# Galois Theory of the Polynomials $f_n(x)$, Pratt Trees, and Mersenne Primes

Orges Leka

April 15, 2026

**Abstract**

We rewrite the Galois–Pratt part of *Polynomials and Perfect Numbers* as a self-contained note. The family $f_n(x)$ is defined directly and naturally, the irreducibility of $f_p(x)$ for primes $p$ is proved in detail using the MathOverflow argument based on a root-location criterion, and the subsequent Galois theory is reorganised around the sets

$$\Omega_{p,q} = \{f_q(\alpha) : f_p(\alpha) = 0\}, \qquad q \mid (p-1).$$

We then explain how the stabilisers of these orbits produce intermediate fields inside the splitting field of $f_p$, and how for Mersenne primes this data is naturally governed by the base-2 Pratt tree. Selected examples are worked out explicitly.

## Contents

# 1 The recursive family $f_n(x)$

We begin by defining the polynomials themselves.

**Definition 1.1** (The polynomials $f_n$)**.** Set

$$f_1(x) := 1, \qquad f_2(x) := x.$$

For an odd prime $p$ define recursively

$$f_p(x) := 1 + \prod_{q|(p-1)} f_q(x)^{v_q(p-1)}, \tag{1}$$

where the product runs over the prime divisors $q$ of $p-1$, and $v_q$ denotes $q$-adic valuation. For an arbitrary positive integer

$$n = \prod_p p^{v_p(n)}$$

we then define

$$f_n(x) := \prod_{p|n} f_p(x)^{v_p(n)}. \tag{2}$$

Thus the family is determined first on primes and then extended multiplicatively to all positive integers.

**Proposition 1.2** (Basic identities)**.** *For all positive integers $m, n$ we have:*

(1) $f_{mn}(x) = f_m(x) f_n(x)$*;*

(2) $f_n(2) = n$*;*

(3) *if $n$ is squarefree, then $f_n(x) = \prod_{p|n} f_p(x)$ is a product of pairwise distinct prime-index factors.*

*Proof.* For (1), write

$$m = \prod_p p^{a_p}, \qquad n = \prod_p p^{b_p}.$$

Then by definition,

$$f_m(x) = \prod_p f_p(x)^{a_p}, \qquad f_n(x) = \prod_p f_p(x)^{b_p}.$$

Multiplying gives

$$f_m(x) f_n(x) = \prod_p f_p(x)^{a_p + b_p} = f_{mn}(x),$$

since $v_p(mn) = a_p + b_p$.

For (2) we argue by induction on $n$. The claim is clear for $n = 1, 2$. Now let $p$ be an odd prime. Using (1) and the induction hypothesis for the primes dividing $p-1$, we obtain

$$f_p(2) = 1 + \prod_{q|(p-1)} f_q(2)^{v_q(p-1)} = 1 + \prod_{q|(p-1)} q^{v_q(p-1)} = 1 + (p-1) = p.$$

For general $n$, formula (2) and the prime case imply

$$f_n(2) = \prod_{p|n} f_p(2)^{v_p(n)} = \prod_{p|n} p^{v_p(n)} = n.$$

For (3), if $n$ is squarefree then every $v_p(n)$ is 0 or 1, so (2) becomes

$$f_n(x) = \prod_{p|n} f_p(x).$$

The factors are indexed by distinct primes, hence they are pairwise distinct as polynomials because evaluating at $x = 2$ gives distinct prime values by part (2). □

**Proposition 1.3** (Polynomial radical)**.** *For every $n \geq 1$,*

$$\mathrm{rad}(f_n(x)) = \prod_{p|n} f_p(x) = f_{\mathrm{rad}(n)}(x).$$

*Proof.* Write $n = \prod_p p^{a_p}$. Then

$$f_n(x) = \prod_{p|n} f_p(x)^{a_p}.$$

The distinct irreducible factors of this product, once we know the prime-index polynomials $f_p$ are irreducible and pairwise distinct, are exactly the polynomials $f_p(x)$ with $p \mid n$. Therefore the polynomial radical is obtained by reducing each exponent $a_p$ to 1, namely

$$\mathrm{rad}(f_n(x)) = \prod_{p|n} f_p(x).$$

On the other hand, by definition of $f_m$ for squarefree $m$,

$$f_{\mathrm{rad}(n)}(x) = \prod_{p|n} f_p(x),$$

which is the same expression. □

## 2 Irreducibility of $f_p(x)$ for prime $p$

The crucial input is the irreducibility of $f_p$ for every prime $p$. We give a complete proof based on the MathOverflow argument suggested by Jonathan Love, with the root-location criterion replacing the original stronger but false condition $|\theta - 2| > 1$ for all roots.

**Lemma 2.1** (A left-half-plane criterion)**.** *Let $g(x) \in \mathbb{Z}[x]$ be monic with constant term $\pm 1$. Suppose every root $\theta$ of $g$ satisfies*

$$\mathrm{Re}(\theta) < -\frac{1}{2}.$$

*Then either $g(x)$ is irreducible or else $g(x) = (x+1)^m$ for some $m \geq 1$. More precisely: every nonconstant irreducible factor of $g$ is equal to $x + 1$.*

*Proof.* Let $h(x) \in \mathbb{Z}[x]$ be a nonconstant irreducible factor of $g(x)$. Since $g$ is monic with constant term $\pm 1$, Gauss' lemma implies that $h$ is also monic and its constant term is $\pm 1$. Let $\theta_1, \ldots, \theta_m$ be the roots of $h$ in $\mathbb{C}$. They are among the roots of $g$, hence $\mathrm{Re}(\theta_j) < -\frac{1}{2}$ for all $j$.

For any complex number $\theta = a + bi$ with $a < -\frac{1}{2}$ we have

$$|\theta + 1|^2 = (a+1)^2 + b^2 < a^2 + b^2 = |\theta|^2,$$

so $|\theta+1|<|\theta|$. Applying this to each root $\theta_j$ gives

$$|h(-1)|=\prod_{j=1}^{m}|1+\theta_j|<\prod_{j=1}^{m}|\theta_j|=|h(0)|.$$

Because $h(0)=\pm 1$, the right-hand side equals 1. Therefore

$$|h(-1)|<1.$$

But $h(-1)$ is an integer, so the only possibility is $h(-1)=0$. Hence $x+1$ divides $h(x)$. Since $h$ is irreducible, we must have $h(x)=x+1$.

This proves the stated refinement: every nonconstant irreducible factor of $g$ is $x+1$. Consequently, if $g$ is reducible then it is a power of $x+1$. □

**Lemma 2.2** (Root location for the prime-index polynomials)**.** *Let $p$ be a prime and let $z\in\mathbb{C}$ satisfy*

$$\mathrm{Re}(z)\geq\frac{3}{2}.$$

*Then*

$$|f_p(z)|>2.$$

*In particular, every root $\theta$ of $f_p(x)$ satisfies*

$$\mathrm{Re}(\theta)<\frac{3}{2}.$$

*Proof.* We prove the first statement by induction on the prime $p$.

For $p=2$, one has $f_2(z)=z$, so $|f_2(z)|=|z|\geq\mathrm{Re}(z)\geq\frac{3}{2}$. The final strict inequality $|f_p(z)|>2$ is only needed later for odd primes, so the case $p=2$ serves merely as a base value appearing in the recursion.

For $p=3$, we have $f_3(x)=x+1$, hence

$$|f_3(z)|=|z+1|\geq\mathrm{Re}(z+1)=\mathrm{Re}(z)+1\geq\frac{5}{2}>2.$$

For $p=5$, one has $f_5(x)=x^2+1$. Writing $z=a+bi$ with $a\geq\frac{3}{2}$, we get

$$|z^2+1|^2=(a^2-b^2+1)^2+(2ab)^2=(a^2+(b-1)^2)(a^2+(b+1)^2)\geq a^4.$$

Hence

$$|f_5(z)|=|z^2+1|\geq a^2\geq\left(\frac{3}{2}\right)^2>2.$$

Now let $p\geq 7$ be prime and assume the claim known for every prime divisor of $p-1$. From the recursive definition,

$$f_p(z)=1+\prod_{q|(p-1)}f_q(z)^{v_q(p-1)}.$$

Therefore the reverse triangle inequality gives

$$|f_p(z)|\geq\prod_{q|(p-1)}|f_q(z)|^{v_q(p-1)}-1.$$

We distinguish two cases.

*Case 1: $p-1$ has an odd prime divisor $q$.* Then 2 and $q$ both divide $p-1$. By the induction hypothesis for the odd prime $q$, we have $|f_q(z)| > 2$, while $|f_2(z)| = |z| \geq \frac{3}{2}$. Since all other factors have modulus at least 1, we obtain

$$|f_p(z)| \geq |f_2(z)|\,|f_q(z)| - 1 > \frac{3}{2} \cdot 2 - 1 = 2.$$

*Case 2: $p-1$ is a power of 2.* Then $p-1 = 2^k$ with $k \geq 3$ because $p \geq 7$. Hence

$$f_p(z) = 1 + f_2(z)^k = 1 + z^k,$$

and therefore

$$|f_p(z)| \geq |z|^k - 1 \geq \left(\frac{3}{2}\right)^3 - 1 = \frac{27}{8} - 1 > 2.$$

This completes the induction and proves $|f_p(z)| > 2$ for all odd primes $p$ and all $z$ with real part at least $\frac{3}{2}$. If $\theta$ were a root of $f_p$ with $\mathrm{Re}(\theta) \geq \frac{3}{2}$, then the first part would give $|f_p(\theta)| > 2$, contradicting $f_p(\theta) = 0$. Thus every root satisfies $\mathrm{Re}(\theta) < \frac{3}{2}$. □

**Theorem 2.3** (Irreducibility of $f_p$)**.** *For every prime $p$, the polynomial $f_p(x)$ is irreducible in $\mathbb{Z}[x]$.*

*Proof.* The case $p = 2$ is clear because $f_2(x) = x$.

Now let $p$ be odd, and suppose for contradiction that $f_p(x)$ is reducible in $\mathbb{Z}[x]$. Then we may write

$$f_p(x) = u(x)v(x)$$

with $u, v \in \mathbb{Z}[x]$ nonconstant. Evaluating at $x = 2$ and using Proposition 1.2(2), we get

$$p = f_p(2) = u(2)v(2).$$

Since $p$ is prime, one of the two integers $u(2), v(2)$ must have absolute value 1. Replacing $u$ by that factor, we may assume

$$u(2) = \pm 1.$$

Define

$$g(x) := u(x+2) \in \mathbb{Z}[x].$$

Then $g$ is monic up to sign; multiplying $u$ by $-1$ if necessary does not change reducibility, so we may assume $g$ is monic. Moreover,

$$g(0) = u(2) = \pm 1.$$

Thus $g$ satisfies the hypotheses of Lemma 2.1 once we know where its roots lie.

If $\eta$ is a root of $g$, then $\eta + 2$ is a root of $u$, hence also a root of $f_p$. By Lemma 2.2, every root $\theta$ of $f_p$ satisfies $\mathrm{Re}(\theta) < \frac{3}{2}$. Therefore every root $\eta = \theta - 2$ of $g$ satisfies

$$\mathrm{Re}(\eta) < -\frac{1}{2}.$$

By Lemma 2.1, every irreducible factor of $g$ is equal to $x + 1$. Since $g$ itself is reducible, this forces

$$g(x) = (x+1)^m$$

for some $m \geq 1$. Translating back,

$$u(x) = (x-1)^m.$$

So $u(1) = 0$.

