suggestion can be verified by the observation that for a prime number $M_p = 2^p - 1$ we have $M_p \equiv 1 \bmod 6$, so M_p splits in $\mathbb{Q}(\zeta_6)$.

Next we calculate W_L via its definition. First we show $L \cap K = \mathbb{Q}$. The prime ideal (2) of $\mathbb{Q}$ is inert in $\mathbb{Q}(\zeta_6)/\mathbb{Q}$, so we have $\mathbb{Q}(\zeta_6) \cap K = \mathbb{Q}$. The Galois group of $L/\mathbb{Q}(\zeta_6)$ is cyclic of order 6, so we have $L \cap K \subset \mathbb{Q}(\sqrt[6]{2})$. Moreover the fields $\mathbb{Q}(\zeta_6, \sqrt[3]{5})$ and $\mathbb{Q}(\zeta_6, \sqrt{5})$ are the only intermediate fields of $L/\mathbb{Q}(\zeta_6)$. Note that the prime ideal (5) of $\mathbb{Q}$ is inert in $\mathbb{Q}(\zeta_6)/\mathbb{Q}$ and totally ramifies in $L/\mathbb{Q}(\zeta_6)$. Since (5) does not divide the discriminant of $x^3 - 2$ or $x^2 - 2$, we have $\sqrt[3]{2} \notin \mathbb{Q}(\zeta_6, \sqrt[3]{5})$ and $\sqrt{2} \notin \mathbb{Q}(\zeta_6, \sqrt{5})$. Hence we can conclude that $L \cap K = \mathbb{Q}$.

The commutator subgroup of G is $[G, G] = \langle \sigma^2 \rangle$. The order of $G/[G, G]$ is $12/3 = 4$. Therefore L^{ab}, the maximal abelian extension of $L \cap K$ in L, equals $\mathbb{Q}(\zeta_6, \sqrt{5})$. The conductor of $L^{\mathrm{ab}}/\mathbb{Q}$ is (15). The order of (2 mod 15) in $(\mathbb{Z}/15\mathbb{Z})^*$ is 4, so $d_{L^{\mathrm{ab}},1} = 4$. The Artin symbol of the ideal $(2^1 - 1)$ in $L^{\mathrm{ab}}/\mathbb{Q}$ is trivial. The prime ideal $(2^3 - 1)$ is inert in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ and splits completely in $\mathbb{Q}(\zeta_6)/\mathbb{Q}$. Hence the map

$$\tau_{d_{L^{\mathrm{ab}},1}} : (\mathbb{Z}/4\mathbb{Z})^* \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q})$$

has image $\mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\zeta_6))$ and $k_{L^{\mathrm{ab}},1} = d_{L^{\mathrm{ab}},1}$. Therefore T_L equals $\langle \sigma \rangle$. Since $\langle \sigma \rangle$ is a normal subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, we have $W_L = \langle \sigma \rangle$. Hence we have verified Proposition 11.3 for the case $L = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$.

Example. The field L used in this example comes from an article of H.W. Lenstra and P. Stevenhagen (see [9]). In the article they prove an observation of F. Lemmermeyer: if a Mersenne prime is written as $x^2 + 7y^2$ with $x, y \in \mathbb{Z}_{\geq 0}$, then x is divisible by 8.

Define $\omega = -1 + 2\sqrt{2}$ and $\overline{\omega} = -1 - 2\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. Let L be the field $\mathbb{Q}(\sqrt{\omega}, \sqrt{\overline{\omega}})$. Then the field L is Galois over $\mathbb{Q}$, its Galois group G is isomorphic to the dihedral group of order 8 and the intersection $L \cap K$ equals $\mathbb{Q}(\sqrt{2})$.

Therefore L^{ab}, the maximal abelian extension of $L \cap K$ in L, equals L, so $L^{\mathrm{ab}} = L$. Let $\sigma \in G$ be defined by $\sigma : \sqrt{\omega} \mapsto -\sqrt{\omega}$ and $\sigma : \sqrt{\overline{\omega}} \mapsto \sqrt{\overline{\omega}}$, and $\psi \in G$ be defined by $\psi : \sqrt{\omega} \mapsto \sqrt{\omega}$ and $\psi : \sqrt{\overline{\omega}} \mapsto -\sqrt{\overline{\omega}}$. In the table below we state a list of the Frobenius symbols $(2^p - 1, L/\mathbb{Q})$ with $p \in \mathcal{E}_{2012} \backslash \{3\}$.

Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{\omega\overline{\omega}}) = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$. Let ϕ be the non-trivial element of $\mathrm{Gal}(L/E)$. Note that $\phi = \sigma\psi$. The element ϕ does not appear in the table below. Indeed, let $K_1 = \mathbb{Q}(\sqrt{\omega})$, let $K_2 = \mathbb{Q}(\sqrt{\overline{\omega}})$ and consider the following field diagram.

conjugacy class	#hits	exponents p
$\{\mathrm{id}\}$	23	$p \equiv 1 \bmod 3$
$\{\sigma, \psi\}$	23	$p \equiv 2 \bmod 3$
others	0	

$$\begin{tikzcd}
 & L \arrow[dl, dash, double, "\langle\phi\rangle"'] \arrow[d, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & K_1 \arrow[d, dash] & K_2 \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) &
\end{tikzcd}$$

Let $\mathfrak{f}$ be the conductor of $L/\mathbb{Q}(\sqrt{2})$. By Theorem 6.3 we have $\mathrm{ord}_{\sqrt{2}}(\mathfrak{f}) \leq 7$. The prime ideals (ω) and $(\overline{\omega})$ of $\mathbb{Q}(\sqrt{2})$ are the only ramified primes in $L/\mathbb{Q}(\sqrt{2})$ that are tamely ramified. Hence $\mathfrak{f}_{L,2}$ divides $(8\sqrt{2})(7)$. Therefore $d_{L,2}$ divides 6. This implies that the order of $(\mathbb{Z}/d_{L,2}\mathbb{Z})^*$ is 1 or 2. Hence the order of T_L is 1 or 2. One can show that the Artin symbol of $((8\sqrt{2} - 1), L/\mathbb{Q}(\sqrt{2}))$ is trivial. This implies $\mathrm{id} \in T_L$. Moreover, one can also show the Artin symbol $((32\sqrt{2}-1), E/\mathbb{Q}(\sqrt{2}))$ is non-trivial. Hence we have $\phi \notin T_L$. Therefore we have $T_L = \{\mathrm{id}, \sigma\}$ or $T_L = \{\mathrm{id}, \psi\}$. Since σ and ψ are conjugate and $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{2}))$ is a normal subgroup of G, we conclude $W_L = \{\mathrm{id}, \sigma, \psi\}$. Now Proposition 11.3 has been verified for the case $L = \mathbb{Q}(\sqrt{\omega}, \sqrt{\overline{\omega}})$.

Theorem 11.5. *The following two statements are equivalent*

(i) *For every finite Galois extension L of $\mathbb{Q}$ and for every element σ of $T_L \subset$ $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[n]{2}))$ with $n = [L \cap K : \mathbb{Q}]$ there are infinitely many primes $\mathfrak{m}$ of L and $p \in \mathbb{Z}_{>0}$ with $\gcd(p, n) = 1$ such that $\sigma = (\mathfrak{m}, L/\mathbb{Q}(\sqrt[n]{2}))$ and $\mathfrak{m} \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$.*

(ii) *For each finite Galois extension L of $\mathbb{Q}$ we have $\mathrm{Mer}_L = W_L$.*

We prove Theorem 11.5 in the last section of this chapter.

A profinite reformulation

In this section we will reformulate Theorem 11.5(ii) in terms of projective limits. By Proposition 11.4 we can define Mer and W to be the projective limit of all Mer_L and W_L respectively, where L runs over all finite Galois extensions of $\mathbb{Q}$.

The Galois group $G_{\mathbb{Q}}$ of the algebraic closure $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ can be seen as the projective limit of all Galois groups $\mathrm{Gal}(L/\mathbb{Q})$ where $L \subset \overline{\mathbb{Q}}$ runs over all finite Galois extensions of $\mathbb{Q}$. This group $G_{\mathbb{Q}}$ is a topological group. The following proposition shows the relation with the previous chapter.

Proposition 11.6. *Let the horizontal arrows be inclusion maps and let the vertical arrows be restriction maps in the diagram below.*

$$\begin{tikzcd}
\mathrm{Mer} \arrow[r] \arrow[d] & W \arrow[r] \arrow[d] & G_{\mathbb{Q}} \arrow[d] \\
\mathrm{Mer}_{\mathrm{ab}} \arrow[r] & W_{\mathrm{ab}} \arrow[r] & G_{\mathbb{Q}}^{\mathrm{ab}}
\end{tikzcd}$$

Then this diagram commutes. Moreover the vertical arrows are surjective and both Mer *and* W *are closed subsets of* $G_{\mathbb{Q}}$.

We prove Proposition 11.6 in the next section. The set W is the smallest upper bound for Mer that we are aware of. The working hypothesis is the assumption that the equality $\mathrm{Mer} = W$ holds. In the next chapter we will see that the working hypothesis implies the converse to Theorem 7.5.

