Polynomials and perfect numbers

Orges Leka

December 4, 2025

Abstract

This article is a first step towards a systematic connection between the classical theory of perfect numbers and the Galois theory of polynomials. We view perfect numbers through the lens of field extensions generated by suitably chosen polynomials, and ask to what extent the perfection condition

$$\sigma(n) = 2n$$

can be expressed or detected in Galois-theoretic terms. After recalling the basic notions about perfect numbers and Galois groups, we introduce families of polynomials whose arithmetic encodes divisor-sum information, and we investigate how properties of their splitting fields and discriminants reflect the (im)perfection of the integers they parametrize. Several explicit examples and small computational experiments illustrate the phenomena that occur. Rather than aiming at definitive classification results, our goal is to formulate a conceptual framework and to isolate concrete questions that might guide further work. We conclude by listing a collection of open problems and directions, both on the side of perfect numbers and on the side of Galois groups, where the interaction between the two theories appears particularly promising.

Contents

1 Introduction

Perfect numbers occupy a central place in classical number theory. By definition, a positive integer n is *perfect* if the sum of its positive divisors satisfies $\sigma(n) = 2n$. The even perfect numbers are completely described by the ancient Euclid–Euler theorem, which shows that every even perfect number has the form

$$n = 2^{p-1}(2^p - 1),$$

where $2^p - 1$ is prime. In contrast, essentially nothing is known about odd perfect numbers: it is not even known whether any exist. This mixture of elementary definitions and deep open problems has inspired a substantial literature.

Galois theory, on the other hand, provides a powerful language for understanding the algebraic and arithmetic properties of polynomials. Given a polynomial $f(x) \in \mathbb{Q}[x]$, the structure of its Galois group over $\mathbb{Q}$, together with invariants such as its discriminant and ramification data, encode subtle information about the arithmetic of the values of f and of the fields cut out by its roots.

The aim of this paper is to explore a first connection between these two worlds. Very loosely, we ask:

> *Can the condition that an integer be perfect (or nearly perfect) be interpreted in terms of the Galois theory of naturally associated polynomials?*

Our approach is deliberately modest. We begin by recalling the necessary background on perfect numbers and on Galois groups, keeping the exposition self-contained and focused on the examples used later. We then introduce specific families of polynomials whose coefficients and values are designed to reflect divisor-sum information. For these families, we study the associated splitting fields and their Galois groups, and we examine how perfection (or the failure of perfection) manifests itself in the algebraic data.

This article should be viewed as a starting point rather than a culmination. The results obtained here are mostly of an illustrative nature: they show that interesting patterns do appear, and they suggest several conjectural links between classical questions on perfect numbers and natural problems in inverse Galois theory.

Structure of the paper. The paper is organised as follows.

- **Section 1** defines the recursive polynomial family $f_n(x)$ and establishes the fundamental connection between integer divisibility and field inclusions. It applies this framework to describe the field towers associated with perfect numbers.
- **Section 2** classifies polynomials and integers by their parity types (g-, u-, and m-types). We analyse the distribution of these types among primes and discuss the algebraic properties of the set S_4.
- **Section 3** investigates the solvability of the associated Galois groups. We prove that if the defining parameter k of a k-perfect number involves a prime with a non-solvable group, the global Galois group inherits this property.
- **Section 4** recalls standard results on cyclotomic polynomials and derives the basic cyclotomic factorisation of the divisor sum function $\sigma(N)$.
- **Section 5** refines the previous analysis to provide a precise description of the radical $\mathrm{rad}(\sigma(n))$ in terms of prime divisors of cyclotomic values.

- **Section 6** introduces the auxiliary family of multiplicative cyclotomic polynomials $g_n(x)$. We determine their splitting fields and Galois groups, contrasting them with the recursive family $f_n(x)$.
- **Section 7** returns to the recursive polynomials $f_n(x)$, studying the transitive action of the Galois group on the roots. We define and analyse the orbits $\Omega_{p,q}$ arising from the divisors of $p-1$.
- **Section 8** specialises the Galois–Pratt analysis to Mersenne primes. We describe how the stabilizer subgroups of the Galois action mirror the structure of the Pratt tree for these primes.
- **Section 9** incorporates Zsigmondy's Theorem into our framework. We identify primitive prime divisors within the cyclotomic factors and link them to specific Galois orbits.
- **Section 10** synthesises the results on Zsigmondy primes and Galois data. We distinguish the behavior of even perfect numbers from hypothetical odd perfect numbers within this setting.
- **Section 11** concludes the paper with a summary of the conceptual framework and a list of open problems at the interface of perfect numbers and inverse Galois theory.