But for every $n \geq 1$ the polynomial $f_n(x)$ has nonnegative coefficients, and in fact positive constant term 1 when $n$ is odd. In particular, for odd prime $p$ we have $f_p(1) > 0$ by the recursive definition. Since $u$ divides $f_p$, the identity $u(1) = 0$ would imply $f_p(1) = 0$, contradiction. Therefore $f_p$ is irreducible. □

**Corollary 2.4** (Prime detection by irreducibility)**.** *For every $n \geq 1$, the polynomial $f_n(x)$ is irreducible if and only if $n$ is prime.*

*Proof.* If $n = p$ is prime, this is exactly Theorem 2.3. Conversely, if $n$ is composite then (2) expresses $f_n$ as a nontrivial product of lower-index prime polynomials, so it is reducible. □

# 3 Splitting fields and elementary Galois theory

For each prime $p$, let

$$K_p := \mathrm{Spl}(f_p/\mathbb{Q}), \qquad G_p := \mathrm{Gal}(K_p/\mathbb{Q}),$$

and let $R_p \subset K_p$ be the set of roots of $f_p$.

**Lemma 3.1** (Transitivity on the roots)**.** *For every prime $p$, the group $G_p$ acts transitively on $R_p$.*

*Proof.* By Theorem 2.3, the polynomial $f_p$ is irreducible over $\mathbb{Q}$. Hence any two of its roots are Galois-conjugate over $\mathbb{Q}$. Equivalently, for any $\alpha, \beta \in R_p$ there exists $\sigma \in G_p$ such that $\sigma(\alpha) = \beta$. This is exactly transitivity. □

**Proposition 3.2** (Field inclusions from divisibility)**.** *Let $m$ be squarefree and let $d \mid m$. Write*

$$K_m := \mathrm{Spl}(f_m/\mathbb{Q}), \qquad K_d := \mathrm{Spl}(f_d/\mathbb{Q}).$$

*Then $K_d \subseteq K_m$. Consequently the restriction map*

$$\mathrm{res} : \mathrm{Gal}(K_m/\mathbb{Q}) \to \mathrm{Gal}(K_d/\mathbb{Q})$$

*is surjective with kernel* $\mathrm{Gal}(K_m/K_d)$.

*Proof.* Since $m$ is squarefree, we have

$$f_m(x) = \prod_{p \mid m} f_p(x).$$

If $d \mid m$, then

$$f_d(x) = \prod_{p \mid d} f_p(x)$$

is a factor of $f_m(x)$. Hence every root of $f_d$ is also a root of $f_m$. Therefore the splitting field of $f_d$ is contained in the splitting field of $f_m$, i.e. $K_d \subseteq K_m$.

Because $K_m/\mathbb{Q}$ is Galois and $K_d$ is an intermediate field, the fundamental theorem of Galois theory implies that restriction from $K_m$ to $K_d$ is surjective and its kernel is precisely the subgroup fixing $K_d$, namely $\mathrm{Gal}(K_m/K_d)$. □

## 4 The values $f_q(\alpha)$ for $q \mid (p-1)$

Fix a prime $p$, and let $\alpha \in R_p$ be any root of $f_p$. For each prime divisor $q \mid (p-1)$ we study the value $f_q(\alpha)$. The recursive identity for $f_p$ yields the fundamental relation

$$f_p(\alpha) = 0 \iff 1 + f_{p-1}(\alpha) = 0 \iff \prod_{r|(p-1)} f_r(\alpha)^{v_r(p-1)} = -1. \tag{3}$$

**Definition 4.1** (The sets $\Omega_{p,q}$)**.** For a prime divisor $q \mid (p-1)$ define

$$\Omega_{p,q} := \{f_q(\beta) : \beta \in R_p\} \subset K_p.$$

We also set

$$\Omega_p := \bigcup_{q|(p-1)} \Omega_{p,q}.$$

**Proposition 4.2** (Galois action on $\Omega_p$)**.** *The group $G_p$ acts on $\Omega_p$ by*

$$\sigma \cdot f_q(\beta) := f_q(\sigma(\beta)), \qquad \sigma \in G_p,\ \beta \in R_p,\ q \mid (p-1).$$

*For each fixed prime $q \mid (p-1)$, the subset $\Omega_{p,q}$ is stable under this action.*

*Proof.* We first check that the formula is well defined. Suppose $f_q(\beta_1) = f_q(\beta_2)$ for two roots $\beta_1, \beta_2 \in R_p$. Since $\sigma$ fixes the rational coefficients of $f_q$, we have

$$f_q(\sigma(\beta_1)) = \sigma(f_q(\beta_1)) = \sigma(f_q(\beta_2)) = f_q(\sigma(\beta_2)).$$

Hence the image depends only on the element of $\Omega_p$, not on the chosen representative.

Next let $x \in \Omega_{p,q}$. Then $x = f_q(\beta)$ for some $\beta \in R_p$, and so

$$\sigma(x) = \sigma(f_q(\beta)) = f_q(\sigma(\beta)).$$

Because $\sigma(\beta)$ is again a root of $f_p$, the right-hand side belongs to $\Omega_{p,q}$. Thus each $\Omega_{p,q}$ is $G_p$-stable. □

**Corollary 4.3** (Orbit description)**.** *Fix a root $\alpha \in R_p$ and set*

$$\beta_q := f_q(\alpha).$$

*Then for every prime divisor $q \mid (p-1)$,*

$$\Omega_{p,q} = G_p \cdot \beta_q = \{\sigma(\beta_q) : \sigma \in G_p\}.$$

*In particular, $\Omega_{p,q}$ is a single $G_p$-orbit.*

*Proof.* By Lemma 3.1, every root $\beta \in R_p$ can be written as $\beta = \sigma(\alpha)$ for some $\sigma \in G_p$. Therefore

$$\Omega_{p,q} = \{f_q(\beta) : \beta \in R_p\} = \{f_q(\sigma(\alpha)) : \sigma \in G_p\} = \{\sigma(f_q(\alpha)) : \sigma \in G_p\} = G_p \cdot \beta_q.$$

So $\Omega_{p,q}$ is exactly the orbit of $\beta_q$. □

**Lemma 4.4** (Orbit size and degree)**.** *Let $d = \deg f_p$. For every prime divisor $q \mid (p-1)$, the orbit size $|\Omega_{p,q}|$ divides $d$. More precisely, if $L_{p,q} := \mathbb{Q}(\beta_q)$, then*

$$[L_{p,q} : \mathbb{Q}] = |\Omega_{p,q}| \mid d.$$

*Proof.* Since $\beta_q = f_q(\alpha)$ and $f_q \in \mathbb{Q}[x]$, we have $\beta_q \in \mathbb{Q}(\alpha)$. Now $f_p$ is irreducible of degree $d$, so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = d.$$

Because $\beta_q \in \mathbb{Q}(\alpha)$, the tower law gives

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : L_{p,q}][L_{p,q} : \mathbb{Q}],$$

whence $[L_{p,q} : \mathbb{Q}] \mid d$.

It remains to show $[L_{p,q} : \mathbb{Q}] = |\Omega_{p,q}|$. The conjugates of $\beta_q$ over $\mathbb{Q}$ are precisely the values $\sigma(\beta_q)$ with $\sigma \in G_p$, i.e. precisely the elements of the orbit $G_p \cdot \beta_q = \Omega_{p,q}$. Hence the minimal polynomial of $\beta_q$ over $\mathbb{Q}$ has exactly $|\Omega_{p,q}|$ distinct roots, and therefore

$$[L_{p,q} : \mathbb{Q}] = \deg \min(\beta_q, \mathbb{Q}) = |\Omega_{p,q}|.$$

Combining the two parts gives the result. □

**Definition 4.5** (Stabilisers and intermediate fields)**.** For $q \mid (p-1)$ define

$$H_q := \mathrm{Stab}_{G_p}(\beta_q) = \{\sigma \in G_p : \sigma(\beta_q) = \beta_q\}$$

and

$$L_{p,q} := \mathbb{Q}(\beta_q).$$

**Proposition 4.6** (Orbit-stabiliser and Galois correspondence)**.** *For every prime divisor $q \mid (p-1)$,*

$$|\Omega_{p,q}| = [G_p : H_q] = [L_{p,q} : \mathbb{Q}],$$

*and the fixed field of $H_q$ inside $K_p$ is exactly $L_{p,q}$.*

*Proof.* The equality $|\Omega_{p,q}| = [G_p : H_q]$ is the ordinary orbit-stabiliser theorem applied to the action of $G_p$ on $\Omega_{p,q}$.

We next show that the fixed field of $H_q$ is $L_{p,q}$. Every element of $H_q$ fixes $\beta_q$, hence fixes the field $\mathbb{Q}(\beta_q) = L_{p,q}$. Therefore $L_{p,q} \subseteq K_p^{H_q}$.

Conversely, the subgroup fixing $L_{p,q}$ pointwise is $\mathrm{Gal}(K_p/L_{p,q})$. Since an automorphism fixes $L_{p,q}$ if and only if it fixes the generator $\beta_q$, we have

$$\mathrm{Gal}(K_p/L_{p,q}) = H_q.$$

By the fundamental theorem of Galois theory, the corresponding fixed field is exactly $L_{p,q}$. Finally,

$$[L_{p,q} : \mathbb{Q}] = [G_p : H_q],$$

again by the fundamental theorem, and combining with orbit-stabiliser yields the claimed chain of equalities. □

**Lemma 4.7** (When two orbits coincide)**.** *Let $q, r \mid (p-1)$ be primes. Then the following are equivalent:*

(1) $\Omega_{p,q} = \Omega_{p,r}$*;*

(2) $\beta_q$ *and* $\beta_r$ *are Galois-conjugate under* $G_p$*;*

(3) $H_q$ *and* $H_r$ *are conjugate subgroups of* $G_p$*.*

*Proof.* By Corollary 4.3,

$$\Omega_{p,q} = G_p \cdot \beta_q, \qquad \Omega_{p,r} = G_p \cdot \beta_r.$$

Therefore (1) holds if and only if $\beta_r \in G_p \cdot \beta_q$, i.e. if and only if there exists $\sigma \in G_p$ such that $\sigma(\beta_q) = \beta_r$. This proves the equivalence of (1) and (2).

Now assume (2) and choose $\sigma \in G_p$ with $\sigma(\beta_q) = \beta_r$. For $\tau \in H_q$ we have

$$(\sigma\tau\sigma^{-1})(\beta_r) = \sigma\tau(\beta_q) = \sigma(\beta_q) = \beta_r,$$

so $\sigma H_q \sigma^{-1} \subseteq H_r$. Applying the same argument to $\sigma^{-1}$ gives the reverse inclusion. Thus

$$H_r = \sigma H_q \sigma^{-1},$$

which is (3).

Conversely, suppose (3) holds, say $H_r = \sigma H_q \sigma^{-1}$. Then $H_r$ fixes both $\beta_r$ and $\sigma(\beta_q)$. These two elements lie in the same transitive $G_p$-set, and in such a set the stabiliser determines the point up to the action of $G_p$. Equivalently, by orbit-stabiliser, two points have conjugate stabilisers exactly when they lie in the same orbit. Hence $\sigma(\beta_q)$ and $\beta_r$ lie in the same orbit, so (2) holds. □

# 5 Worked examples

The following examples are not needed for the abstract theory, but they show concretely how the sets $\Omega_{p,q}$ and fields $L_{p,q}$ behave.

**Example 5.1** (The prime $p = 11$)**.** We have

$$f_{11}(x) = x^3 + x + 1.$$

Its discriminant is $-31$, which is not a square, so the Galois group of its splitting field is $S_3$. The prime divisors of $11 - 1 = 10$ are 2 and 5.

Take a root $\alpha$ of $f_{11}$. Then

$$\beta_2 = f_2(\alpha) = \alpha, \qquad \beta_5 = f_5(\alpha) = \alpha^2 + 1.$$

A direct elimination computation gives

$$\min(\beta_2, \mathbb{Q}) = x^3 + x + 1, \qquad \min(\beta_5, \mathbb{Q}) = x^3 - x^2 - 1.$$

Hence

$$[L_{11,2} : \mathbb{Q}] = [L_{11,5} : \mathbb{Q}] = 3,$$

and both $\Omega_{11,2}$ and $\Omega_{11,5}$ have size 3.