Theorem 11.7. *The following three statements are equivalent*

(i) *For every finite Galois extension L of $\mathbb{Q}$ and for every element σ of $T_L \subset \mathrm{Gal}(L/\mathbb{Q}(\sqrt[n]{2}))$ with $n = [L \cap K : \mathbb{Q}]$ there are infinitely many primes $\mathfrak{m}$ of L and $p \in \mathbb{Z}_{>0}$ with $\gcd(p, n) = 1$ such that $\sigma = (\mathfrak{m}, L/\mathbb{Q}(\sqrt[n]{2}))$ and $\mathfrak{m} \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$.*

(ii) *For each finite Galois extension L of $\mathbb{Q}$ we have $\mathrm{Mer}_L = W_L$.*

(iii) *We have $\mathrm{Mer} = W$.*

A proof of Theorem 11.7 can be found in the next section.

Next we describe W as the image of a generalisation of the map τ_{ab} of the previous chapter. Denote by K^{ab} the maximal abelian extension of K. Let G_K^{ab} be the Galois group of K^{ab}/K. Recall the maps $\tau_{F,n}$ of the previous section.

Proposition 11.8. *The maps $\tau_{F,n}$ induce an injective continuous map τ from $\hat{\mathbb{Z}}^*$ to G_K^{ab}. Furthermore we have $\tau_{\mathrm{ab}} = r \circ \tau$, where r is the restriction map from G_K^{ab} to $G_{\mathbb{Q}}^{\mathrm{ab}}$.*

We prove this proposition in the last section. Let G_K be the Galois group of $\overline{\mathbb{Q}}/K$, let $r : G_K \to G_K^{\mathrm{ab}}$ be the restriction map and define $T = r^{-1}(\text{image of } \tau)$.

Proposition 11.9. *The set W equals $\bigcup_\sigma \sigma T \sigma^{-1}$ where σ runs over all elements of $G_{\mathbb{Q}}$.*

We prove Proposition 11.9 in the next section.

Justifying the reformulations

In this section we prove the lemmas, propositions and theorems of this chapter.

Proof of Proposition 11.3. Recall the notation above Definition 11.2. We recall $n = [L \cap K : \mathbb{Q}]$. Suppose $\sigma \in \mathrm{Mer}_L$. Then there exists a prime $p \in \mathbb{Z}_{>0}$ such that $M_p = 2^p - 1$ is prime, $\gcd(k_{L^{\mathrm{ab}},n} \cdot n, p)$ equals 1, we have $p > \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f}_{L^{\mathrm{ab}},n})$ and $((M_p), L/\mathbb{Q}) = [\sigma]$. Now by the assumptions on p the element $((\sqrt[n]{2}^p - 1), L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ is in the image of $\tau_{L^{\mathrm{ab}},n}$. By definition of T_L there exists $\phi \in T_L$ such that $\phi|_{L^{\mathrm{ab}}} = ((\sqrt[n]{2}^p - 1), L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$. Since the ideal $(\sqrt[n]{2}^p - 1)$ of $\mathbb{Q}(\sqrt[n]{2})$ is a prime of degree 1 over M_p, we have $[\sigma] = [\phi]$ as conjugacy classes of $\mathrm{Gal}(L/\mathbb{Q})$. Now the definition of W_L implies $\sigma \in W_L$. □

Lemma 11.10. *Let $n, m \in \mathbb{Z}_{>0}$ be such that $n \mid m$. Let $E/\mathbb{Q}(\sqrt[m]{2})$ and $F/\mathbb{Q}(\sqrt[n]{2})$ be finite abelian extensions such that F is a subfield of E. Then $k_{F,n}$ divides $k_{E,m}$ and the diagram*

$$\begin{tikzcd}
\hat{\mathbb{Z}}^* \arrow[r] \arrow[d, "\mathrm{id}"] & (\mathbb{Z}/k_{E,m}\mathbb{Z})^* \arrow[r, "\tau_{E,m}"] \arrow[d] & \mathrm{Gal}(E/\mathbb{Q}(\sqrt[m]{2})) \arrow[d, "\mathrm{res}"] \\
\hat{\mathbb{Z}}^* \arrow[r] & (\mathbb{Z}/k_{F,n}\mathbb{Z})^* \arrow[r, "\tau_{F,n}"] & \mathrm{Gal}(F/\mathbb{Q}(\sqrt[n]{2}))
\end{tikzcd}$$

commutes.

Proof. Set $t = m \cdot d_{F,n} \cdot d_{E,m}$ and $g = \max(\mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f}_{F,n}), \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f}_{E,m}))$. By definition we have $k_{F,n} | d_{F,n}$. Let $A = \{x \in \mathbb{Z} : \gcd(x, t) = 1 \text{ and } x \geq g\}$. Let $r : A \to (\mathbb{Z}/k_{F,n}\mathbb{Z})^*$ be the restriction map. Note that $\tau_{F,n} \circ r$ is periodic modulo $k_{F,n}$ (see just above Lemma 10.10).

Let $x \in \mathbb{Z}_{>0} \cap A$ be such that all the prime ideals of $\mathbb{Q}(\sqrt[n]{2})$ that divide $(\sqrt[n]{2}^x - 1)$ are unramified in E. Since x is relatively prime to m, the norm of $\sqrt[m]{2}^x - 1$ over $\mathbb{Q}(\sqrt[m]{2})/\mathbb{Q}(\sqrt[n]{2})$ equals $\sqrt[n]{2}^x - 1$. The norm map and the Artin map are compatible for ideals which are not divisible by ramified primes (see [7, Chapter X, §1, A4]). Hence we have

$$((\sqrt[m]{2}^x - 1), E/\mathbb{Q}(\sqrt[m]{2}))|_F = ((\sqrt[n]{2}^x - 1), F/\mathbb{Q}(\sqrt[n]{2})). \tag{11.1}$$

Hence the map $\tau_{F,n} \circ r$ is periodic modulo $k_{E,m}$.

By Lemma 10.10 the map $\tau_{F,n} \circ r$ is periodic modulo $\gcd(k_{F,n}, k_{E,m})$. The definition of $k_{F,n}$ implies $k_{F,n} = \gcd(k_{F,n}, k_{E,m})$. Hence $k_{F,n}$ divides $k_{E,m}$. Therefore the left square of the diagram in Lemma 11.10 commutes. By equation 11.1 the right square of the diagram in Lemma 11.10 commutes. □

Proof of Proposition 11.4. Let $\sigma \in \mathrm{Mer}_L$. Then there exist infinitely many Mersenne primes M with $[\sigma] = (M, L/\mathbb{Q})$. Since there are only finitely many conjugacy classes ϕ of $\mathrm{Gal}(L'/\mathbb{Q})$ with $\phi|_L = \sigma$, the consistency property (see Proposition 5.4) implies that there exists $\phi \in \mathrm{Gal}(L'/\mathbb{Q})$ with $\phi|_L = \sigma$ such that there are infinitely many Mersenne primes M with $[\phi] = (M, L'/\mathbb{Q})$.

Let E be the maximal abelian extension of $L' \cap K = \mathbb{Q}(\sqrt[m]{2})$ in L' and let F be the maximal abelian extension of $L \cap K = \mathbb{Q}(\sqrt[n]{2})$ in L. Since $L \subset L'$, the integer n divides m. Lemma 11.10 implies that the restriction map $\mathrm{Gal}(E/\mathbb{Q}(\sqrt[m]{2})) \to \mathrm{Gal}(F/\mathbb{Q}(\sqrt[n]{2}))$ maps the image of $\tau_{E,m}$ surjectively to the image of $\tau_{F,n}$. Hence the map $T_{L'} \to T_L$ is surjective. Therefore the map $W_{L'} \to W_L$ is surjective. □

Proof of Proposition 11.6. Let L and L' be finite Galois extensions of $\mathbb{Q}$ such that $L \subset L'$. Proposition 11.4 implies that the surjective restriction map $\mathrm{Gal}(L'/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ induces surjective maps $\mathrm{Mer}_{L'} \to \mathrm{Mer}_L$ and $W_{L'} \to W_L$. By using [19, Chapter 1, §1, Proposition 1.1.6] we deduce that the vertical arrows in the diagram of Proposition 11.6 are surjective. Proposition 11.3 implies $\mathrm{Mer}_L \subset W_L$. By definition of W_L we have $W_L \subset \mathrm{Gal}(L/\mathbb{Q})$. Hence all horizontal arrows in the diagram of Proposition 11.6 are injective. Therefore the diagram in Proposition 11.6 commutes. Since Mer, W and $G_{\mathbb{Q}}$ are projective limits, they are Hausdorff and compact (see [19, Chapter 1, §1, Proposition 1.1.5(d)]). Every compact subset of a Hausdorff space is closed (see [13, Chapter 3, §3, Theorem 5.3]). Hence Mer and W are closed subsets of $G_{\mathbb{Q}}$. □

Proof of Proposition 11.8. By Lemma 11.10 the maps $\tau_{F,n}$ induce a map τ from $\hat{\mathbb{Z}}^*$ to G_K^{ab}. Fix $n = 1$ in Lemma 11.10. The projective limit of the maps $\tau_{F,1}$, where F runs over all finite abelian extensions of $\mathbb{Q}$, is τ_{ab}. The projective limit of all restriction maps $\mathrm{Gal}(E/\mathbb{Q}(\sqrt[m]{2})) \to \mathrm{Gal}(F/\mathbb{Q})$, where the integer m and the fields E and F are such that $E/\mathbb{Q}(\sqrt[m]{2})$ and $F/\mathbb{Q}$ are finite abelian with $F \subset E$, yields the restriction map $r : G_K^{\mathrm{ab}} \to G_{\mathbb{Q}}^{\mathrm{ab}}$. Hence Lemma 11.10 implies $\tau_{\mathrm{ab}} = r \circ \tau$.