2 Field Towers for the Polynomials $f_n(x)$ and Applications to Perfect Numbers

In this section we summarise the Galois–theoretic relations among the polynomials $f_n(x)$ as introduced in the MathOverflow discussions "polynomials for natural numbers" and "are most primes symmetric?" We then apply these relations to perfect numbers using the identity

$$\operatorname{rad}(\sigma(n)) = \begin{cases} \operatorname{rad}(n), & n \text{ even}, \\ 2\operatorname{rad}(n), & n \text{ odd}. \end{cases}$$

2.1 Definition and fundamental properties of $f_n(x)$

We assume the following axioms, all proved in the cited MO threads and the paper of Leka:

(1) (*Prime case*) For primes $p > 2$,

$$f_p(x) = 1 + \prod_{q \mid p-1} f_q(x)^{v_q(p-1)}, \qquad f_2(x) = x.$$

(2) (*Multiplicativity*)

$$f_{mn}(x) = f_m(x)\, f_n(x) \qquad \forall m, n \in \mathbb{N}.$$

(3) (*Prime-power rule*) If $n = \prod_p p^{a_p}$ then

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

(4) (*Evaluation*)

$$f_n(2) = n \qquad \forall n \geq 1.$$

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

(6) (*Separability*) $f_n(x)$ is separable if and only if n is squarefree.

A key consequence is the following.

Proposition 2.1 (Radical factorisation)**.** *For every $n \in \mathbb{N}$,*

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

Proof. By (3), $f_n(x) = \prod_{p|n} f_p(x)^{a_p}$. Irreducibility of f_p implies that all these factors are distinct. Taking the polynomial radical reduces all exponents to 1. □

2.2 Squarefree integers and field inclusions

Let n be squarefree:

$$n = p_1 p_2 \cdots p_r.$$

Then

$$f_n(x) = \prod_{i=1}^{r} f_{p_i}(x)$$

is a product of distinct irreducible polynomials. Let K_n denote the splitting field of f_n over $\mathbb{Q}$.

For any divisor $d \mid n$, write

$$d = \prod_{i \in I} p_i, \qquad f_d(x) = \prod_{i \in I} f_{p_i}(x),$$

and let K_d be its splitting field.

Theorem 2.2 (Field inclusion)**.** *For every squarefree n and $d \mid n$,*

$$K_d \subseteq K_n.$$

Proof. Every root of f_d is a root of f_n, hence $K_d \subseteq K_n$. □

Theorem 2.3 (Galois groups as quotients)**.** *Let*

$$G_n = \operatorname{Gal}(K_n/\mathbb{Q}), \qquad G_d = \operatorname{Gal}(K_d/\mathbb{Q}).$$

Then the restriction map

$$\operatorname{res}\colon G_n \to G_d, \qquad \sigma \mapsto \sigma|_{K_d},$$

is surjective with kernel $\operatorname{Gal}(K_n/K_d)$*. Thus*

$$G_d \;\cong\; G_n/\operatorname{Gal}(K_n/K_d).$$

Thus $\operatorname{Gal}(f_d)$ is canonically a *quotient* of a subgroup of $\operatorname{Gal}(f_n)$.

Remark 2.4. If the splitting fields K_{p_i} of the prime-index polynomials f_{p_i} are linearly disjoint over $\mathbb{Q}$ (expected heuristically), then

$$G_n \cong \prod_{i=1}^{r} G_{p_i}, \qquad G_d \cong \prod_{i \in I} G_{p_i} \subseteq \prod_{i=1}^{r} G_{p_i},$$

so G_d embeds naturally as a subgroup of G_n.

2.3 Perfect numbers and reduction to the squarefree radical

Let n be a perfect number: $\sigma(n) = 2n$.