**Example 5.2** (The prime $p = 31$)**.** Here

$$f_{31}(x) = x^4 + x^3 + x^2 + x + 1 = \Phi_5(x).$$

Therefore its splitting field is the cyclotomic field $\mathbb{Q}(\zeta_5)$, and

$$G_{31} \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4.$$

The prime divisors of $31 - 1 = 30$ are $2, 3, 5$. For a root $\alpha$ of $f_{31}$ one finds

$$\min(\alpha + 1, \mathbb{Q}) = x^4 - 3x^3 + 4x^2 - 2x + 1,$$

and exactly the same minimal polynomial for $\alpha^2 + 1 = f_5(\alpha)$. Thus

$$\Omega_{31,3} = \Omega_{31,5},$$

which shows that different primes dividing $p - 1$ need not produce different orbits.

**Example 5.3** (The prime $p = 127$)**.** The polynomial is

$$f_{127}(x) = x^5 + 3x^4 + 4x^3 + 3x^2 + x + 1.$$

Its discriminant is $47^2$, hence a square. A direct computation of the Galois group shows

$$G_{127} \cong D_5.$$

The prime divisors of $127 - 1 = 126$ are $2, 3, 7$. For a root $\alpha$ of $f_{127}$ one computes

$$\min(\alpha, \mathbb{Q}) = x^5 + 3x^4 + 4x^3 + 3x^2 + x + 1,$$

$$\min(\alpha + 1, \mathbb{Q}) = x^5 - 2x^4 + 2x^3 - x^2 + 1,$$

$$\min(\alpha^2 + \alpha + 1, \mathbb{Q}) = x^5 - 3x^4 + 3x^3 - 2x^2 + x - 1.$$

Hence the three fields $L_{127,2}, L_{127,3}, L_{127,7}$ are distinct quintic subfields of the dihedral splitting field.

# 6 Mersenne primes and their Galois–Pratt profile

In this section we specialise the general discussion to Mersenne primes and describe the interaction between the Galois group $G_q = \mathrm{Gal}(K_q/\mathbb{Q})$ and the sets

$$\Omega_{q,r} := \{\, f_r(\alpha) : \alpha \in R_q \,\} \subset K_q$$

associated to the prime divisors $r \mid (q - 1)$, where $q$ is a Mersenne prime and $R_q$ is the set of roots of $f_q(x)$ in a fixed algebraic closure.

## 6.1 The structure of $q - 1$ and the Pratt tree

Let

$$q = 2^p - 1$$

be a Mersenne prime, with $p$ prime. Then

$$q \equiv 3 \pmod 4,$$

so $\nu_2(q - 1) = 1$ and

$$q - 1 = 2 \cdot (2^{p-1} - 1).$$

In particular, every odd prime divisor $r \mid (q - 1)$ divides $2^{p-1} - 1$. Equivalently, every such $r$ satisfies

$$\mathrm{ord}_r(2) \mid (p - 1).$$

Consider the Pratt tree of $q$ with base 2. The root is $q$ and its children are precisely the prime divisors of $q - 1$, i.e.

$$\{2\} \ \cup \ \{\, r > 2 : r \mid 2^{p-1} - 1 \,\}.$$

For each such prime $r$ the tree continues via the prime divisors of $\mathrm{ord}_r(2)$, and so on. All levels of the tree are governed by multiplicative orders of 2 modulo the primes that appear.

Informally: the entire Pratt tree of a Mersenne prime $q = 2^p - 1$ is *based on* 2; every edge is controlled by the order of 2 in an appropriate multiplicative group $(\mathbb{Z}/r\mathbb{Z})^\times$.

### 6.2 The Galois group $G_q$ and the orbit $\Omega_{q,2}$

For each prime $q$ we have the irreducible polynomial $f_q(x) \in \mathbb{Z}[x]$, with

$$f_q(x) \text{ irreducible}, \qquad d := \deg f_q,$$

and let $K_q$ be its splitting field over $\mathbb{Q}$. We write

$$G_q := \mathrm{Gal}(K_q/\mathbb{Q}), \qquad R_q := \{\text{roots of } f_q \text{ in } \overline{\mathbb{Q}}\}.$$

Then $G_q$ acts transitively on $R_q$.

For the prime divisor $2 \mid (q-1)$ we have $f_2(x) = x$. Fix a root $\alpha \in R_q$ of $f_q$. Then

$$\beta_2 := f_2(\alpha) = \alpha,$$

and therefore

$$\Omega_{q,2} = \{f_2(\sigma(\alpha)) : \sigma \in G_q\} = \{\sigma(\alpha) : \sigma \in G_q\} = R_q.$$

Thus

$$|\Omega_{q,2}| = d = \deg f_q,$$

and the stabiliser

$$H_2 := \mathrm{Stab}_{G_q}(\beta_2) = \mathrm{Stab}_{G_q}(\alpha)$$

has index $d$ in $G_q$. In particular,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = d, \qquad G_q \text{ acts transitively of degree } d \text{ on } R_q.$$

For small Mersenne primes one finds, for example:

- $q = 3$: $f_3(x) = x + 1$, so $K_3 = \mathbb{Q}$ and $G_3$ is trivial.
- $q = 7$: $f_7(x) = x^2 + x + 1$, so $[K_7 : \mathbb{Q}] = 2$ and $|G_7| = 2$.
- $q = 31$: $f_{31}(x) = x^4 + x^3 + x^2 + x + 1$, so $[K_{31} : \mathbb{Q}] = 4$ and $G_{31} \cong C_4$.
- $q = 127$: $f_{127}(x) = x^5 + 3x^4 + 4x^3 + 3x^2 + x + 1$, so $[K_{127} : \mathbb{Q}] = 10$ and $G_{127} \cong D_5$ (a dihedral group of order 10).

Heuristically one expects that for large $q$ the groups $G_q$ are often "large" (frequently $S_d$ or $A_d$), but this is far from being proved.

### 6.3 Other divisors $r \mid (q-1)$ and their orbits $\Omega_{q,r}$

Now let $r \mid (q-1)$ be any prime divisor (including $r = 2$ if desired). Fix a root $\alpha \in R_q$ and define

$$\beta_r := f_r(\alpha) \in K_q.$$

We then consider:

- the Galois orbit
$$\Omega_{q,r} := \{\sigma(\beta_r) : \sigma \in G_q\} = G_q \cdot \beta_r \subset K_q,$$
- the stabiliser
$$H_r := \mathrm{Stab}_{G_q}(\beta_r) = \{\sigma \in G_q : \sigma(\beta_r) = \beta_r\},$$
- the intermediate field
$$L_{q,r} := \mathbb{Q}(\beta_r) = K_q^{H_r}.$$

By general Galois theory we have:

- $|\Omega_{q,r}| = [G_q : H_r] = [L_{q,r} : \mathbb{Q}]$,
- $\beta_r$ and $\beta_s$ are Galois-conjugate (i.e. lie in the same $G_q$-orbit) if and only if $H_r$ and $H_s$ are conjugate subgroups of $G_q$,
- the orbits $\Omega_{q,r}$ are either disjoint or identical (two distinct orbits never intersect partially),
- the union
$$\Omega_q := \bigcup_{r|(q-1)} \Omega_{q,r}$$
is a union of $G_q$-orbits, and all the structure is encoded in the family of stabilisers $\{H_r\}_{r|(q-1)}$.

For Mersenne primes $q = 2^p - 1$ the family $\{H_r\}_{r|(q-1)}$ is particularly rich, because:

- every odd $r \mid (q-1)$ divides $2^{p-1} - 1$,
- therefore $\mathrm{ord}_r(2) \mid (p-1)$,
- on the Pratt side this means that each such $r$ sits above a path built from the orders of 2 modulo successive primes,
- on the Galois side this translates into the fact that the various values $\beta_r = f_r(\alpha)$ are tied together by the same "base-2" recursive structure that defines the polynomials $f_n$, notably via the evaluation identity $f_n(2) = n$.

### 6.4 Typical phenomena seen in examples

Computations for small Mersenne primes (for instance in Sage) show the following patterns:

- For every Mersenne $q$, the orbit $\Omega_{q,2}$ is the full root set $R_q$ of $f_q$, i.e. the "largest" orbit of size $\deg f_q$.
- For other prime divisors $r \mid (q-1)$ one obtains additional orbits $\Omega_{q,r}$, often of smaller size (e.g. $3, 4, 5$), which correspond to proper intermediate fields $L_{q,r} \subsetneq \mathbb{Q}(\alpha)$.
- These orbits can exhibit various behaviours:
  - they may be pairwise disjoint (e.g. for $p = 11, 13, 19, \ldots$),
  - they may coincide for different primes $r$ (e.g. for $p = 31$, one finds $\Omega_{31,3} = \Omega_{31,5}$),
  - for larger $G_q$ more complicated patterns can arise, depending on the subgroup structure of $G_q$.

In particular, two distinct primes $r \neq s$ dividing $q - 1$ can yield the *same* orbit:

$$\Omega_{q,r} = \Omega_{q,s} \iff \beta_r, \beta_s \text{ are Galois-conjugate} \iff H_r, H_s \text{ are conjugate subgroups of } G_q.$$

Thus the naive expectation "different primes $r$ dividing $(q-1)$ give disjoint orbits $\Omega_{q,r}$" is, in general, *false*; the case $p = 31$ provides an explicit example.

### 6.5 Summary for Mersenne primes

We can summarise the situation for a Mersenne prime $q = 2^p - 1$ as follows:

1. The orbit $\Omega_{q,2}$ is always the full root set of $f_q(x)$, of size $\deg f_q$, and realises the basic transitive permutation representation of $G_q$.

2. Each prime divisor $r \mid (q-1)$ gives rise to an orbit $\Omega_{q,r}$ and a corresponding intermediate field
$$\mathbb{Q} \subseteq L_{q,r} \subseteq K_q,$$
with $[L_{q,r} : \mathbb{Q}] = |\Omega_{q,r}|$.

3. The family of stabilisers $\{H_r\}_{r|(q-1)}$, where $H_r = \mathrm{Stab}_{G_q}(\beta_r)$, acts as a "Galois shadow" of the Pratt tree of $q$:
   - conjugacy classes of $H_r$ correspond to Galois-conjugacy classes of the $\beta_r$;
   - distinct conjugacy classes of $H_r$ give rise to disjoint orbits $\Omega_{q,r}$;
   - identical orbits $\Omega_{q,r} = \Omega_{q,s}$ occur exactly when $H_r$ and $H_s$ are conjugate in $G_q$.

4. For Mersenne primes the arithmetic of the primes $r \mid (q-1)$ is strongly controlled by the powers of 2 (since each such $r$ divides $2^{p-1} - 1$), and the same base 2 appears in the defining properties of the polynomials $f_n$ via $f_n(2) = n$. This is why Mersenne primes form a particularly coherent class in this Galois–Pratt framework.

### 6.6 Extending to Mersenne numbers with composite exponents

So far we have focused on Mersenne *primes*

$$q = 2^p - 1, \qquad p \text{ prime},$$

and we defined a Pratt–recursive class of *Mersenne exponents* $\mathcal{E} \subset \{\text{primes}\}$ such that

$$\mathcal{M} = \{\, 2^p - 1 : p \in \mathcal{E} \,\}$$

is exactly the set of (recursively defined) Mersenne primes.

In this subsection we extend the picture from prime exponents to *arbitrary* exponents $n \geq 2$, i.e. to general Mersenne numbers

$$M_n := 2^n - 1,$$

which are typically composite when $n$ is composite.

#### 6.6.1 From prime exponents to arbitrary exponents

Recall that $\mathcal{E} \subset \{\text{primes}\}$ is the set of Mersenne exponents as in Definition **??**:

- $2 \in \mathcal{E}$ and $3 = 2^2 - 1 \in \mathcal{M}$,
- an odd prime $p > 2$ belongs to $\mathcal{E}$ if and only if every prime divisor $r \mid (p-1)$ lies in $\mathcal{E}$ and $2^p - 1$ is prime.