Let r_L be the restriction map $G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/L \cap K)$. Let $n = [L \cap K : \mathbb{Q}]$. The map $r_L \circ \tau$ factors via the continuous maps $\hat{\mathbb{Z}}^* \to (\mathbb{Z}/k_{L,n}\mathbb{Z})^*$ and τ_L. Therefore $r_L \circ \tau$ is continuous. Hence we can conclude that τ is continuous (see [19, Chapter 1, §1, Proposition 1.1.6(d)]).

By Theorem 10.8 the map τ_{ab} is injective. Since $\tau_{\mathrm{ab}} = r \circ \tau$, the map τ is injective. □

Proof of Proposition 11.9. Note that T can also be defined as the projective limit of all T_L where L runs over all finite Galois extension of $\mathbb{Q}$. Recall that $G_{\mathbb{Q}}$ equals the projective limit of all $\mathrm{Gal}(L/\mathbb{Q})$ where L runs over all finite Galois extensions of $\mathbb{Q}$. By definition we have

$$W_L = \bigcup_{\sigma} \sigma T_L \sigma^{-1} \tag{11.2}$$

where σ runs over all elements of $\mathrm{Gal}(L/\mathbb{Q})$.

Next we show $W = \bigcup_\sigma \sigma T \sigma^{-1}$. Clearly we have $\bigcup_\sigma \sigma T \sigma^{-1} \subset W$. Since both the limits use the same projection maps, $\bigcup_\sigma \sigma T \sigma^{-1}$ lies dense in W. The map $G \times T \to G$ defined by $(\sigma, x) \mapsto \sigma x \sigma^{-1}$ is continuous. Therefore $\bigcup_\sigma \sigma T \sigma^{-1}$ is compact, so it is also closed. Hence we can conclude $W = \bigcup_\sigma \sigma T \sigma^{-1}$. □

Lemma 11.11. *Let $n, m \in \mathbb{Z}_{>0}$ such that $n \mid m$, and let $p \in \mathbb{Z}_{>0}$ such that $p \nmid n$ and $M = 2^p - 1$ is a prime number. Let $\mathfrak{m} \subset \mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$ be a prime of degree 1 above M. Suppose that every m-th root of unity in $(\mathbb{Z}/M\mathbb{Z})^*$ is a $\frac{m}{n}$-th root of unity. Then $\mathfrak{m} \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$.*

Proof. Let $\varphi : \mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})} \to \mathbb{Z}/(2^p - 1)\mathbb{Z}$ be the ring homomorphism with kernel $\mathfrak{m}$. Then we have $\varphi(\sqrt[m]{2}^p)^m = 2^p = 1$. By assumption we get $\varphi(\sqrt[m]{2}^p)^{m/n} = 1$, so $\varphi(\sqrt[n]{2}^p) = 1$. Hence $(\sqrt[n]{2}^p - 1) \subset \mathfrak{m}$. By assumption $p \nmid n$ so the absolute norm of $(\sqrt[n]{2}^p - 1)$ equals $2^p - 1$. Also the absolute norm of $\mathfrak{m}$ equals $2^p - 1$. Now we can conclude that $\mathfrak{m} \cap \mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})} = (\sqrt[n]{2}^p - 1)$. □

Lemma 11.12. *For every open non-empty subset $U \subset \hat{\mathbb{Z}}^*$ and every prime number q there exist an open non-empty subset $V \subset U$ and an integer $t \in \mathbb{Z}_{>0}$ such that for every $x \in V$ we have $\tau_{\mathrm{ab}}(x)(\zeta_{q^t}) \neq \zeta_{q^t}$.*

Proof. Let $q = 2$. Choose $V = U$ and $t = 2$. We have $\tau_{\mathrm{ab}} : \hat{\mathbb{Z}}^* \to \mathbb{Z}_2^* \times \mathbb{Z}_{\mathrm{odd}}^*$ (the codomain may be identified with $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$) by $x \mapsto (-1, 2^x - 1)$, so $\tau_{\mathrm{ab}}(x)(\zeta_{2^2}) = \zeta_4^{-1} \neq \zeta_4$.

Let $q > 2$. The set U is non-empty, so there exist $m \in \mathbb{Z}_{>0}$ and $a \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\{x \in \hat{\mathbb{Z}}^* : x \equiv a \bmod m\} \subset U$. Choose $b \in \mathbb{Z}_{>0}$ such that $b \equiv a \bmod m$, $\gcd(b, q(q-1)) = 1$ and $b > q$. Now we choose $t \in \mathbb{Z}_{>0}$ such that $q^t > 2^b - 1$. Let w be the multiplicative order of $(2 \bmod q^t)$. Then we have $b < w$. The order of the group $(\mathbb{Z}/q^t\mathbb{Z})^*$ is $(q-1)q^{t-1}$, so w divides $(q-1)q^{t-1}$. Let $m' = \mathrm{lcm}(m, w)$. Define V by $V = \{x \in \hat{\mathbb{Z}}^* : x \equiv b \bmod m'\}$. Note that V is non-empty since $\gcd(b, m \cdot w) = 1$. The integer m divides m' and $b \equiv a \bmod m$, so $V \subset \{x \in \hat{\mathbb{Z}}^* : x \equiv a \bmod m\} \subset U$. Let $x \in V$. From $q < b < w$ we get $b \not\equiv 1 \bmod w$. This yields $x \not\equiv 1 \bmod w$. So we have $2^x \not\equiv 2 \bmod q^t$. Therefore $\zeta_{q^t}^{2^x} \neq \zeta_{q^t}^2$ and dividing both sides by ζ_{q^t} we obtain $\zeta_{q^t}^{2^x - 1} \neq \zeta_{q^t}$. The last inequality can be rewritten as $\tau_{\mathrm{ab}}(x)(\zeta_{q^t}) \neq \zeta_{q^t}$. □

Lemma 11.13. *For every open non-empty subset $U \subset \hat{\mathbb{Z}}^*$ and every positive integer n there exist an open non-empty subset $X \subset U$ with the property that for every prime divisor q of n there exists $t_q \in \mathbb{Z}_{>0}$ such that for every $x \in X$ we have $\tau_{\mathrm{ab}}(x)(\zeta_{q^{t_q}}) \neq \zeta_{q^{t_q}}$.*

Proof. By applying Lemma 11.12 successively for each prime divisor q of n one obtains the desired set X. □

Proof of Theorem 11.7. (ii) ⇒ (iii). Follows directly from the definition of Mer and W.

(iii) ⇒ (ii). By assumption Mer equals W. From [19, Chapter 1, §1, Proposition 1.1.6] we get that both Mer $\to \mathrm{Mer}_L$ and $W \to W_L$ are surjective. Hence we have $\mathrm{Mer}_L = W_L$.

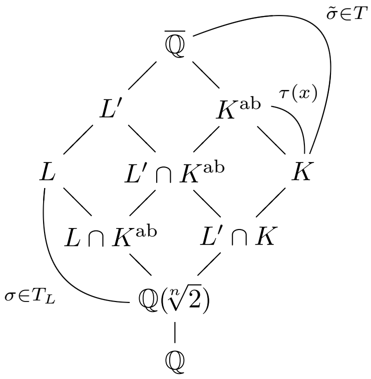
(i) ⇒ (ii). Let $\phi \in W_L$. By definition of W_L there exists an element $\sigma \in T_L$ such that ϕ is conjugate to σ. By (i) one has $\sigma \in \mathrm{Mer}_L$. Hence ϕ is an element of Mer_L.

(ii) ⇒ (i). Let L, σ and n be as in (i). Let τ be as in Proposition 11.8. Define U by

$$U = \{x \in \hat{\mathbb{Z}}^* : \sigma|_{L\cap K^{\mathrm{ab}}} = \tau(x)|_{L\cap K^{\mathrm{ab}}}\}.$$

The map τ is a continuous map, so U is open in $\hat{\mathbb{Z}}^*$. Next we show that U is non-empty. By (i) there exists $p \in \mathbb{Z}$ such that $2^p - 1$ is prime and the element $\sigma|_{L\cap K^{\mathrm{ab}}} = ((\sqrt[n]{2}^p - 1), L\cap K^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$. Therefore σ is an element of the image of $\tau_{L\cap K^{\mathrm{ab}},n}$. Hence there exists $x \in \hat{\mathbb{Z}}^*$ such that $\tau(x)|_{L\cap K^{\mathrm{ab}}} = \sigma|_{L\cap K^{\mathrm{ab}}}$. Therefore U is non-empty.

Let X be as in Lemma 11.13 applied to U and n. Choose $x \in X$. Since $x \in X \subset U$, we have $\sigma|_{L\cap K^{\mathrm{ab}}} = \tau(x)|_{L\cap K^{\mathrm{ab}}}$. Clearly $\sigma \in T_L$ is the identity on $L \cap K$. Hence we can extend σ to $\tilde{\sigma} \in T \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ such that $\tilde{\sigma}|_{K^{\mathrm{ab}}} = \tau(x)$. For an overview see the diagram below.



