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

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.

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

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

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:*

(i) $[T : K_{s,t}] = 1$ *and* $[E : E'] = 8$,
(ii) $[T : K_{s,t}] = 2$ *and* $[E : E'] = 2$ *or* 4.

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 mod 8 Proposition 8.6 implies $[\sigma] = [\sigma^i]$. Therefore in the case $i \equiv 1$ or 7 mod 8 Lemma 8.17 holds.

Let $i \equiv 3$ or 5 mod 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. □