We now extend $\mathcal{E}$ from primes to all positive integers by taking the multiplicative closure.

**Definition 6.1** (Pratt–Mersenne exponents)**.** Let $\mathcal{E}$ be the set of Mersenne exponents (primes) as above. Define the set of *Pratt–Mersenne exponents*

$$\mathcal{E}^* \subset \mathbb{N}_{\geq 1}$$

by

$$n \in \mathcal{E}^* \iff \text{every prime divisor } p \mid n \text{ lies in } \mathcal{E}.$$

Equivalently, if

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

is the prime factorisation of $n$, then

$$n \in \mathcal{E}^* \iff p_i \in \mathcal{E} \quad \text{for all } i.$$

Thus $\mathcal{E}^*$ is the smallest multiplicative subset of $\mathbb{N}$ containing all primes in $\mathcal{E}$; it consists of all integers whose prime factors are themselves (recursively) Mersenne exponents.

**Definition 6.2** (Pratt–Mersenne numbers)**.** The set of *Pratt–Mersenne numbers* is

$$\mathcal{M}^* := \{\, 2^n - 1 : n \in \mathcal{E}^* \,\}.$$

By construction, we have a natural inclusion

$$\mathcal{M} \subset \mathcal{M}^*,$$

where $\mathcal{M}$ is the set of Mersenne primes. The exponents of the primes in $\mathcal{M}$ are precisely the prime elements of $\mathcal{E}^*$:

$$\mathcal{M} = \{\, 2^p - 1 : p \in \mathcal{E}^* \cap \{\text{primes}\} \,\}.$$

### 6.6.2 Factorisation of $2^n - 1$ and the role of the exponent

For any $n \geq 1$, the classical cyclotomic factorisation gives

$$2^n - 1 = \prod_{d \mid n} \Phi_d(2),$$

where $\Phi_d(x)$ is the $d$-th cyclotomic polynomial. In particular, if

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

is the prime factorisation of $n$, then every divisor $d \mid n$ has the form

$$d = \prod_{i=1}^{k} p_i^{b_i}, \qquad 0 \leq b_i \leq a_i,$$

and the factor $\Phi_d(2)$ appears as one of the building blocks of $2^n - 1$.

Now suppose $n \in \mathcal{E}^*$. Then every prime $p_i$ dividing $n$ lies in $\mathcal{E}$, so by Definition of Mersenne prime the 2–Pratt tree of each $p_i$ is itself built entirely out of primes from $\mathcal{E}$. Thus the combinatorial structure of the exponent $n$ can be described as a finite forest of 2–Pratt trees, one for each prime $p_i \mid n$. The factorisation of $2^n - 1$ into cyclotomic values

$$2^n - 1 = \prod_{d \mid n} \Phi_d(2)$$

is therefore governed by the same recursive data that defines the Mersenne exponents: every $d \mid n$ has only primes from $\mathcal{E}$ in its own Pratt tree, and $\Phi_d(2)$ is a product of primes whose behaviour is controlled by these trees.

**Remark 6.3.** If $2^n - 1$ is prime, then $n$ must itself be prime. Thus every *prime* in $\mathcal{M}^*$ lies already in $\mathcal{M}$, and has exponent in $\mathcal{E}$. The new elements of $\mathcal{M}^*$ for composite $n \in \mathcal{E}^*$ are necessarily composite Mersenne numbers whose prime factors come from the cyclotomic values $\Phi_d(2)$ with $d \mid n$ and $d > 1$.

### 6.6.3 Pratt trees and Galois structure for composite exponents

From the point of view of Galois theory, one can still attach to $M_n = 2^n - 1$ a rich structure via the primes dividing the cyclotomic factors $\Phi_d(2)$, $d \mid n$, and their orders modulo suitable primes. The key points are:

- The exponent $n \in \mathcal{E}^*$ decomposes into primes $p_i \in \mathcal{E}$, each carrying its own 2–Pratt tree.
- Each divisor $d \mid n$ inherits its own Pratt structure from the primes $p_i$, and the factors $\Phi_d(2)$ correspond to layers of this forest.
- For primes $\ell \mid \Phi_d(2)$, the multiplicative order $\mathrm{ord}_\ell(2)$ divides $d$, and hence reflects the combinatorics of the exponent $n$ and its prime divisors.

Thus the passage from Mersenne primes $2^p - 1$ to general Mersenne numbers $2^n - 1$ with $n \in \mathcal{E}^*$ amounts to replacing a single 2–Pratt tree (the tree of $p$) by a finite forest of such trees (one for each prime factor of $n$), while the cyclotomic factorisation of $2^n - 1$ ties this recursive structure to the actual prime factorisation of the Mersenne number $M_n$.

# 7 Zsigmondy-primitive primes and Galois orbits: examples

We illustrate the interaction between Zsigmondy-primitive primes, cyclotomic factors, and the polynomials $f_q(x)$ by two explicit examples computed in Sage.

Recall that a prime $q$ is called *Zsigmondy-primitive* for the pair $(p, d)$ if

$$q \mid (p^d - 1) \qquad \text{and} \qquad q \nmid (p^k - 1) \ \text{ for all } 1 \le k < d.$$

Equivalently, $q$ divides the cyclotomic value $\Phi_d(p)$ and the multiplicative order of $p$ modulo $q$ is exactly $d$:

$$\mathrm{ord}_q(p) = d, \qquad q \mid \Phi_d(p).$$

For each such $q$ we consider the MO-polynomial $f_q(x)$ (irreducible over $\mathbb{Q}$), its splitting field $K_q$, Galois group $G_q := \mathrm{Gal}(K_q/\mathbb{Q})$, and for each prime divisor $r \mid (q-1)$ the orbit

$$\Omega_{q,r} := \{\, f_r(\sigma(\alpha)) : \sigma \in G_q \,\} \subset K_q,$$

where $\alpha$ is a fixed root of $f_q$ in $K_q$.

**Example 7.1** (The primitive pair $(p, d, q) = (3, 5, 11)$)**.** We first take $p = 3$ and $d = 5$. Then

$$3^5 - 1 = 243 - 1 = 242 = 2 \cdot 11^2,$$

and one checks that $q = 11$ is Zsigmondy-primitive for $(3, 5)$:

$$11 \mid (3^5 - 1), \qquad 11 \nmid (3^k - 1) \text{ for } k < 5.$$

Equivalently

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \qquad \Phi_5(3) = 121 = 11^2,$$

and $\mathrm{ord}_{11}(3) = 5$.

The MO-polynomial $f_{11}(x)$ is

$$f_{11}(x) = x^3 + x + 1,$$

which is irreducible over $\mathbb{Q}$. Its splitting field $K_{11}$ has degree

$$[K_{11} : \mathbb{Q}] = 6,$$

so the Galois group $G_{11} := \mathrm{Gal}(K_{11}/\mathbb{Q})$ has order 6 and is (as in Example **??**) isomorphic to $S_3$.

The prime divisors of $q - 1 = 10$ are $r = 2$ and $r = 5$. For each such $r$ we study the orbit $\Omega_{11,r}$ of the element

$$\beta_r := f_r(\alpha)$$

under the action of $G_{11}$, where $\alpha$ is a fixed root of $f_{11}$.

**The orbit $\Omega_{11,2}$.** Here $f_2(x) = x$. If we put $\beta_2 = f_2(\alpha) = \alpha$, then

$$\Omega_{11,2} = \{\, \sigma(\alpha) : \sigma \in G_{11} \,\}$$

is just the full $G_{11}$-orbit of $\alpha$. A computation in Sage shows:

- $|\Omega_{11,2}| = 6$ (the action of $G_{11}$ is 6-transitive on the roots when viewed inside $K_{11}$),
- every $\beta \in \Omega_{11,2}$ has the same degree 6 minimal polynomial

$$\mathrm{minpoly}(\beta/\mathbb{Q}) = x^6 + 3x^5 + 29x^4 + 55x^3 + 223x^2 + 151x + 379.$$

Thus $L_{11,2} := \mathbb{Q}(\beta_2)$ is a degree-6 subfield of $K_{11}$, equal to $K_{11}$ itself (since $[K_{11} : \mathbb{Q}] = 6$). The stabiliser $H_2 := \mathrm{Stab}_{G_{11}}(\beta_2)$ is trivial, and the orbit size $|\Omega_{11,2}| = |G_{11}|$ reflects this.

**The orbit $\Omega_{11,5}$.** For $r = 5$ we have $f_5(x) = x^2 + 1$, hence

$$\beta_5 := f_5(\alpha) = \alpha^2 + 1, \qquad \Omega_{11,5} = \{\, \sigma(\alpha^2 + 1) : \sigma \in G_{11} \,\}.$$

Again Sage gives:

- $|\Omega_{11,5}| = 6$;
- every $\gamma \in \Omega_{11,5}$ has minimal polynomial

$$\mathrm{minpoly}(\gamma/\mathbb{Q}) = x^6 + 43x^5 + 727x^4 + 6403x^3 + 31085x^2 + 61725x + 43657.$$

Thus $L_{11,5} := \mathbb{Q}(\beta_5)$ is again a degree-6 subfield of $K_{11}$, so in fact $L_{11,5} = K_{11}$ as well. The corresponding stabiliser $H_5 := \mathrm{Stab}_{G_{11}}(\beta_5)$ is also trivial, and the orbit $\Omega_{11,5}$ has full size $|G_{11}|$.

From the Zsigmondy point of view, the primitive prime $q = 11$ arises from the cyclotomic factor $\Phi_5(3)$, and the Galois side shows that the associated polynomial $f_{11}(x)$ has a highly non-abelian splitting field with Galois group $S_3$; all orbits $\Omega_{11,r}$ for $r \mid (q - 1)$ in this small example have maximal size.

**Example 7.2** (The primitive pair $(p, d, q) = (5, 3, 31)$)**.** We now take $p = 5$ and $d = 3$. Then

$$5^3 - 1 = 125 - 1 = 124 = 2^2 \cdot 31,$$

and $q = 31$ is Zsigmondy-primitive for $(5, 3)$:

$$31 \mid (5^3 - 1), \qquad 31 \nmid (5^k - 1) \text{ for } k < 3.$$

Equivalently

$$\Phi_3(x) = x^2 + x + 1, \qquad \Phi_3(5) = 5^2 + 5 + 1 = 31,$$

and $\mathrm{ord}_{31}(5) = 3$.

The associated MO-polynomial is

$$f_{31}(x) = x^4 + x^3 + x^2 + x + 1,$$

irreducible over $\mathbb{Q}$. Its splitting field $K_{31}$ has degree

$$[K_{31} : \mathbb{Q}] = 4,$$

so $G_{31} := \mathrm{Gal}(K_{31}/\mathbb{Q})$ has order 4; in fact $G_{31} \cong C_4$ (cyclic of order 4), as seen in the data table for small $p$.

The prime divisors of $q - 1 = 30$ are $r \in \{2, 3, 5\}$. For each $r$ we look at $\beta_r := f_r(\alpha)$, where $\alpha$ is a root of $f_{31}(x)$, and its $G_{31}$-orbit $\Omega_{31,r}$.

**The orbit $\Omega_{31,2}$.** Here $f_2(x) = x$, so

$$\Omega_{31,2} = \{\sigma(\alpha) : \sigma \in G_{31}\}$$

is just the set of the four roots of $f_{31}$. The Sage output is

$$\Omega_{31,2} = \{\, \alpha,\ \alpha^2,\ \alpha^3,\ -\alpha^3 - \alpha^2 - \alpha - 1 \,\},$$

and each element has minimal polynomial

$$\mathrm{minpoly}(\cdot/\mathbb{Q}) = x^4 + x^3 + x^2 + x + 1.$$

Thus $L_{31,2} := \mathbb{Q}(\alpha)$ is a quartic subfield of $K_{31}$ with $[L_{31,2} : \mathbb{Q}] = 4$, and in fact $L_{31,2} = K_{31}$ since the splitting field of an irreducible quartic has degree 4 in this case.