Set $m = n \cdot \prod_{q|n} q^{t_q - 1}$ where the product runs over all prime divisors q of n. Let L' be the normal closure of $L(\sqrt[m]{2})/\mathbb{Q}$. Define $\hat{\sigma} \in \mathrm{Gal}(L'/L' \cap K)$ by $\hat{\sigma} = \tilde{\sigma}|_{L'}$. By construction $\hat{\sigma}$ is an element of $T_{L'} \subset W_{L'}$. By (ii) we have $\hat{\sigma} \in \mathrm{Mer}_{L'}$. By definition of $\mathrm{Mer}_{L'}$ there are infinitely many primes p with $M_p = 2^p - 1$ prime such that for some prime $\mathfrak{m}'_p$ in L' above M_p the element $\mathrm{Frob}_{\mathfrak{m}'_p}(L'/\mathbb{Q})$ equals $\hat{\sigma}$. Let $\mathfrak{m}_p = \mathfrak{m}'_p \cap L$.

Next we show that $\mathfrak{m}_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$ for infinitely many p's not dividing n with $2^p - 1$ a prime number. In order to do so, we want to apply Lemma 11.11. Therefore we will show that the hypotheses of Lemma 11.11 are true in our setting. By definition of m we have $n \mid m$. Define $\mathfrak{m}$ by $\mathfrak{m} = \mathfrak{m}'_p \cap \mathbb{Q}(\sqrt[m]{2})$. By definition $\tilde{\sigma}$ is the identity on K, so $\mathfrak{m}$ is a prime of degree 1 over M_p. By definition of $\hat{\sigma}$ and the property of elements in X we have $\hat{\sigma}(\zeta_{q^{t_q}}) \neq \zeta_{q^{t_q}}$. Hence $\mathfrak{m}'_p \cap \mathbb{Q}(\zeta_{q^{t_q}})$ is not a prime of degree one. Therefore there does not exist a primitive q^{t_q}-th root of unity in $(\mathbb{Z}/M_p\mathbb{Z})^*$, so $x^{q^t} \equiv 1 \bmod M_p$ with $t \in \mathbb{Z}_{\geq t_q}$ implies $x^{q^{t_q - 1}} \equiv 1 \bmod M_p$. We conclude that if x is a m-th root of unity in $(\mathbb{Z}/M_p\mathbb{Z})^*$, then x is a $\prod_{q|n} q^{t_q-1}$-th root of unity in $(\mathbb{Z}/M_p\mathbb{Z})^*$. By definition $\prod_{q|n} q^{t_q - 1}$ equals m/n. Now all hypotheses of Lemma 11.11 are satisfied. By Lemma 11.11 we have $\mathfrak{m}'_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$. Since $\mathfrak{m}'_p \cap L = \mathfrak{m}_p$, we conclude that $\mathfrak{m}_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$ for infinitely may p's with $2^p - 1$ a prime number. Hence we have derived (i) of Theorem 11.7. □

Proof of Theorem 11.5. Follows directly from Theorem 11.7. □

Chapter 12

Lehmer's question

In the second edition of Richard Guy's book "Unsolved Problems in Number Theory" one can read in section A3 a question of D.H. Lehmer, namely: what is $\epsilon_4(p)$? In this chapter we prove assuming the working hypothesis Mer $= W$ that $\epsilon_4(p)$ is non-periodic.

Converse of the main theorems

In the following table we see the Lehmer symbol $\epsilon_4(p)$ for the first 25 odd p such that $2^p - 1$ is a Mersenne prime.

p	$\epsilon_4(p)$	mod 3	mod 5	mod 7	mod 9	mod 11	mod 13
3	+	0	3	3	3	3	3
5	+	2	0	5	5	5	5
7	−	1	2	0	7	7	7
13	+	1	3	6	4	2	0
17	−	2	2	3	8	6	4
19	−	1	4	5	1	8	6
31	+	1	1	3	4	9	5
61	+	1	1	5	7	6	9
89	−	2	4	5	8	1	11
107	−	2	2	2	8	8	3
127	+	1	2	1	1	6	10
521	−	2	1	3	8	4	1
607	−	1	2	5	4	2	9
1279	−	1	4	5	1	3	5
2203	+	1	3	5	7	3	6
2281	−	1	1	6	4	4	6
3217	−	1	2	4	4	5	6
4253	+	2	3	4	5	7	2
4423	−	1	3	6	4	1	3
9689	−	2	4	1	5	9	4

p	$\epsilon_4(p)$	mod 3	mod 5	mod 7	mod 9	mod 11	mod 13
9941	+	2	1	1	5	8	9
11213	−	2	3	6	8	4	7
19937	+	2	2	1	2	5	8
21701	−	2	1	1	2	9	4
23209	+	1	4	4	7	10	4

If the working hypothesis is true then one cannot find patterns between the column with the signs and the modulo-columns. We state this more precisely in the following theorem.

Theorem 12.1. *If ϵ_4 is periodic, then* Mer *is not W.*

Theorem 12.1 implies that if one proves that ϵ_4 is periodic, then one has new knowledge about the Frobenius symbols of Mersenne primes.

We will prove the following generalization of Theorem 12.1 in the next section. This Theorem can been seen as the converse of Theorem 7.5.

Theorem 12.2. *Let $s \in K$ be a universal starting value. If ϵ_s is periodic and $4 - s^2 \notin K^{*2}$, then* Mer *is not W.*

We get the following similar result for a related pair of potential starting values. This result can been seen as the converse of Corollary 9.4.

Theorem 12.3. *Let $s, t \in K$ be a related pair of potential starting values and suppose both s and t are universal starting values. If $\epsilon_{s,t}$ is periodic and $(2 + \sqrt{2+s})(2 + \sqrt{2+t})$ is not a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$, then* Mer *is not W.*

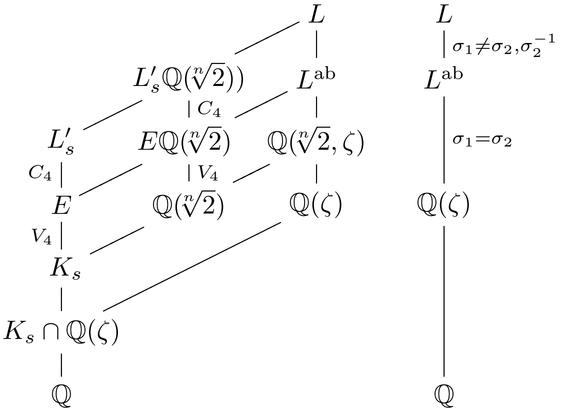
We prove Theorem 12.3 in the next section.

Lehmer's question and the working hypothesis

In this section we prove Theorem 12.1, Theorem 12.2 and Theorem 12.3.

Proof of Theorem 12.2. Let $s \in K$ be a universal starting value. Theorem 3.2 implies that s is a potential starting value. Assume that $4 - s^2 \notin K^{*2}$. Then Proposition 4.3 implies that the Galois group of the extension L'_s/K_s is isomorphic to the dihedral group D_8 of 16 elements. Let $E = K_s(\sqrt{4-s^2}, \sqrt{s+2}) \subset L'_s$. Since s is a potential starting value and $4 - s^2 \notin K^{*2}$, we have $[E : K_s] = 4$. The commutator subgroup of D_8 has 4 elements and $[E : K_s] = 4$, so E is the maximal abelian extension of K_s in L'_s. By assumption ϵ_s is periodic. Let $l \in \mathbb{Z}_{>0}$ and $m \in \mathbb{Z}_{>0}$ be as in Definition 7.4. Define $\zeta = \zeta_{2^m-1} \in \overline{\mathbb{Q}}$ to be a primitive $(2^m - 1)$-th root of unity. Let L be the Galois closure of $L'_s(\zeta)$ over $\mathbb{Q}$. Let $n = [L \cap K : \mathbb{Q}]$, so that $L \cap K = \mathbb{Q}(\sqrt[n]{2})$. By definition $K_s = L'_s \cap K$. Therefore $L'_s \cap \mathbb{Q}(\sqrt[n]{2})$ equals K_s. Hence the restriction map $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism. Therefore $E\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $L'_s\mathbb{Q}(\sqrt[n]{2})$.

We denote the maximal abelian extension of $L \cap K$ in L by L^{ab}. Since $E\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $L'_s\mathbb{Q}(\sqrt[n]{2})$, the field $E\mathbb{Q}(\sqrt[n]{2})$ is a subfield of L^{ab} and $L^{\mathrm{ab}} \cap L'_s\mathbb{Q}(\sqrt[n]{2})$ equals $E\mathbb{Q}(\sqrt[n]{2})$. Clearly $\mathbb{Q}(\zeta)$ is a subfield of L^{ab}. In the following diagram we see an overview of the fields, four Galois groups and three group elements used in this proof.


