Mersenne primes and class field theory

Jansen, B.J.H.

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 $\mathcal{E}=\{p\in\mathcal{E}_{2012}:3\le p\le 20000\}$. 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	

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

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 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 $\tau_{\text{ab}}(x)(\zeta_{q^t}) \neq \zeta_{q^t}$.*

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

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 $m' = \text{lcm}(m, w)$. 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 $\tau_{\text{ab}}(x)(\zeta_{q^t}) \neq \zeta_{q^t}$. □

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 $\tau_{\text{ab}}(x)(\zeta_{q^{t_q}}) \neq \zeta_{q^{t_q}}$.*

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 $\to \text{Mer}_L$ and $W \to W_L$ are surjective. Hence we have $\text{Mer}_L = W_L$.

(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 $\sigma \in \text{Mer}_L$. Hence ϕ is an element of Mer_L.

(ii) $\Rightarrow$ (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.

$$\begin{tikzcd}
 & & \overline{\mathbb{Q}} \arrow[dl, no head] \arrow[dr, no head] \arrow[ddrr, bend left=60, no head, "\tilde{\sigma}\in T"] & & \\
 & L' \arrow[dl, no head] \arrow[dr, no head] & & K^{\mathrm{ab}} \arrow[dl, no head] \arrow[dr, no head] \arrow[dr, bend left, no head, "\tau(x)"] & \\
L \arrow[dr, no head] \arrow[ddrr, bend right=60, no head, "\sigma\in T_L"'] & & L'\cap K^{\mathrm{ab}} \arrow[dl, no head] \arrow[dr, no head] & & K \arrow[dl, no head] \\
 & L\cap K^{\mathrm{ab}} \arrow[dr, no head] & & L'\cap K \arrow[dl, no head] & \\
 & & \mathbb{Q}(\sqrt[n]{2}) \arrow[d, no head] & & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

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. □