**The orbits $\Omega_{31,3}$ and $\Omega_{31,5}$.** For $r = 3$ and $r = 5$ we have

$$f_3(x) = x + 1, \qquad f_5(x) = x^2 + 1.$$

The Sage computation gives:

$$\Omega_{31,3} = \{\, \alpha + 1,\ \alpha^2 + 1,\ -\alpha^3 - \alpha^2 - \alpha,\ \alpha^3 + 1 \,\},$$

and

$$\Omega_{31,5} = \{\, \alpha^2 + 1,\ -\alpha^3 - \alpha^2 - \alpha,\ \alpha^3 + 1,\ \alpha + 1 \,\}.$$

Thus $\Omega_{31,3} = \Omega_{31,5}$ as sets: the four elements coincide exactly, just in different order. Moreover, each of these elements has the same minimal polynomial

$$\mathrm{minpoly}(\cdot/\mathbb{Q}) = x^4 - 3x^3 + 4x^2 - 2x + 1.$$

Therefore they generate a *second* quartic field

$$L_{31,3} := \mathbb{Q}(\Omega_{31,3}) = \mathbb{Q}(\Omega_{31,5}) =: L_{31} \subset K_{31},$$

distinct from $\mathbb{Q}(\alpha)$, but still of degree 4 over $\mathbb{Q}$. The two quartic subfields $L_{31,2} = K_{31}$ and $L_{31}$ correspond to two index-one and index-two subgroups in the cyclic group $G_{31} \cong C_4$, reflecting the dihedral structure of the subfield lattice in this simple case.

From the Zsigmondy viewpoint, the primitive prime $q = 31$ appears as a prime divisor of $\Phi_3(5)$, whereas on the Galois side the polynomial $f_{31}(x)$ has cyclic Galois group of order 4. The three primes $r \mid (q-1)$ give rise to only *two* distinct $G_{31}$-orbits:

- $\Omega_{31,2} = R_{31}$ is the orbit of a root of $f_{31}$ and corresponds to the quartic field $\mathbb{Q}(\alpha)$ with minimal polynomial $x^4 + x^3 + x^2 + x + 1$;
- $\Omega_{31,3} = \Omega_{31,5}$ is a single $G_{31}$-orbit of size 4, corresponding to a different quartic subfield $L_{31} \subset K_{31}$ with minimal polynomial $x^4 - 3x^3 + 4x^2 - 2x + 1$.

In particular, this shows that the naive expectation that for a fixed prime $q$ the sets $\Omega_{q,r}$ attached to different primes $r \mid (q-1)$ should always be disjoint is, in general, *false*: here the orbits for $r = 3$ and $r = 5$ coincide.

**Lemma 7.3** (Galois-theoretic meaning of the orbits $\Omega_{q,r}$)**.** *Let $q$ be a prime, let $f_q(x) \in \mathbb{Z}[x]$ be irreducible, and let $K_q$ be its splitting field over $\mathbb{Q}$ with Galois group*

$$G_q := \mathrm{Gal}(K_q/\mathbb{Q}).$$

*Fix a root $\alpha$ of $f_q$ in $K_q$, and let $R_q$ be the set of all roots of $f_q$ in $K_q$.*

*For each prime divisor $r \mid (q-1)$, let $f_r(x) \in \mathbb{Z}[x]$ be the corresponding MO–polynomial (as in the recursive definition), put*

$$\beta_r := f_r(\alpha) \in K_q,$$

*and define the $G_q$–orbit*

$$\Omega_{q,r} := \{\, f_r(\sigma(\alpha)) : \sigma \in G_q \,\} = \{\, \sigma(\beta_r) : \sigma \in G_q \,\} \subset K_q.$$

*Let*

$$H_r := \mathrm{Stab}_{G_q}(\beta_r) = \{\, \sigma \in G_q : \sigma(\beta_r) = \beta_r \,\}$$

*be the stabiliser of $\beta_r$ in $G_q$, and let*

$$L_r := \mathbb{Q}(\Omega_{q,r}) \subseteq K_q$$

*be the subfield generated (over $\mathbb{Q}$) by all conjugates of $\beta_r$. Then:*

1. *$H_r$ is a subgroup of $G_q$, and $\Omega_{q,r}$ is a single $G_q$–orbit with*

$$|\Omega_{q,r}| = [G_q : H_r].$$

2. *The fixed field $K_q^{H_r}$ is equal to $L_r$:*

$$L_r = K_q^{H_r},$$

*in particular $L_r/\mathbb{Q}$ is Galois and*

$$[L_r : \mathbb{Q}] = |\Omega_{q,r}|.$$

*3. Two primes $r, s \mid (q-1)$ give the same orbit*

$$\Omega_{q,r} = \Omega_{q,s}$$

*if and only if $\beta_r$ and $\beta_s$ are Galois-conjugate over $\mathbb{Q}$, if and only if the stabilisers $H_r$ and $H_s$ are conjugate subgroups of $G_q$. In this case $L_r = L_s$.*

*Proof.* First note that, since $G_q$ acts as field automorphisms of $K_q$ fixing $\mathbb{Q}$, we have for any $\sigma \in G_q$:

$$\sigma(f_r(\alpha)) = f_r(\sigma(\alpha)),$$

because $\sigma$ acts coefficientwise and the coefficients of $f_r$ lie in $\mathbb{Q}$. Thus

$$\Omega_{q,r} = \{f_r(\sigma(\alpha)) : \sigma \in G_q\} = \{\sigma(\beta_r) : \sigma \in G_q\} = G_q \cdot \beta_r$$

is indeed the $G_q$–orbit of $\beta_r$.

*(i) Subgroup and orbit size.* By definition,

$$H_r = \{\sigma \in G_q : \sigma(\beta_r) = \beta_r\}.$$

It is immediate that $H_r$ is a subgroup: the identity fixes $\beta_r$; if $\sigma, \tau \in H_r$ then

$$(\sigma\tau)(\beta_r) = \sigma(\tau(\beta_r)) = \sigma(\beta_r) = \beta_r,$$

so $\sigma\tau \in H_r$, and if $\sigma(\beta_r) = \beta_r$ then also $\sigma^{-1}(\beta_r) = \beta_r$.

Since $\Omega_{q,r} = G_q \cdot \beta_r$ is a single orbit, the orbit–stabiliser formula gives

$$|\Omega_{q,r}| = [G_q : H_r],$$

as claimed.

*(ii) Identification of $L_r$ with the fixed field $K_q^{H_r}$.* Let

$$F_r := K_q^{H_r} = \{\, x \in K_q : \sigma(x) = x \text{ for all } \sigma \in H_r \,\}$$

be the fixed field of $H_r$. Since $K_q/\mathbb{Q}$ is Galois, we know $F_r/\mathbb{Q}$ is Galois and

$$[F_r : \mathbb{Q}] = [G_q : H_r] = |\Omega_{q,r}|.$$

We claim that $L_r = F_r$. First, $H_r$ fixes $\beta_r$ by definition, and therefore it fixes every conjugate $\sigma(\beta_r) \in \Omega_{q,r}$. Hence $H_r$ fixes every element of $\Omega_{q,r}$, and thus fixes the field $L_r = \mathbb{Q}(\Omega_{q,r})$. This shows

$$L_r \subseteq F_r.$$

Let $H_r' := \mathrm{Gal}(K_q/L_r)$ be the subgroup of $G_q$ consisting of all automorphisms of $K_q$ that fix $L_r$ pointwise. Clearly $H_r \subseteq H_r'$, since any element fixing $\beta_r$ fixes all $\sigma(\beta_r)$ (and hence $L_r$). By the Galois correspondence we have

$$[L_r : \mathbb{Q}] = \frac{|G_q|}{|H_r'|}.$$

On the other hand, the number of distinct $\mathbb{Q}$–embeddings of $L_r$ into $K_q$ is equal to $[L_r : \mathbb{Q}]$. Each such embedding is uniquely determined by the image of $\beta_r$, and the image of $\beta_r$ must be a Galois-conjugate of $\beta_r$, hence lies in $\Omega_{q,r}$. Therefore

$$[L_r : \mathbb{Q}] \leq |\Omega_{q,r}| = [G_q : H_r] = [F_r : \mathbb{Q}].$$

Combining the inequalities

$$[L_r : \mathbb{Q}] = \frac{|G_q|}{|H_r'|} \geq \frac{|G_q|}{|H_r|} = [F_r : \mathbb{Q}],$$

with the previous inequality $[L_r : \mathbb{Q}] \leq [F_r : \mathbb{Q}]$ forces equality throughout:

$$[L_r : \mathbb{Q}] = [F_r : \mathbb{Q}] \quad \text{and} \quad |H_r'| = |H_r|.$$

Since $H_r \subseteq H_r'$ and they have the same order, we get $H_r = H_r'$, and therefore their fixed fields coincide:

$$L_r = K_q^{H_r'} = K_q^{H_r} = F_r.$$

This proves (ii), in particular

$$[L_r : \mathbb{Q}] = [F_r : \mathbb{Q}] = [G_q : H_r] = |\Omega_{q,r}|.$$

*(iii) Equality of orbits and conjugacy of stabilisers.* Suppose first that $\Omega_{q,r} = \Omega_{q,s}$. Then in particular $\beta_r \in \Omega_{q,s}$, so $\beta_r$ is Galois-conjugate to $\beta_s$. Conversely, if $\beta_r$ and $\beta_s$ are Galois-conjugate, there exists $\tau \in G_q$ with $\tau(\beta_r) = \beta_s$, and hence

$$\tau(\Omega_{q,r}) = \{\, \tau(\sigma(\beta_r)) : \sigma \in G_q \,\} = \{\, \sigma(\beta_s) : \sigma \in G_q \,\} = \Omega_{q,s},$$

so the orbits coincide up to the action of $G_q$ and hence as subsets of $K_q$.

That $\beta_r$ and $\beta_s$ are Galois-conjugate is equivalent to saying that the subgroups $H_r$ and $H_s$ are conjugate in $G_q$. Indeed, in a finite Galois extension $K_q/\mathbb{Q}$, two elements have conjugate stabilisers if and only if they are Galois-conjugate, and conjugate subgroups always have fixed fields of the same degree. In particular, conjugacy of $H_r$ and $H_s$ implies that the fixed fields $K_q^{H_r}$ and $K_q^{H_s}$ have the same degree and are conjugate subfields of $K_q$; hence, by (ii), $L_r$ and $L_s$ coincide as subfields of $K_q$ if and only if the orbits $\Omega_{q,r}$ and $\Omega_{q,s}$ coincide.

This proves (iii). □

**Remark 7.4.** In the Zsigmondy setting, where $q$ is a primitive prime divisor of $p^d - 1$ (equivalently $q \mid \Phi_d(p)$ and $\mathrm{ord}_q(p) = d$), the lemma applies to the associated MO–polynomial $f_q$ and its splitting field $K_q$. The primes $r \mid (q-1)$ appearing in the Pratt tree of $q$ give a family of subgroups $(H_r)_{r|(q-1)} \subseteq G_q$ and Galois subfields $L_r = K_q^{H_r}$ whose degrees are exactly the orbit sizes $|\Omega_{q,r}|$. The explicit computations for $(p, d, q) = (3, 5, 11)$ and $(5, 3, 31)$ above illustrate how these subfields and orbits behave in practice.

## 7.1 PG-data at a fixed prime $p$

We work with polynomials $f_n(x) \in \mathbb{Z}[x]$ satisfying:

- $f_p(x)$ is irreducible over $\mathbb{Q}$ for every prime $p$;
- $f_p(x) = 1 + f_{p-1}(x)$ for every prime $p$;
- $f_n(x) = \prod_{q|n} f_q(x)^{v_q(n)}$ for all $n \geq 1$.