L
$L'_s\mathbb{Q}(\sqrt[n]{2}))$
L^{ab}
C_4
L'_s
$E\mathbb{Q}(\sqrt[n]{2})$
$\mathbb{Q}(\sqrt[n]{2}, \zeta)$
C_4
V_4
E
$\mathbb{Q}(\sqrt[n]{2})$
$\mathbb{Q}(\zeta)$
V_4
K_s
$K_s \cap \mathbb{Q}(\zeta)$
$\mathbb{Q}$
L
$\sigma_1 \neq \sigma_2, \sigma_2^{-1}$
L^{ab}
$\sigma_1 = \sigma_2$
$\mathbb{Q}(\zeta)$
$\mathbb{Q}$

Next we recall the definition of T_L. Denote the conductor of L^{ab} over $\mathbb{Q}(\sqrt[n]{2})$ by $\mathfrak{f}$. Write $\mathfrak{f} = (\sqrt[n]{2})^{\mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})} \cdot \mathfrak{f}_{\mathrm{odd}}$. Denote the multiplicative order of $\sqrt[n]{2}$ modulo $\mathfrak{f}_{\mathrm{odd}}$ in the group $(\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}/\mathfrak{f}_{\mathrm{odd}})^*$ by k. The map $\tau : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ is defined by $u \mapsto ((\sqrt[n]{2}^x - 1), L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$, where $x \in \mathbb{Z}$ is such that $x \equiv u \bmod k$ and $x \geq \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})$. Let $r : \mathrm{Gal}(L/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ be the restriction map. We recall $T_L = r^{-1}(\text{image of } \tau)$.

Suppose for a contradiction the working hypothesis Mer $= W$. Since the restriction map $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism, Proposition 4.3 and Proposition 5.10(iv) imply that for any $\sigma \in T_L$ the element $\sigma|_{L'_s\mathbb{Q}(\sqrt[n]{2})}$ generates the cyclic group $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2}, \sqrt{4-s^2}))$ of order 8 . Since $L^{\mathrm{ab}} \cap L'_s\mathbb{Q}(\sqrt[n]{2})$ equals $E\mathbb{Q}(\sqrt[n]{2})$, there exist $\sigma_1, \sigma_2 \in T_L$ such that $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$ and $\sigma_1|_{L'_s\mathbb{Q}(\sqrt[n]{2})} \neq (\sigma_2|_{L'_s\mathbb{Q}(\sqrt[n]{2})})^{\pm 1}$. Since $\sigma_1|_{L'_s\mathbb{Q}(\sqrt[n]{2})} \neq (\sigma_2|_{L'_s\mathbb{Q}(\sqrt[n]{2})})^{\pm 1}$ and the restriction map $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism, we have $\sigma_1|_{L'_s} \neq (\sigma_2|_{L'_s})^{\pm 1}$. Hence Definition 4.6 and Definition 4.5 imply $\lambda'_s([\sigma_1|_{L'_s}]) \neq \lambda'_s([\sigma_2|_{L'_s}])$.

Let $\sigma_1, \sigma_2 \in T_L$ be as above. Then Theorem 11.7(i), applied to the extension $L/\mathbb{Q}(\sqrt[n]{2})$, implies that there exist $p, q \in \mathbb{Z}_{>l}$ with $\gcd(pq, n) = 1$ such that $\sigma_1 = (\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))$ and $\sigma_2 = (\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))$, and both ideals $\mathfrak{M}_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$ and $\mathfrak{M}_q \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^q - 1)$ are prime ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}$. Since $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$, we have $(\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)} = (\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)}$. The extension $\mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})$ is abelian, so $((\sqrt[n]{2}^p - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})) = ((\sqrt[n]{2}^q - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2}))$. Since the prime ideals $(\sqrt[n]{2}^p - 1)$ and $(\sqrt[n]{2}^q - 1)$ are of degree 1 over $\mathbb{Q}$, we have $((2^p - 1), \mathbb{Q}(\zeta)/\mathbb{Q}) = ((2^q - 1), \mathbb{Q}(\zeta)/\mathbb{Q})$. This implies $2^p - 1 \equiv 2^q - 1 \bmod (2^m - 1)$, so $p \equiv q \bmod m$. By construction $p, q > l$ and by assumption ϵ_s is periodic, so $\epsilon_s(p) = \epsilon_s(q)$. The consistency property implies

$[\sigma_1|_{L'_s}] = (\mathfrak{M}_p \cap L'_s, L'_s/K_s)$ and $[\sigma_2|_{L'_s}] = (\mathfrak{M}_q \cap L'_s, L'_s/K_s)$. Recall the definition of Frob' above Corollary 5.7. Now we see that $\mathrm{Frob}'(p) = (\mathfrak{M}_p \cap L'_s, L'_s/K_s)$ and $\mathrm{Frob}'(q) = (\mathfrak{M}_q \cap L'_s, L'_s/K_s)$. Therefore we have $(\lambda'_s \circ \mathrm{Frob}')(p) \neq (\lambda'_s \circ \mathrm{Frob}')(q)$. Now Corollary 5.7 implies $\epsilon_s(p) \neq \epsilon_s(q)$. This is a contradiction. Hence $\mathrm{Mer} \neq W$. □

Proof of Theorem 12.1. Note that $4 - 4^2 = -12$ is not a square in K^*. Now Theorem 12.2 implies Theorem 12.1. □

The ideas of the proof of Theorem 12.2 can also be applied to pairs of universal starting values. To illustrate this we give the following proof. The following proof is similar to the proof of Theorem 12.2.

Proof of Theorem 12.3. Let $s, t \in K$ be a related pair of potential starting values. We will recall from Chapter 8 the definition of the fields $K_{s,t}$, E', E'', E and F. Recall $f_s = x^{16} - sx^8 + 1$, the element $\alpha = \alpha_s \in \overline{\mathbb{Q}}$ a zero of f_s and L_s the splitting field of f_s over $\mathbb{Q}(s)$. Recall $K_{s,t} = (L_s L_t) \cap K$ and $F_s = K_{s,t}(\sqrt{4-s^2}, \alpha_s + \alpha_s^{-1})$. Finally we recall $F = F_s F_t$, the field $E = F_s \cap F_t$, the field $E' = K_{s,t}(\sqrt{4-s^2})$ and $E'' = E'(\sqrt{s+2})$. By assumption $e'' = (2 + \sqrt{2+s})(2 + \sqrt{2+t})$ is not a square in E''^*, so Lemma 9.13 implies $[E : E'] \neq 4$ or 8. Therefore Lemma 8.16 implies $[E : E'] = 2$. Denote the maximal abelian extension of $K_{s,t}$ in F by D. Let T be as in Proposition 8.9. Then D equals TE''.

By assumption $\epsilon_{s,t}$ is periodic. Let $l \in \mathbb{Z}_{>0}$ and $m \in \mathbb{Z}_{>0}$ be as in Definition 7.4. Define $\zeta = \zeta_{2^m - 1} \in \overline{\mathbb{Q}}$ to be a primitive $(2^m - 1)$-th root of unity. Let L be the Galois closure of $F(\zeta)$ over $\mathbb{Q}$. Let $n = [L \cap K : \mathbb{Q}]$, so that $L \cap K = \mathbb{Q}(\sqrt[n]{2})$. By definition $K_{s,t} = F \cap K$. Therefore $F \cap \mathbb{Q}(\sqrt[n]{2})$ equals $K_{s,t}$. Hence the restriction map $\mathrm{Gal}(F\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(F/K_{s,t})$ is an isomorphism. Therefore $D\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $F\mathbb{Q}(\sqrt[n]{2})$.

We denote the maximal abelian extension of $L \cap K$ in L by L^{ab}. Since $D\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $F\mathbb{Q}(\sqrt[n]{2})$, the field $D\mathbb{Q}(\sqrt[n]{2})$ is a subfield of L^{ab} and $L^{\mathrm{ab}} \cap F\mathbb{Q}(\sqrt[n]{2})$ equals $D\mathbb{Q}(\sqrt[n]{2})$. Clearly $\mathbb{Q}(\zeta)$ is a subfield of L^{ab}. In the following diagram we see an overview of the fields used in this proof.

$$\begin{tikzcd}
 & & L \arrow[d, dash] \\
 & F\mathbb{Q}(\sqrt[n]{2})) \arrow[ur, dash] \arrow[d, dash] & L^{\mathrm{ab}} \arrow[d, dash] \\
F \arrow[ur, dash] \arrow[d, dash] & D\mathbb{Q}(\sqrt[n]{2}) \arrow[ur, dash] \arrow[d, dash] & \mathbb{Q}(\sqrt[n]{2}, \zeta) \arrow[d, dash] \\
D = TE'' \arrow[ur, dash] \arrow[d, dash] & \mathbb{Q}(\sqrt[n]{2}) \arrow[ur, dash] & \mathbb{Q}(\zeta) \\
K_{s,t} \arrow[ur, dash] \arrow[d, dash] & & \\
K_{s,t} \cap \mathbb{Q}(\zeta) \arrow[uurr, dash] \arrow[d, dash] & & \\
\mathbb{Q} & &
\end{tikzcd}$$

Next we recall the definition of T_L. Denote the conductor of L^{ab} over $\mathbb{Q}(\sqrt[n]{2})$ by $\mathfrak{f}$. Write $\mathfrak{f} = (\sqrt[n]{2})^{\mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})} \cdot \mathfrak{f}_{\mathrm{odd}}$. Denote the multiplicative order of $\sqrt[n]{2}$ modulo $\mathfrak{f}_{\mathrm{odd}}$ in the group $(\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}/\mathfrak{f}_{\mathrm{odd}})^*$ by k. The map $\tau : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ is defined by $u \mapsto ((\sqrt[n]{2}^x - 1), L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$, where $x \in \mathbb{Z}$ is such that $x \equiv u \bmod k$ and $x \geq \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})$. Let $r : \mathrm{Gal}(L/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ be the restriction map. We recall $T_L = r^{-1}(\text{image of } \tau)$.

