Mersenne primes and class field theory

Jansen, B.J.H.

Author: Jansen, Bas
Title: Mersenne primes and class field theory
Date: 2012-12-18

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

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. $\square$

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 $L = \mathbb{Q}(\sqrt[m]{2})$. $\square$

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 $L = \mathbb{Q}(\sqrt[2n]{2})$. $\square$

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 $[E \cap K : \mathbb{Q}(\sqrt[n]{2})] \leq 2$. $\square$

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.

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

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 $\mathrm{i} \notin EK$. $\square$

Proof of Proposition 3.8. Suppose for a contradiction that -1 is a square in E^*. Define the subgroup H of K^* by $H = H_n = \langle \alpha_1, \ldots, \alpha_n \rangle$. 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^*. $\square$

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 $s \notin \mathcal{S}$. $\square$

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. $\square$

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

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

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. $\square$