Fix a prime $p$. Define:

$$\begin{aligned} K_p &:= \mathrm{Spl}(f_p(x)/\mathbb{Q}), \\ G_p &:= \mathrm{Gal}(K_p/\mathbb{Q}), \\ R_p &:= \{\text{roots of } f_p(x) \text{ in } K_p\}, \\ d &:= \deg(f_p) = |R_p|. \end{aligned}$$

**Definition 7.5** (Root and Galois data at level $p$)**.** We set

$$t_p := \big(p, f_p(x), K_p, G_p, R_p, \Sigma_p\big),$$

where $\Sigma_p$ denotes the permutation representation

$$\Sigma_p : G_p \longrightarrow \mathrm{Sym}(R_p), \qquad \sigma \mapsto (\alpha \mapsto \sigma(\alpha)).$$

**Proposition 7.6** (Collected properties at level $p$)**.** *With notation as above, the following hold.*

(PG1) ***Irreducibility and roots.***

(a) *$f_p(x)$ is irreducible over $\mathbb{Q}$ of degree $d$.*

(b) *$R_p \subset K_p$ is a finite set with $|R_p| = d$.*

(c) *For each $\alpha \in R_p$ we have* $\mathrm{minpoly}(\alpha/\mathbb{Q}) = f_p(x)$.

(PG2) ***Splitting field and Galois extension.***

(a) *$K_p/\mathbb{Q}$ is a finite Galois extension.*

(b) *$K_p$ is generated over $\mathbb{Q}$ by the roots:*

$$K_p = \mathbb{Q}(R_p).$$

(c) *The Galois group $G_p := \mathrm{Gal}(K_p/\mathbb{Q})$ acts on $K_p$ by field automorphisms fixing $\mathbb{Q}$.*

(PG3) ***Transitive and faithful action on roots.***

(a) *$G_p$ acts transitively on $R_p$; equivalently $\Sigma_p$ is a transitive permutation representation.*

(b) *The kernel of $\Sigma_p$ is trivial, i.e. the action is faithful. Thus we may regard $G_p$ as a transitive subgroup of* $\mathrm{Sym}(R_p) \cong S_d$.

(c) *For any fixed $\alpha \in R_p$, the stabiliser*

$$N := \mathrm{Gal}(K_p/\mathbb{Q}(\alpha)) = \{\sigma \in G_p : \sigma(\alpha) = \alpha\}$$

*is a normal subgroup of index*

$$[G_p : N] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d,$$

*and we have a field tower*

$$\mathbb{Q} \ \subset \ \mathbb{Q}(\alpha) \ \subset \ K_p.$$

(PG4) ***Multiplicative relation at the roots.***

(a) *By multiplicativity,*

$$f_{p-1}(x) = \prod_{r \mid (p-1)} f_r(x)^{v_r(p-1)}.$$

(b) *For each $\alpha \in R_p$ we have*

$$f_p(\alpha) = 0 \quad \Longleftrightarrow \quad 1 + f_{p-1}(\alpha) = 0,$$

*hence*

$$f_{p-1}(\alpha) = -1 = \prod_{r \mid (p-1)} f_r(\alpha)^{v_r(p-1)}.$$

(c) *This equation is $G_p$-invariant: for all $\sigma \in G_p$ and $\alpha \in R_p$,*

$$-1 = \sigma(-1) = \sigma(f_{p-1}(\alpha)) = f_{p-1}(\sigma(\alpha)) = \prod_{r|(p-1)} f_r(\sigma(\alpha))^{v_r(p-1)}.$$

(PG5) ***The sets $\Omega_{p,q}$ and their definition.***

(a) *For each prime divisor $q \mid (p-1)$ we define*

$$\Omega_{p,q} := \{\, f_q(\alpha) : \alpha \in R_p \,\} \subset K_p.$$

(b) *The union*

$$\Omega_p := \bigcup_{\substack{q|(p-1) \\ q \text{ prime}}} \Omega_{p,q}$$

*is a subset of $K_p$. In general this union is* not *disjoint.*

(c) *For each $q \mid (p-1)$ and each $\alpha \in R_p$, the element $f_q(\alpha)$ lies in $K_p$, and all Galois conjugates of $f_q(\alpha)$ under $G_p$ lie in $\Omega_{p,q}$.*

(PG6) ***Galois action on $\Omega_p$ and $\Omega_{p,q}$.***

(a) *The formula*

$$\sigma \cdot f_q(\alpha) := f_q(\sigma(\alpha)), \qquad \sigma \in G_p,\ \alpha \in R_p,\ q \mid (p-1),$$

*defines a well-defined action of $G_p$ on $\Omega_p$.*

(b) *This action is compatible with the action by field automorphisms: $\sigma(f_q(\alpha)) = f_q(\sigma(\alpha))$ for all $\sigma \in G_p$.*

(c) *Each subset $\Omega_{p,q}$ is stable under this action, i.e. $G_p \cdot \Omega_{p,q} = \Omega_{p,q}$.*

(d) *We write $\Sigma_{p,q}$ for the corresponding permutation representation*

$$\Sigma_{p,q} : G_p \longrightarrow \mathrm{Sym}(\Omega_{p,q}), \qquad \sigma \mapsto (x \mapsto \sigma(x)).$$

(PG7) ***Equivariance of $R_p \to \Omega_{p,q}$.***

(a) *For each $q \mid (p-1)$ the map*

$$\varphi_{p,q} : R_p \longrightarrow \Omega_{p,q}, \qquad \alpha \longmapsto f_q(\alpha)$$

*is $G_p$-equivariant:*

$$\varphi_{p,q}(\sigma(\alpha)) = f_q(\sigma(\alpha)) = \sigma(f_q(\alpha)) = \sigma(\varphi_{p,q}(\alpha)).$$

(b) *The action of $G_p$ on $\Omega_{p,q}$ is thus the permutation representation induced from $\Sigma_p$ via the equivariant map $\varphi_{p,q}$.*

(PG8) ***$\Omega_{p,q}$ as single $G_p$-orbits.*** *Fix a root $\alpha \in R_p$ and set*

$$\beta_q := f_q(\alpha) \in K_p.$$

*Then:*

(a) *Every other root has the form $\sigma(\alpha)$ for some $\sigma \in G_p$, and*

$$f_q(\sigma(\alpha)) = \sigma(f_q(\alpha)) = \sigma(\beta_q).$$

(b) *Hence*

$$\Omega_{p,q} = \{f_q(\alpha') : \alpha' \in R_p\} = \{f_q(\sigma(\alpha)) : \sigma \in G_p\} = \{\sigma(\beta_q) : \sigma \in G_p\} =: G_p \cdot \beta_q.$$

*In particular,* $\Omega_{p,q}$ *is a* single $G_p$*-orbit.*

(PG9) ***Stabilisers and orbit sizes.***

(a) *For each* $q \mid (p-1)$ *we define the stabiliser*

$$H_q := \mathrm{Stab}_{G_p}(\beta_q) = \{\sigma \in G_p : \sigma(\beta_q) = \beta_q\}.$$

(b) *The standard orbit–stabiliser formula gives*

$$|\Omega_{p,q}| = |G_p \cdot \beta_q| = [G_p : H_q].$$

(c) *The subgroup*

$$N := \mathrm{Gal}(K_p/\mathbb{Q}(\alpha))$$

*fixes* $\alpha$ *and hence every polynomial in* $\alpha$ *with rational coefficients; in particular,*

$$N \subseteq H_q \quad \textit{for all } q \mid (p-1).$$

(PG10) ***Location of*** $\beta_q$ ***and degree bounds.***

(a) *For each* $q \mid (p-1)$ *we have*

$$\beta_q = f_q(\alpha) \in \mathbb{Q}(\alpha).$$

(b) *Setting* $L_{p,q} := \mathbb{Q}(\beta_q)$*, we obtain a field tower*

$$\mathbb{Q} \;\subset\; L_{p,q} \;\subset\; \mathbb{Q}(\alpha) \;\subset\; K_p.$$

(c) *Galois theory gives*

$$\mathrm{Gal}(K_p/L_{p,q}) = \mathrm{Stab}_{G_p}(\beta_q) = H_q.$$

(d) *The degree of* $L_{p,q}$ *over* $\mathbb{Q}$ *is the orbit size:*

$$[L_{p,q} : \mathbb{Q}] = \deg(\mathrm{minpoly}(\beta_q/\mathbb{Q})) = |\Omega_{p,q}| = [G_p : H_q].$$

(e) *Since* $N \subseteq H_q$ *and* $[G_p : N] = d$*, we have*

$$|\Omega_{p,q}| = [G_p : H_q] = \frac{[G_p : N]}{[H_q : N]} \mid [G_p : N] = d.$$

*In particular,* $[L_{p,q} : \mathbb{Q}]$ *divides the degree* $d = \deg(f_p)$*.*

(PG11) ***Quotients of*** $G_p$ ***coming from the data*** $q \mid (p-1)$***.***

(a) *The natural quotient*

$$G_p/\,\mathrm{Gal}(K_p/L_{p,q}) = G_p/H_q$$

*has order* $|G_p/H_q| = |\Omega_{p,q}| \mid d$*.*

(b) *The permutation representation* $\Sigma_{p,q}$ *of* $G_p$ *on* $\Omega_{p,q}$ *has kernel* $H_q$ *and image isomorphic to* $G_p/H_q$*.*

(c) *Thus $\Sigma_{p,q}$ is a transitive quotient representation of $\Sigma_p$, whose degree does not exceed the number of roots $d$.*

(PG12) ***Relations between different prime divisors*** *$q, r \mid (p-1)$. Let again $\beta_q = f_q(\alpha)$, $\beta_r = f_r(\alpha)$ for a fixed root $\alpha \in R_p$. Then the following are equivalent:*

(a) *$\beta_q$ and $\beta_r$ are Galois-conjugate under $G_p$, i.e. there exists $\sigma \in G_p$ with $\sigma(\beta_q) = \beta_r$.*

(b) *The orbits (equivalently, the sets) coincide:*

$$\Omega_{p,q} = G_p \cdot \beta_q = G_p \cdot \beta_r = \Omega_{p,r}.$$

(c) *The stabilisers are conjugate:*

$$H_r = \sigma H_q \sigma^{-1} \quad \text{for some } \sigma \in G_p.$$

(d) *The corresponding intermediate fields $L_{p,q} = K_p^{H_q}$ and $L_{p,r} = K_p^{H_r}$ are conjugate in $K_p$, i.e. $L_{p,r} = \sigma(L_{p,q})$ for the same $\sigma$.*

*In particular, the assignment*

$$q \;\longmapsto\; \Omega_{p,q}$$

*is in general not injective: different prime divisors $q, r \mid (p-1)$ may produce the same set $\Omega_{p,q} = \Omega_{p,r}$ and the same intermediate field $L_{p,q} = L_{p,r}$.*

(PG13) ***Decomposition of $\Omega_p$ into orbits.***

(a) *The set $\Omega_p$ is a union of finitely many disjoint $G_p$-orbits.*

(b) *Each of these orbits is one of the sets $\Omega_{p,q}$, or is a set occurring as $\Omega_{p,q}$ for several different prime divisors $q \mid (p-1)$ (cf. Example **??**).*

**Definition 7.7** (Pratt–Galois tree (PG-tree))**.** A *PG-tree* is a rooted tree whose vertices are labelled by primes $p$, and to each vertex we attach a PG-node $t_p$ as above. For each edge

$$p \longrightarrow q \quad \text{with} \quad q \mid (p-1)$$

we attach the *edge data*

$$(\beta_{p,q},\, \Omega_{p,q},\, H_{p,q},\, L_{p,q},\, \Sigma_{p,q}),$$

where

- $\Omega_{p,q} = G_p \cdot \beta_{p,q}$ is the orbit in $K_p$;
- $H_{p,q} = \mathrm{Stab}_{G_p}(\beta_{p,q})$ is the stabiliser;
- $L_{p,q} = K_p^{H_{p,q}}$ is the corresponding intermediate field;
- $\Sigma_{p,q} : G_p \to \mathrm{Sym}(\Omega_{p,q})$ is the permutation representation on $\Omega_{p,q}$.