Suppose for a contradiction the working hypothesis $\mathrm{Mer} = W$. Since the restriction map $\mathrm{Gal}(F\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(F/K_{s,t})$ is an isomorphism, Proposition 9.8 and the consistency property imply that for any $\sigma \in T_L$ the conjugacy class $[\sigma|_F]$ is an element of $\mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim$. Since $[E : E'] = 2$, Theorem 8.10 implies that the map $\lambda'_{s,t} : \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \to \{\pm 1\}$ does not factor via the restriction map $\mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \to \mathrm{Gal}(T/K_{s,t})$. Hence $L^{\mathrm{ab}} \cap F\mathbb{Q}(\sqrt[n]{2}) = D\mathbb{Q}(\sqrt[n]{2}) = (TE'')\mathbb{Q}(\sqrt[n]{2})$ implies that there exist $\sigma_1, \sigma_2 \in T_L$ such that $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$ and $\lambda'_{s,t}([\sigma_1|_F]) \neq \lambda'_{s,t}([\sigma_2|_F])$.

Let $\sigma_1, \sigma_2 \in T_L$ be as above. Then by Theorem 11.7(i) (applied to the extension $L/\mathbb{Q}(\sqrt[n]{2})$) there exist $p, q \in \mathbb{Z}_{>l}$ with $\gcd(pq, n) = 1$ such that $\sigma_1 = (\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))$ and $\sigma_2 = (\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))$, and $\mathfrak{M}_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$ and $\mathfrak{M}_q \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^q - 1)$ both prime ideals of $\mathbb{Q}(\sqrt[n]{2})$. Since $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$, the Frobenius symbol $(\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)}$ equals $(\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)}$. The extension $\mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})$ is abelian, so $((\sqrt[n]{2}^p - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})) = ((\sqrt[n]{2}^q - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2}))$. Since the prime ideals $(\sqrt[n]{2}^p - 1)$ and $(\sqrt[n]{2}^q - 1)$ are of degree 1 over $\mathbb{Q}$, we have $((2^p - 1), \mathbb{Q}(\zeta)/\mathbb{Q}) = ((2^q - 1), \mathbb{Q}(\zeta)/\mathbb{Q})$. This implies $2^p - 1 \equiv 2^q - 1 \bmod (2^m - 1)$, so $p \equiv q \bmod m$. By construction we have $\lambda'_{s,t}([\sigma_1|_F]) \neq \lambda'_{s,t}([\sigma_2|_F])$. The consistency property implies $[\sigma_1|_F] = (\mathfrak{M}_p \cap F, F/K_{s,t})$ and $[\sigma_2|_F] = (\mathfrak{M}_q \cap F, F/K_{s,t})$. Recall the definition of Frob_2 above Corollary 9.10. Now we see that $\mathrm{Frob}_2(p) = (\mathfrak{M}_p \cap F, F/K_{s,t})$ and $\mathrm{Frob}_2(q) = (\mathfrak{M}_q \cap F, F/K_{s,t})$. Therefore we have $(\lambda'_{s,t} \circ \mathrm{Frob}_2)(p) \neq (\lambda'_{s,t} \circ \mathrm{Frob}_2)(q)$. Now Corollary 9.10 implies $\epsilon_{s,t}(p) \neq \epsilon_{s,t}(q)$. This is a contradiction. Hence $\mathrm{Mer} \neq W$. □

Appendix

The set of currently known exponents $p \in \mathbb{Z}_{>0}$ such that $2^p - 1$ is a Mersenne prime, is

$$\{2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,\\ 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243,\\ 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221,\\ 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457,\\ 32582657, 37156667, 42643801, 43112609\}.$$

Bibliography

[1] D.A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley-Interscience, 1989.

[2] A. Fröhlich and M.J. Taylor, *Algebraic number theory*, Cambridge University Press, 1994.

[3] S.Y. Gebre-Egziabher, unpublished thesis work, U.C. Berkeley.

[4] R.K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1994.

[5] G. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

[6] S. Lang, *Algebra*, third edition, Addison-Wesley Publishing Company, 1999.

[7] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 1994.

[8] F. Lemmermeyer, *Reciprocity laws*, Springer-Verlag, 2000.

[9] H.W. Lenstra, Jr., P. Stevenhagen, *Artin reciprocity and Mersenne primes*, Nieuw Archief voor Wiskunde 5/1. nr.1, maart 2000, pp. 44-54.

[10] J.S. Milne, *Algebraic Number Theory*, http://www.jmilne.org/math, 2011.

[11] J.S. Milne, *Class Field Theory*, http://www.jmilne.org/math, 2011.

[12] J.S. Milne, *Fields and Galois Theory*, http://www.jmilne.org/math, 2011.

[13] J.R. Munkres, *Topology: a first course*, Prentice-Hall, 1975.

[14] J.-P. Serre, *Local Fields*, Springer-Verlag, 1979.

[15] J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[16] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[17] A. Vardhana, personal communication, 2004.

[18] H.C. Williams, *Édouard Lucas and Primality Testing*, Wiley-Interscience, 1998.

[19] J.S. Wilson, *Profinite Groups*, Oxford, 1998.

Samenvatting

Priemgetallen

Op de middelbare school leer je dat alle materie is opgebouwd uit atomen. Zo bestaat een watermolecuul (H_2O) uit twee waterstofatomen en één zuurstofatoom. De atomen kun je daarom zien als de bouwstenen van de materie. Binnen de verzameling van de natuurlijke getallen

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots\}$$

heb je ook bouwstenen waaruit je alle natuurlijke getallen kunt maken. Zo is 45 “opgebouwd” uit twee 3’en en één 5, want $45 = 3 \cdot 3 \cdot 5$. De getallen 3 en 5 zijn voorbeelden van priemgetallen. Priemgetallen zijn de bouwstenen van de natuurlijke getallen.

In het scheikundelokaal hangt een poster van het periodiek systeem der elementen. Hierop staan alle atomen afgebeeld gerangschikt naar hun chemische eigenschappen. In het wiskundelokaal zie je geen poster met daarop alle priemgetallen afgebeeld. Dit komt niet omdat zo’n poster niet interessant zou zijn. Integendeel, één van de belangrijkste problemen in de wiskunde (de Riemann hypothese) gaat over de priemgetallen. Rond 300 voor Christus bewees Euclides echter dat er oneindig veel priemgetallen zijn. Dus alle priemgetallen passen niet op een poster. Als je de priemgetallen rangschikt van klein naar groot, dan ziet de verzameling van de priemgetallen er als volgt uit

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots\}.$$

Perfecte getallen

Een ander onderwerp dat Euclides bestudeerde waren de zogenaamde perfecte getallen. Aan de hand van het volgende voorbeeld wordt duidelijk wat een perfect getal is.

De delers van 6 zijn 1, 2 en 3 (de deler 6 doet niet mee). De som $1 + 2 + 3$ van deze delers is weer gelijk aan het oorspronkelijke getal 6. Als een getal deze bijzondere eigenschap heeft dan noemen het getal een perfect getal. Ook het getal 28 is perfect, want de delers van 28 zijn 1, 2, 4, 7, 14 en

$$1 + 2 + 4 + 7 + 14 = 28.$$

De volgende twee perfecte getallen zijn 496 en 8128. Er geldt

$$1+2+4+8+16+31+62+124+248=496 \text{ en}$$

$$1+2+4+8+16+32+64+127+254+508+1016+2032+4064=8128.$$

Het volgende patroon dringt zich op

$$\begin{aligned}(1+2)\cdot 2 &= 6\\ (1+2+4)\cdot 4 &= 28\\ (1+2+4+8+16)\cdot 16 &= 496\\ (1+2+4+8+16+32+64)\cdot 64 &= 8128.\end{aligned}$$

Je kunt je afvragen waarom bijvoorbeeld $(1+2+4+8)\cdot 8=120$ geen perfect getal oplevert. Dit getal lijkt immers dezelfde structuur te hebben als de perfecte getallen hierboven. Toch is er een groot verschil tussen 120 en de getallen hierboven. Namelijk de som $1+2+4+8=15$ is geen priemgetal, terwijl de som tussen de haakjes bij de perfecte getallen wel een priemgetal is. Ga maar na

$$\begin{aligned}(1+2) &= 3\\ (1+2+4) &= 7\\ (1+2+4+8+16) &= 31\\ (1+2+4+8+16+32+64) &= 127.\end{aligned}$$

Euclides bewees dat elk getal van de vorm

$$\underbrace{(1+2+4+8+16+\ldots+\text{ laatste term })}_{\text{priemgetal}}\cdot\text{ laatste term}$$

perfect is. Later bewees Leonhard Euler (1707–1783) dat alle even perfecte getallen van deze vorm zijn. Men vermoedt dat er geen oneven perfecte getallen bestaan.

Mersenne-priemgetallen

Met het resultaat van Euclides werd een zoektocht naar perfecte getallen een zoektocht naar priemgetallen van de vorm $1+2+4+8+\ldots+$ laatste term. Getallen van deze vorm zullen we noteren met M_n waarbij n het aantal termen is in de som. Zo is $M_3=1+2+4$ en $M_8=1+2+4+8+16+32+64+128$. Priemgetallen van de vorm M_n noemen we Mersenne-priemgetallen, naar de Franse monnik Marin Mersenne (1588–1648).

