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 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

$$\begin{array}{ccccc} & & L_s & & \\ & \diagup & & \diagdown & \\ L'_s & & & & K''_s \\ & \diagdown & & \diagup & \\ & & K'_s & & \\ & \diagup & & & \\ K_s & & & & \end{array}$$

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 $[L_s : \mathbb{Q}_s''] \le 8$. Hence ω generates $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$, so $\mathrm{Gal}(L_s/\mathbb{Q}_s'')$ is cyclic of order 8. $\square$

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 $[\mathbb{Q}_s'' \cap K : \mathbb{Q}(s)] \le 2$. By definition $K_s = L_s \cap K$, therefore $[K_s : \mathbb{Q}(s)] = [\mathbb{Q}_s'' \cap K : \mathbb{Q}(s)] \le 2$ 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 $K_s'' = \mathbb{Q}_s''$. $\square$

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 $[L_s' : K_s'] \ge 8$ and $[L_s'' : K_s] \ge 8$. 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 $8 = [L_s : K_s''] \le [L_s' : L_s' \cap K_s''] \le [L_s' : K_s'] = 8$, so $L_s' \cap K_s'' = K_s'$. Similarly we have $8 = [L_s' : K_s'] \le [L_s'' : L_s'' \cap K_s'] \le [L_s'' : K_s] = 8$, so $L_s'' \cap K_s' = K_s$. $\square$

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. $\square$

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 $\sigma(\alpha) = \alpha^{\pm 1}$. 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 $\mathrm{Gal}(L'_s/K'_s)$. $\square$

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. $\square$

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. $\square$