At every vertex $p$ the data satisfy all conditions of Proposition 7.6, and the edges of the tree encode the divisibility relations $q \mid (p-1)$ together with the associated quotients of $G_p$ and intermediate fields $L_{p,q}$.

## 7.2 Primitive element primes and local Galois quotients

Throughout, let $p$ be a prime, and let

$$t_p = \big(p, K_p, G_p, R_p, \Sigma_p,\ (\beta_{p,q})_{q|(p-1)}\big)$$

be a PG-node at level $p$ in the sense of the previous subsection. We write $d := |R_p| = \deg(f_p)$, fix $\alpha \in R_p$, and set

$$N_p := \mathrm{Gal}(K_p/\mathbb{Q}(\alpha)).$$

For each prime divisor $q \mid (p-1)$ we have

$$\beta_{p,q} \in \mathbb{Q}(\alpha), \quad \Omega_{p,q} := G_p \cdot \beta_{p,q}, \quad H_{p,q} := \mathrm{Stab}_{G_p}(\beta_{p,q}), \quad L_{p,q} := K_p^{H_{p,q}},$$

and Proposition 7.6 (PG10) gives

$$[L_{p,q} : \mathbb{Q}] = |\Omega_{p,q}| = [G_p : H_{p,q}] \mid d \quad \text{and} \quad N_p \subseteq H_{p,q},\ [G_p : N_p] = d.$$

**Definition 7.8** (Primitive element prime)**.** A prime $p$ is called a *primitive element prime* if there exists a PG-node $t_p$ at level $p$ and a choice of root $\alpha \in R_p$ with the following property:

for every prime divisor $q \mid (p-1)$ we have

$$|\Omega_{p,q}| = d,$$

equivalently

$$\mathbb{Q}(\beta_{p,q}) = \mathbb{Q}(\alpha) \quad \text{and} \quad H_{p,q} = \mathrm{Gal}(K_p/\mathbb{Q}(\alpha)) = N_p.$$

In this situation each $\beta_{p,q}$ is a primitive element of the degree-$d$ field $\mathbb{Q}(\alpha)$, and all intermediate fields $L_{p,q}$ coincide with $\mathbb{Q}(\alpha)$.

**Remark 7.9** (Empirical evidence and non-universality)**.** For the small primes $p = 2, 3, \ldots, 37$ examined computationally, every prime $p$ appearing as a node in the PG-trees constructed from the polynomials $f_p$ satisfies

$$|\Omega_{p,q}| = d \quad \text{for all primes } q \mid (p-1),$$

hence is a primitive element prime in the sense of Definition 7.8.

We do not currently see a conceptual proof that *every* prime is a primitive element prime, and there is no clear reason to expect this to hold in general. Thus we regard Definition 7.8 as a genuine restriction, and we will systematically distinguish the two global scenarios:

1. every node $p$ in a given PG-tree is a primitive element prime;
2. at least one node $p$ in the PG-tree is not a primitive element prime.

### 7.2.1 Local structure at a primitive element prime

We first record the strengthening of PG10 that holds under Definition 7.8.

**Proposition 7.10** (Full-orbit phenomenon at a primitive element prime)**.** *Let $p$ be a primitive element prime, and fix a PG-node $t_p$ and $\alpha \in R_p$ as in the definition. Then for every prime divisor $q \mid (p-1)$ the following hold:*

*1. The orbit has maximal size:*

$$|\Omega_{p,q}| = d = |R_p|.$$

2. *The field generated by $\beta_{p,q}$ coincides with the root field:*

$$L_{p,q} = \mathbb{Q}(\beta_{p,q}) = \mathbb{Q}(\alpha).$$

3. *The stabiliser coincides with $N_p$:*

$$H_{p,q} = \mathrm{Gal}(K_p/\mathbb{Q}(\alpha)) = N_p.$$

4. *The quotient groups attached to different $q \mid (p-1)$ are canonically isomorphic:*

$$\mathrm{Gal}(L_{p,q}/\mathbb{Q}) \cong G_p/H_{p,q} = G_p/N_p \cong \mathrm{Gal}\big(\mathbb{Q}(\alpha)/\mathbb{Q}\big),$$

*independently of $q$.*

*In particular there is a distinguished transitive Galois group*

$$A_p := \mathrm{Gal}\big(\mathbb{Q}(\alpha)/\mathbb{Q}\big)$$

*at level $p$ such that for every edge $p \to q$ with $q \mid (p-1)$ the associated quotient $G_p/H_{p,q}$ is canonically isomorphic to $A_p$.*

*Proof.* By assumption, $|\Omega_{p,q}| = d$ for all $q \mid (p-1)$. Since $|\Omega_{p,q}| = [G_p : H_{p,q}]$ and $[G_p : N_p] = d$ with $N_p \subseteq H_{p,q}$, we must have $H_{p,q} = N_p$, proving (iii). Then

$$[L_{p,q} : \mathbb{Q}] = |\Omega_{p,q}| = d = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

and the inclusion $\mathbb{Q}(\beta_{p,q}) \subseteq \mathbb{Q}(\alpha)$ forces equality, giving (ii). The remaining statements follow directly from the definitions and from the Galois correspondence. □

**Proposition 7.11** (Universal local quotient and lack of vertical maps)**.** *Let $p$ be any prime (primitive element or not), and let $q \mid (p-1)$ be a prime divisor. Then:*

1. *The edge $p \to q$ induces a canonical surjection*

$$\pi_{p,q} : G_p \twoheadrightarrow \mathrm{Gal}(L_{p,q}/\mathbb{Q}) \cong G_p/H_{p,q},$$

*with kernel $H_{p,q}$.*

2. *In general there is no canonical field embedding $K_q \hookrightarrow K_p$, and hence no canonical group homomorphism*

$$G_q = \mathrm{Gal}(K_q/\mathbb{Q}) \;\longrightarrow\; G_p = \mathrm{Gal}(K_p/\mathbb{Q}).$$

*Thus the group naturally associated to the edge $p \to q$ is the quotient $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$, rather than the group $G_q$ at the node $q$.*

**Remark 7.12.** When $p$ is a primitive element prime, Proposition 7.10 shows that all quotients $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$ (for $q \mid (p-1)$) are canonically isomorphic to a single transitive group $A_p$. The dependence on $q$ is then encoded entirely in the choice of primitive element $\beta_{p,q} \in \mathbb{Q}(\alpha)$, not in the abstract Galois group attached to the edge.

### 7.2.2 Global scenarios for a PG-tree

Let $\mathcal{T}$ be a PG-tree with root prime $p_0$. Each vertex $p$ carries a PG-node $t_p$, and each edge $p \to q$ with $q \mid (p-1)$ carries the associated data $(\beta_{p,q}, \Omega_{p,q}, H_{p,q}, L_{p,q}, \Sigma_{p,q})$.

**Case (a): every vertex is a primitive element prime.**

Assume that every prime $p$ occurring as a vertex of $\mathcal{T}$ is a primitive element prime. Then for each such $p$ we can choose a root $\alpha_p \in R_p$ and obtain a distinguished degree-$d_p$ field $\mathbb{Q}(\alpha_p) \subset K_p$ with

$$d_p := |R_p| = \deg(f_p), \qquad A_p := \mathrm{Gal}(\mathbb{Q}(\alpha_p)/\mathbb{Q}) \cong G_p/N_p,$$

where $N_p = \mathrm{Gal}(K_p/\mathbb{Q}(\alpha_p))$.

For every edge $p \to q$ with $q \mid (p-1)$ we then have:

- the intermediate field is independent of $q$:

$$L_{p,q} = \mathbb{Q}(\beta_{p,q}) = \mathbb{Q}(\alpha_p);$$

- the attached quotient $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$ is canonically isomorphic to $A_p$;
- the subgroup $H_{p,q}$ is independent of $q$ and equals $\mathrm{Gal}(K_p/\mathbb{Q}(\alpha_p))$.

In this fully primitive situation, the PG-tree $\mathcal{T}$ has the following flavour:

1. At each vertex $p$ there is a "universal local quotient" $A_p$, and all outgoing edges $p \to q$ carry the same abstract Galois group $A_p$.
2. The distinguishing information along edges $p \to q$ is the choice of primitive elements $\beta_{p,q} \in \mathbb{Q}(\alpha_p)$, together with the multiplicative relation

$$\prod_{q \mid (p-1)} \beta_{p,q}^{v_q(p-1)} = -1$$

   in $\mathbb{Q}(\alpha_p)$, which is $G_p$-invariant.
3. There is no canonical Galois-theoretic map relating $A_p$ and the groups $A_q$, $G_q$ at lower levels; only the quotients $\pi_{p,q} : G_p \twoheadrightarrow A_p$ and the combinatorial divisibility pattern $q \mid (p-1)$ are canonical.

In other words, when all vertices are primitive element primes, the PG-tree records, at each level $p$, a single transitive Galois group $A_p$ and several distinguished primitive elements $\beta_{p,q}$ of the same field $\mathbb{Q}(\alpha_p)$, constrained by a global multiplicative relation.

**Case (b): existence of a non-primitive element prime.**

Suppose that at least one vertex $p$ of $\mathcal{T}$ is *not* a primitive element prime. By definition, this means that for every choice of PG-node $t_p$ and root $\alpha \in R_p$ there exists a prime divisor $q \mid (p-1)$ such that

$$|\Omega_{p,q}| < d.$$

Equivalently,

$$[L_{p,q} : \mathbb{Q}] = |\Omega_{p,q}| < d = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

so that

$$L_{p,q} \subsetneq \mathbb{Q}(\alpha)$$

is a proper subfield, and the quotient

$$\mathrm{Gal}(L_{p,q}/\mathbb{Q}) \cong G_p/H_{p,q}$$

is a proper quotient of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong G_p/N_p$.

At such a non-primitive vertex $p$, the PG-data therefore exhibit *genuine* variation among the fields $L_{p,q}$ and groups $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$ as $q$ ranges over the prime divisors of $p-1$:

1. There exists at least one "defective" edge $p \to q$ for which $L_{p,q}$ is a proper subfield of $\mathbb{Q}(\alpha)$ and the quotient $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$ is strictly smaller than the maximal local quotient $G_p/N_p$.

2. Different primes $q, r \mid (p-1)$ may yield different intermediate fields $L_{p,q}$, $L_{p,r}$ and non-isomorphic quotient groups $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$, $\mathrm{Gal}(L_{p,r}/\mathbb{Q})$, or they may coincide as in the orbit-identification phenomena of Proposition 7.6(PG11).

3. Along a branch $p \to q \to r \to \cdots$ of the PG-tree, these proper subfields can be viewed as recording a sequence of "shrinking" quotients of the local Galois groups as one moves down the tree, although no canonical comparison map between the Galois groups at different levels is available.

From this perspective, the global behaviour of a PG-tree $\mathcal{T}$ splits into two qualitatively different regimes:

- In the *fully primitive* regime (case (a)), each node $p$ carries a single transitive group $A_p$ and all outgoing edges $p \to q$ realise the same quotient $G_p \twoheadrightarrow A_p$; the edge data differ only by the choice of primitive elements $\beta_{p,q}$.

- In the *non-primitive* regime (case (b)), some vertices $p$ carry a richer family of intermediate fields $L_{p,q}$ and quotient groups $\mathrm{Gal}(L_{p,q}/\mathbb{Q})$, with at least one edge $p \to q$ encoding a strictly smaller quotient than the maximal local quotient $G_p/N_p$.

In both cases, there is no canonical homomorphism between the Galois groups $G_q$ and $G_p$ attached to different levels of the tree; what is canonical is the collection of surjective maps $\pi_{p,q} : G_p \twoheadrightarrow \mathrm{Gal}(L_{p,q}/\mathbb{Q})$ attached to the edges, together with the combinatorial structure of the tree itself.