In de volgende tabel zie je in chronologische volgorde tot het computertijdperk voor welke n het getal M_n een Mersenne-priemgetal is (zie [18, Hoofdstuk 8.5]). (Voor de volledige lijst van bekende Mersenne-priemgetallen zie de appendix.)

n	M_n	jaar van ontdekking	ontdekker
2	3	5e eeuw voor Christus	de Oude Grieken
3	7	5e eeuw voor Christus	de Oude Grieken
5	31	3e eeuw voor Christus	de Oude Grieken
7	127	3e eeuw voor Christus	de Oude Grieken
13	8191	1456	onbekend
17	131071	1588	Cataldi
19	524287	1588	Cataldi
31	2147483647	1772	Euler
127	17014118...884105727	1876	Lucas
61	2305843009213693951	1883	Pervushin
89	618970019...449562111	1911	Powers
107	162259276...010288127	1914	Powers

Opmerkelijk is het resultaat van Edouard Lucas (1842–1891). Hoe is hij in staat geweest om aan te tonen dat het getal M_{127}, dat uit 39 cijfers bestaat, een priemgetal is? Het antwoord op deze vraag is: veel geduld en een slimme door Lucas zelf ontwikkelde priemtest voor getallen van de vorm M_n. Deze test werd in 1930 aangepast door Derrick Lehmer (1905–1991). De aangepaste versie van de test noemen we nu de Lucas-Lehmer-test.

Pas in 1952 toonde de Amerikaanse wiskundige Raphael Robinson (1911–1995) m.b.v. de computer en de Lucas-Lehmer-test aan dat M_{521} een Mersenne-priemgetal is. Hiermee was Lucas' record M_{127} van het grootste bekende priemgetal verbroken.

Vandaag de dag gebruikt men nog steeds de Lucas-Lehmer-test om grote priemgetallen te vinden. Het grootst bekende priemgetal op dit moment is $M_{43112609}$. Het is gevonden door een netwerk van computers die zich hebben aangesloten bij het GIMPS-project (Great Internet Mersenne Prime Search) opgericht door George Woltman (1957) in 1996.

De Lucas-Lehmer-test

Lucas wist dat M_n alleen een priemgetal kan zijn als n zelf een priemgetal is. Aangezien 127 een priemgetal is maakte Lucas een kans met het testen van M_{127} op primaliteit. Zijn test deed hij op twee grote damborden van 127 bij 127 hokjes. Op het ene dambord werd geschoven met steentjes en op het andere dambord werden de tussenresultaten bijgehouden.

Om dit te illustreren zullen we gaan testen of M_5 een priemgetal is. Daartoe tekenen we een dambord van 5 bij 5 hokjes en leggen op de eerste rij derde kolom één steen neer. Dit is de beginpositie. Vanaf de beginpositie gaan we $5-2$ keer de volgende stappen uitvoeren (voor M_n voer je de stappen $n-2$ keer uit).

STAP 1: Leg voor elke steen in de i-de kolom van de eerste rij een kopie van de eerste rij neer en schuif deze kopie $i-1$ hokjes naar rechts. Als je een steen in de laatste kolom één hokje naar rechts moet verschuiven, dan leg je de steen in de eerste kolom neer.

STAP 2: Verwijder zo mogelijk één steen uit de tweede kolom. Als er geen steen in de tweede kolom ligt, dan leg je in alle kolommen behalve de tweede kolom een steen neer.

STAP 3: Pak zo lang dat mogelijk is twee stenen uit kolom i en leg daarvoor in de plaats één steen in kolom $i+1$. Twee stenen uit de laatste kolom worden vervangen door één steen in de eerste kolom. Daarna schuif je elke steen naar de eerste rij zonder de steen van kolom te veranderen.

De borden 1 t/m 4 zien we hieronder. Op bord 1 zie je de beginpositie. De eerste rij van deze beginpositie neem je over op het resultatendambord. Door STAP 1 uit te voeren krijg je de positie op bord 2. Door STAP 2 uit te voeren krijg je de positie op bord 3, en door STAP 3 uit te voeren krijg je de positie op bord 4.

Nu hebben we de stappen 1 t/m 3 één keer uitgevoerd. De eerste rij van bord 4 zou Lucas op zijn resultatendambord overnemen. Door vanaf bord 4 nogmaals de stappen 1 t/m 3 uit te voeren komen we bij bord 7. De eerste rij van bord 7 wordt wederom op het resultatendambord overgenomen.

De laatste drie stappen staan hieronder op de borden 7 t/m 10. We zien dat bij het eindresultaat (bord 10) de eerste rij leeg is. Het resultatendambord krijgen we door de eerste rij van bord 1, bord 4, bord 7 en bord 10 onder elkaar te zetten in een dambord van 5 bij 5. Hieronder zie je de resultatendamborden voor M_3 t/m M_8.

De Lucas-Lehmer-test zegt dat M_n een priemgetal is alleen als de voorlaatste rij van het resultatendambord dat bij M_n behoort leeg is of helemaal vol ligt met stenen. Door bij de resultatendamborden hieronder de voorlaatste rij af te lezen zien we dat M_3, M_5 en M_7 priemgetallen zijn en M_4, M_6 en M_8 geen priemgetallen zijn.

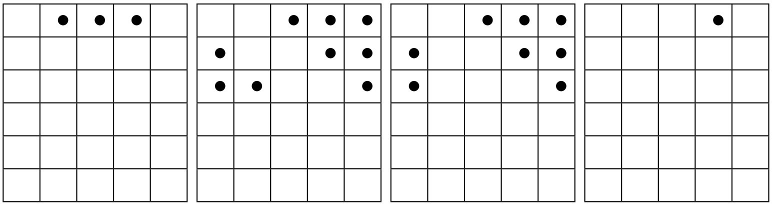
		●		

				●

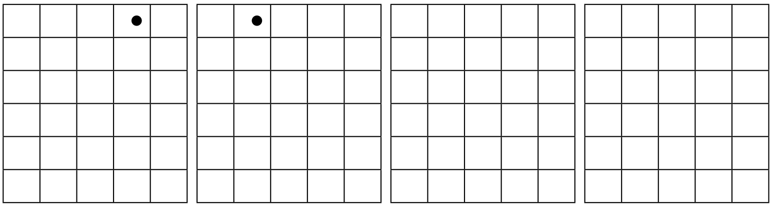
				●
●		●	●	●

	●	●	●	

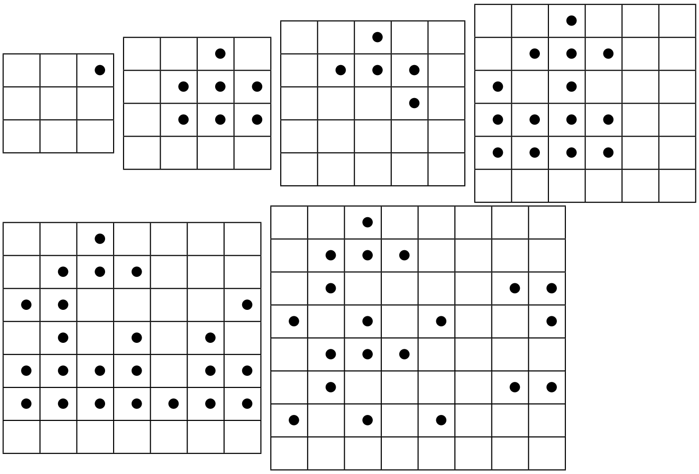
Bord 1 t/m 4



Bord 4 t/m 7



Bord 7 t/m 10



Resultatendamborden behorend bij M_3 t/m M_8

Lehmer's vraag

Als M_n een Mersenne-priemgetal is, dan weet je dat de voorlaatste rij van het resultatendambord van M_n óf helemaal leeg is óf helemaal vol ligt met stenen. Lehmer vroeg zich af of het mogelijk is om snel te bepalen welke van de twee mogelijkheden zich zal voordoen. Dit proefschrift gaat over deze vraag.

Vele beginposities

Tot nu toe was de beginpositie telkens één steen in de derde kolom (beginpositie I). Er zijn ook andere beginposities waarmee je de Lucas-Lehmer-test kunt uitvoeren. Zowel in de tweede als vierde kolom één steen is zo'n andere beginpositie (beginpositie II). Voor borden met meer dan vier hokjes is een steen in de eerste én tweede kolom en daarna alternerend geen en wel een steen in overige kolommen ook beginpositie waarmee je de Lucas-Lehmer-test kunt uitvoeren (beginpositie III). Voor elke beginpositie kunnen we Lehmer's vraag stellen.

In dit proefschrift geven we meerdere formules waarmee je oneindig veel beginposities kunt maken en we geven aan hoe je andere van dit soort formules kunt maken. Deze formules komen in twee typen, A en B. De formules van type A zijn de formules waarvoor we voor alle beginposities die uit de formule komen Lehmer's vraag kunnen beantwoorden met ja, en de formules van type B zijn de formules waarvoor we voor geen van de beginposities die uit de formule komen Lehmer's vraag kunnen beantwoorden.