### 7.3 First examples of non–primitive element primes: $p = 43$ and $p = 101$

Recall that for a prime $p$ we write $f_p \in \mathbb{Q}[x]$ for the polynomial defined in the beginning, and we fix a splitting field

$$K_p/\mathbb{Q}, \qquad G_p := \mathrm{Gal}(K_p/\mathbb{Q}),$$

together with a root $\alpha_p$ of $f_p$ in $K_p$. We denote

$$d_p := \deg f_p = [\mathbb{Q}(\alpha_p) : \mathbb{Q}], \qquad N_p := \mathrm{Gal}\big(K_p/\mathbb{Q}(\alpha_p)\big),$$

so that $[G_p : N_p] = d_p$. For each prime divisor $q \mid (p-1)$ we consider

$$\beta_{p,q} := f_q(\alpha_p) \in K_p, \qquad \Omega_{p,q} := G_p \cdot \beta_{p,q},$$

and set

$$H_{p,q} := \mathrm{Stab}_{G_p}(\beta_{p,q}), \qquad L_{p,q} := K_p^{H_{p,q}} = \mathbb{Q}(\beta_{p,q}).$$

By PG10 we have

$$|\Omega_{p,q}| = [G_p : H_{p,q}] = [L_{p,q} : \mathbb{Q}] \quad \text{and} \quad N_p \subseteq H_{p,q}.$$

**Definition 7.13.** A prime $p$ is called a *primitive element prime* if for every prime divisor $q \mid (p-1)$ we have

$$|\Omega_{p,q}| = d_p,$$

equivalently, $\mathbb{Q}(\beta_{p,q}) = \mathbb{Q}(\alpha_p)$ for all $q \mid (p-1)$.

For all primes $2 \le p \le 37$ our computations satisfy this condition, so all these primes are primitive element primes. The next two primes $p = 43$ and $p = 101$ provide the first examples where this fails.

**Example 7.14** (The prime $p = 43$)**.** For $p = 43$ we compute

$$d_{43} = \deg f_{43} = 4, \qquad [K_{43} : \mathbb{Q}] = 8, \qquad |G_{43}| = 8,$$

so $|N_{43}| = |G_{43}|/d_{43} = 8/4 = 2$.

The prime divisors of 42 are $2, 3, 7$. From the Sage output we obtain:

- For $q = 2$:

$$|\Omega_{43,2}| = 4 = d_{43}, \quad [L_{43,2} : \mathbb{Q}] = 4, \quad |H_{43,2}| = \frac{|G_{43}|}{|\Omega_{43,2}|} = \frac{8}{4} = 2.$$

- For $q = 3$:

$$|\Omega_{43,3}| = 4 = d_{43}, \quad [L_{43,3} : \mathbb{Q}] = 4, \quad |H_{43,3}| = \frac{8}{4} = 2.$$

- For $q = 7$:

$$|\Omega_{43,7}| = 2 < d_{43}, \quad [L_{43,7} : \mathbb{Q}] = 2, \quad |H_{43,7}| = \frac{8}{2} = 4.$$

Since $N_{43}$ has order 2, it follows from $|H_{43,2}| = |H_{43,3}| = 2$ and $N_{43} \subseteq H_{43,q}$ that

$$H_{43,2} = H_{43,3} = N_{43}, \qquad L_{43,2} = L_{43,3} = \mathbb{Q}(\alpha_{43}).$$

For $q = 7$, on the other hand, we obtain a proper subgroup

$$N_{43} \subsetneq H_{43,7} \subsetneq G_{43},$$

and a proper intermediate field

$$\mathbb{Q} \subset L_{43,7} \subsetneq \mathbb{Q}(\alpha_{43}) \subset K_{43}$$

with $[L_{43,7} : \mathbb{Q}] = 2 < 4 = [\mathbb{Q}(\alpha_{43}) : \mathbb{Q}]$.

In particular, 43 is *not* a primitive element prime, since there exists a divisor $q = 7$ of 42 for which $|\Omega_{43,7}| < d_{43}$ holds.

**Example 7.15** (The prime $p = 101$)**.** For $p = 101$ we obtain

$$d_{101} = \deg f_{101} = 6, \qquad [K_{101} : \mathbb{Q}] = 12, \qquad |G_{101}| = 12,$$

so $|N_{101}| = |G_{101}|/d_{101} = 12/6 = 2$.

The prime divisors of 100 are 2 and 5. The computed data are:

- For $q = 2$:

$$|\Omega_{101,2}| = 6 = d_{101}, \quad [L_{101,2} : \mathbb{Q}] = 6, \quad |H_{101,2}| = \frac{12}{6} = 2.$$

- For $q = 5$:

$$|\Omega_{101,5}| = 3 < d_{101}, \quad [L_{101,5} : \mathbb{Q}] = 3, \quad |H_{101,5}| = \frac{12}{3} = 4.$$

As above, from $|N_{101}| = 2$ and $N_{101} \subseteq H_{101,q}$ we deduce that

$$H_{101,2} = N_{101}, \qquad L_{101,2} = \mathbb{Q}(\alpha_{101}),$$

whereas

$$N_{101} \subsetneq H_{101,5} \subsetneq G_{101}$$

and

$$\mathbb{Q} \subset L_{101,5} \subsetneq \mathbb{Q}(\alpha_{101}) \subset K_{101}$$

with $[L_{101,5} : \mathbb{Q}] = 3 < 6 = [\mathbb{Q}(\alpha_{101}) : \mathbb{Q}]$.

Thus 101 is also not a primitive element prime: for $q = 5 \mid 100$ the orbit size $|\Omega_{101,5}|$ is strictly smaller than $d_{101}$.

**Remark 7.16.** For all tested primes $2 \le p \le 37$ the data satisfy the condition $|\Omega_{p,q}| = d_p$ for all $q \mid (p-1)$, so these $p$ are primitive element primes. The examples $p = 43$ and $p = 101$ show that the "optimal" Case (a) does *not* hold in general, and they explicitly illustrate the mechanism described in Case (b), where for some $q \mid (p-1)$ proper intermediate fields $L_{p,q}$ between $\mathbb{Q}$ and $\mathbb{Q}(\alpha_p)$ occur.

# 8 PEP primes and the recursive class Pr

The computational data suggest separating a local notion from its recursive global analogue. Let $p$ be a prime and let

$$K_p = \mathrm{Spl}(f_p/\mathbb{Q}).$$

For every prime divisor $q \mid (p-1)$ we consider the set

$$\Omega_{p,q} = \{\sigma(f_q(\alpha)) : \sigma \in \mathrm{Gal}(K_p/\mathbb{Q})\},$$

where $\alpha$ is any root of $f_p(x)$. Since $f_p(x)$ is irreducible, the cardinality of $\Omega_{p,q}$ does not depend on the choice of $\alpha$.

**Definition 8.1.** A prime $p$ is called a *primitive element prime*, abbreviated *PEP prime*, if for every prime divisor $q$ of $p-1$ one has

$$|\Omega_{p,q}| = \deg(f_p).$$

Equivalently, for every such $q$, the element $f_q(\alpha)$ has the same degree over $\mathbb{Q}$ as $\alpha$ itself.

This is exactly the local "Case A" condition at the vertex $p$: every child $q \mid (p-1)$ gives rise to a full orbit of cardinality $\deg(f_p)$.

The recursive class that naturally corresponds to the global Case A scenario is obtained by requiring the same phenomenon at every vertex of the Pratt–Galois tree.

**Definition 8.2.** The class Pr of *Pr primes* is the smallest class of primes satisfying the following conditions. First, $2 \in \mathrm{Pr}$. Second, if $p$ is an odd prime, then

$$p \in \mathrm{Pr}$$

if and only if $p$ is a PEP prime and every prime divisor $q$ of $p-1$ also belongs to Pr.

Thus a prime belongs to Pr precisely when every vertex of its Pratt–Galois tree lies in Case A. The definition is well posed, since every prime divisor $q$ of $p-1$ satisfies $q < p$, so the recursion runs strictly downward.

There is a convenient algebraic reformulation of the PEP condition which avoids explicit splitting fields. If $p$ and $q$ are primes with $q \mid (p-1)$, let

$$R_{p,q}(T) = \mathrm{Res}_x\big(f_p(x),\, T - f_q(x)\big) \in \mathbb{Q}[T].$$

The roots of $R_{p,q}(T)$ are precisely the values $f_q(\alpha_i)$ obtained from the roots $\alpha_i$ of $f_p(x)$. Hence the degree of the squarefree part of $R_{p,q}(T)$ is exactly $|\Omega_{p,q}|$. Consequently $p$ is a PEP prime if and only if for every $q \mid (p-1)$ the squarefree part of $R_{p,q}(T)$ has degree $\deg(f_p)$.

The first computations show that the class Pr is rather large, but not equal to the set of all primes. The first failures already occur at

$$43 \qquad \text{and} \qquad 101.$$

Indeed, for $p = 43$ one has $\deg(f_{43}) = 4$, but the orbit attached to $q = 7$ has cardinality $|\Omega_{43,7}| = 2$, so 43 is not a PEP prime and therefore not a Pr prime. Likewise, for $p = 101$ one has $\deg(f_{101}) = 6$, whereas $|\Omega_{101,5}| = 3$, so again the local Case A condition fails. By contrast, the displayed data show that

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$$

all satisfy Case A at the root, and therefore lie in Pr because the same is true recursively for all lower vertices.

A systematic computation based on the resultant criterion yields the following first one hundred Pr primes:

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 103, 107, 109, 113,$
$127, 131, 137, 139, 149, 151, 163, 167, 179, 181, 191, 193, 197, 199, 211, 227, 229, 233, 239, 241, 251,$
$257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 349, 353, 359, 367, 373, 379, 383,$
$389, 397, 409, 419, 421, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521,$
$523, 541, 547, 557, 563, 569, 571, 577, 587, 593.$

These data suggest that Pr is much denser than one might first expect from the exceptional examples 43 and 101, but still thin enough to carry nontrivial arithmetic information. In particular, Pr is closed under the recursive descent forced by the Pratt tree, and therefore behaves much more like a genuinely self-similar prime class than a condition imposed only at the top vertex.

## References


[1] mathoverflowUser, *Abelian characters and odd perfect numbers?*, MathOverflow question 458100, 2023, `https://mathoverflow.net/questions/458100/abelian-characters-and-odd-perfect-numbers`.

[2] O. Leka, *Pratt–Galois tree data*, text file, available at `https://www.orges-leka.de/pratt_galois_tree_data.txt`.

[3] O. Leka, *Pratt–Galois tree Sage script*, SageMath script, available at `https://www.orges-leka.de/pratt_galois_tree_sage_script.sage`.

[4] O. Leka, *Polynomials for natural numbers and irreducible polynomials for prime numbers*, LaTeX source available at `https://www.orges-leka.de/polynomials_and_perfect_numbers.tex`.

[5] O. Leka, *Polynomials for natural numbers and irreducible polynomials for prime numbers*, MathOverflow question, available at `https://mathoverflow.net/questions/483571/polynomials-for-natural-numbers-and-irreducible-polynomials-for-prime-numbers`.

# A Small examples and a short table

The following data points are the ones used in the examples above.

| $p$ | $f_p(x)$ | $\deg f_p$ | $\mathrm{Gal}(f_p/\mathbb{Q})$ |
|---|---|---|---|
| 2 | $x$ | 1 | 1 |
| 3 | $x+1$ | 1 | 1 |
| 5 | $x^2+1$ | 2 | $C_2$ |
| 7 | $x^2+x+1$ | 2 | $C_2$ |
| 11 | $x^3+x+1$ | 3 | $S_3$ |
| 31 | $x^4+x^3+x^2+x+1$ | 4 | $C_4$ |
| 127 | $x^5+3x^4+4x^3+3x^2+x+1$ | 5 | $D_5$ |

These examples are compatible with the larger computational tables in the original paper.