Beginpositie I en II komen uit formules van type B. Beginpositie III komt uit een formule van type A. Voor beginpositie III geldt dat de voorlaatste rij van het resultatendambord van M_n leeg is dan en slechts dan als $n-1$ deelbaar is door 4 (en $n \neq 5$). Voor andere beginposities die uit formules van type A komen gelden soortgelijke uitspraken.

Woltman's vermoeden

Hoewel we geen antwoord hebben op Lehmer's vraag voor beginpositie I en beginpositie II is er wel een verband tussen deze twee beginposities. De voorlaatste rij van het resultaatbord van M_n met beginpositie I is gelijk aan de voorlaatste rij van het resultaatbord van M_n met beginpositie II dan en slechts dan als $n-5$ of $n-7$ deelbaar is door 8 en $n \neq 5$. Dit verband werd als eerste gezien door Woltman in 1996. In dit proefschrift bewijzen we dit vermoeden en geven we andere voorbeelden van relaties tussen verschillende beginposities die komen van formules van type B.

Terug naar Lehmer's vraag voor beginpositie I

Lehmer's vraag voor beginpositie I blijft onbeantwoord. Wel laten we in dit proefschrift zien: als iemand voor beginpositie I (of elke andere beginpositie die komt van een formule van type B) een soortgelijke stelling kan vinden als voor beginpositie III, dan is het gedrag van de Mersenne-priemgetallen heel anders dan je zou mogen verwachten.

Klassenlichamentheorie en priemgetallen van de vorm $x^2 - 2 \cdot y^2$

Diophantische problemen vormen een belangrijke motor voor het ontwikkelen van nieuwe getaltheorie. Een voorbeeld van een Diophantisch probleem is de vraag: welke priemgetallen kun je schrijven als het verschil van een kwadraat en tweemaal een ander kwadraat? Voor de priemgetallen kleiner dan of gelijk aan 53 geeft dit het volgende resultaat.

p	wel of geen oplossing?	bijvoorbeeld
2	wel	$2^2 - 2 \cdot 1^2$
3	geen	
5	geen	
7	wel	$5^2 - 2 \cdot 3^2$
11	geen	
13	geen	
17	wel	$7^2 - 2 \cdot 4^2$
19	geen	
23	wel	$5^2 - 2 \cdot 1^2$
29	geen	
31	wel	$9^2 - 2 \cdot 5^2$
37	geen	
41	wel	$7^2 - 2 \cdot 2^2$
43	geen	
47	wel	$7^2 - 2 \cdot 1^2$
53	geen	

Het is niet lastig om aan te tonen dat voor priemgetallen 3, 5, 11, 13, 19, 29, 37, 43, 47 en 53 er inderdaad geen oplossing bestaat voor het hierboven beschreven probleem.

Veel interessante Diophantische problemen kunnen worden aangepakt door in een handige uitbreiding van de natuurlijke getallen te gaan redeneren. Voor het bovenstaande probleem is de verzameling $\mathbb{Z}[\sqrt{2}]$ van alle elementen van de vorm $a + \sqrt{2} \cdot b$ met a en b gehele getallen een handige uitbreiding. De term $x^2 - 2 \cdot y^2$ kan met coëfficiënt $\sqrt{2}$ uit de verzameling $\mathbb{Z}[\sqrt{2}]$ worden geschreven als een product, namelijk $(x - \sqrt{2} \cdot y) \cdot (x + \sqrt{2} \cdot y)$. Dit betekent: als een priemgetal p te schrijven is als $x^2 - 2 \cdot y^2$, dan is p geen priemgetal meer in $\mathbb{Z}[\sqrt{2}]$. Bijvoorbeeld:

$$\begin{aligned} 2 &= \sqrt{2} \cdot \sqrt{2} \\ 7 &= (5 - \sqrt{2} \cdot 3) \cdot (5 + \sqrt{2} \cdot 3) \\ 17 &= (7 - \sqrt{2} \cdot 4) \cdot (7 + \sqrt{2} \cdot 4). \end{aligned}$$

De getallen $\sqrt{2}$, $(5 - \sqrt{2} \cdot 3)$, $(5 + \sqrt{2} \cdot 3)$, $(7 - \sqrt{2} \cdot 4)$ en $(7 + \sqrt{2} \cdot 4)$ zijn voorbeelden van priemgetallen in $\mathbb{Z}[\sqrt{2}]$. Tevens geldt: als een priemgetal p ook in $\mathbb{Z}[\sqrt{2}]$ een priemgetal blijft, dan is p niet te schrijven als $x^2 - 2 \cdot y^2$. Bijvoorbeeld: 3, 5 en 11 zijn priemgetallen in $\mathbb{Z}[\sqrt{2}]$.

Klassenlichamentheorie vertelt direct of een priemgetal p in de verzameling $\mathbb{Z}[\sqrt{2}]$ een priemgetal blijft. De theorie impliceert namelijk: een priemgetal p blijft alleen een priemgetal in $\mathbb{Z}[\sqrt{2}]$ als $p - 3$ of $p - 5$ deelbaar is door 8. Hiermee is het bovenstaande Diophantische probleem in essentie opgelost (we gebruiken namelijk ook dat in de verzameling $\mathbb{Z}[\sqrt{2}]$ elk getal op een unieke manier te schrijven is als product van priemgetallen). De volgende tabel geeft een overzicht.

p	wel of geen oplossing?	p priemgetal in $\mathbb{Z}[\sqrt{2}]$?	8 deelt $p-3$ of $p-5$?
2	wel	nee	nee
3	geen	ja	ja
5	geen	ja	ja
7	wel	nee	nee
11	geen	ja	ja
13	geen	ja	ja
17	wel	nee	nee
19	geen	ja	ja
23	wel	nee	nee
29	geen	ja	ja
31	wel	nee	nee
37	geen	ja	ja
41	wel	nee	nee
43	geen	ja	ja
47	wel	nee	nee
53	geen	ja	ja

De uitbreiding van de natuurlijke getallen naar $\mathbb{Z}[\sqrt{2}]$ komt van een zogenaamde abelse uitbreiding van getallenlichamen. Klassenlichamentheorie geeft voor elke abelse uitbreiding van getallenlichamen op soortgelijke wijze als in ons voorbeeld aan hoe de priemgetallen zich in de uitbreiding gedragen.

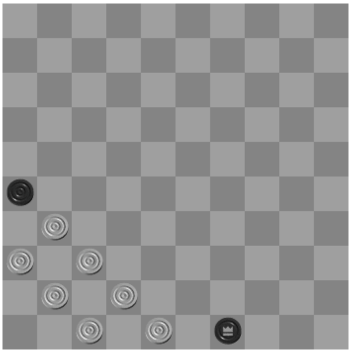
Bewijsmethode

In dit proefschrift wordt Lehmer's vraag vertaald naar een probleem dat met behulp van de klassenlichamentheorie kan worden aangepakt. Op deze manier zijn de resultaten in dit proefschrift komend van Lehmer's vraag bewezen.

Aangezien klassenlichamentheorie een diepgaande moderne theorie is waar vele grote wiskundigen aan hebben gewerkt, zal het hoogstwaarschijnlijk ondoenlijk zijn om met elementaire wiskunde deze resultaten te bewijzen.

Curriculum Vitae

Bastiaan Johannes Hendrikus Jansen werd geboren op 4 maart 1977 te Gouda. Op zesjarige leeftijd verdiende hij zo nu en dan een gulden in het dorpscafé van Haastrecht door zo snel mogelijk de tafel van zeven op te noemen. In datzelfde jaar leerde hij dammen. Samen met zijn vader loste hij elke zaterdagmiddag het dampropleem in de zaterdageditie van de Goudsche Courant op. De enige uitzondering is het onderstaande probleem dat hem altijd is bijgebleven. Zijn vader loste dit probleem pas zaterdagavond op en hij maakte Bas wakker om de oplossing te laten zien.



Wit speelt en wint.

Van 1989 tot 1993 bezocht Bas het atheneum van het St.-Antoniuscollege te Gouda, waar hij in het eerste jaar schoolschaakkampioen werd. In 1994 speelde hij remise in een simultaan tegen schaakgrootmeester John van der Wiel. In 1996 behaalde hij het theoretische gedeelte van de Lange Opleiding Medische Laboratoriumtechniek aan Het Utrecht College. Het jaar daarop slaagde hij voor zijn propedeuse Biologie en Medisch Laboratoriumonderzoek aan de Hogeschool van Utrecht. Daarna begon hij zijn studie wiskunde aan de Universiteit van Utrecht. Onder begeleiding van Frits Beukers en Bart de Smit studeerde hij in 2002 af met zijn scriptie getiteld 'Mersenne primes of the form $x^2 + n \cdot y^2$'. In 2002 startte hij als aio aan de Universiteit van Leiden met een onderzoek onder begeleiding van Hendrik Lenstra en Bart de Smit. Het eindproduct van het onderzoek is dit proefschrift.

Vanaf 2006 is Bas actief in het middelbaar onderwijs. Hij werkte als auteur bij Netwerk en hij gaf les op het Boerhaave College te Leiden. Sinds 2007 tot heden is hij docent wiskunde bij het vavo te Gouda. Daarnaast werkt hij vanaf augustus 2012 als docent bij de lerarenopleiding wiskunde van Hogeschool Utrecht. In 2012 behaalde hij zijn eerstegraads lesbevoegdheid aan de Vrije Universiteit te Amsterdam. Tevens schrijft hij een eigen lesmethode voor het schoolvak wiskunde D.