Even perfect numbers

Every even perfect number is of the form

$$n = 2^{p-1}(2^p - 1)$$

with $2^p - 1$ prime. Since 2 divides n,

$$\mathrm{rad}(\sigma(n)) = \mathrm{rad}(2n) = \mathrm{rad}(n) = 2(2^p - 1).$$

This is squarefree, and

$$f_{\mathrm{rad}(n)}(x) = f_2(x)\, f_{2^p-1}(x) = x\, f_{2^p-1}(x).$$

The factor x has trivial splitting field, hence

$$K_{\mathrm{rad}(n)} = K_{2^p-1}.$$

Thus the Galois structure of an even perfect number is completely determined by the irreducible polynomial $f_{2^p-1}(x)$ for the associated Mersenne prime.

Odd perfect numbers

If n is odd and perfect, then

$$\mathrm{rad}(\sigma(n)) = \mathrm{rad}(2n) = 2\ \mathrm{rad}(n).$$

Thus $m = 2\ \mathrm{rad}(n)$ is squarefree and

$$f_m(x) = f_2(x)\, f_{\mathrm{rad}(n)}(x).$$

Again $f_2(x) = x$ contributes no extension, so

$$K_m = K_{\mathrm{rad}(n)}.$$

Hence any odd perfect number (if it exists) is controlled by the splitting field of $f_{\mathrm{rad}(n)}(x)$, together with the prime 2.

2.4 Prime towers

Let

$$\mathrm{rad}(n) = p_1 p_2 \cdots p_r$$

list the distinct prime divisors of n, and include $p_1 = 2$ if n is odd. Define

$$m_k = p_1 p_2 \cdots p_k.$$

Theorem 2.5 (Prime tower for perfect numbers)**.** *For any perfect number n, the splitting fields satisfy a tower*

$$\mathbb{Q} \subseteq K_{m_1} \subseteq K_{m_2} \subseteq \cdots \subseteq K_{m_r} = K_{\mathrm{rad}(\sigma(n))},$$

and the Galois groups form a dual tower of surjective restriction maps

$$\mathrm{Gal}(K_{m_r}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K_{m_{r-1}}/\mathbb{Q}) \twoheadrightarrow \cdots \twoheadrightarrow \mathrm{Gal}(K_{m_1}/\mathbb{Q}).$$

Thus every prime factor of a perfect number contributes a new Galois quotient; even perfect numbers produce a trivial tower of height 2, while an odd perfect number would yield a long, nontrivial Galois tower.

3 g- and m-primes for the polynomials $f_n(x)$

In this section we work with the family of polynomials $f_n(x) \in \mathbb{Z}[x]$ defined in the MathOverflow discussions *"polynomials for natural numbers"* and *"are most primes symmetric?"*. We only use the following axioms.

- $f_1(x) = 1$, $f_2(x) = x$.
- For every prime $p > 2$,

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

- For all $n = \prod_p p^{v_p(n)}$,

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

From these axioms one easily checks by induction on n that:

Lemma 3.1. *For all $n \in \mathbb{N}$,*

1. *$f_n(x)$ has nonnegative integer coefficients.*
2. *$f_n(2) = n$.*
3. *$f_2(0) = 0$, and for every odd prime p, $f_p(0) = 1$.*
4. *Consequently, for every n,*

$$f_n(0) = \prod_{p|n} f_p(0)^{v_p(n)} = \begin{cases} 0, & n \text{ even}, \\ 1, & n \text{ odd}. \end{cases}$$

Proof. (1) and (3) follow inductively from the defining formulas and the fact that products and sums of polynomials with nonnegative integer coefficients again have nonnegative integer coefficients. Item (2) is proved by the same induction using only the scalar evaluations at $x = 2$. Finally (4) is a direct consequence of (3) and the multiplicative formula for $f_n(x)$. □

3.1 Parity types: g-, u- and m-numbers

We classify polynomials and integers via parity symmetry.

Definition 3.2. For a polynomial $F(x) \in \mathbb{R}[x]$ we say:

- F is of *g-type* (even) if $F(-x) = F(x)$ for all x,
- F is of *u-type* (odd) if $F(-x) = -F(x)$ for all x,
- F is of *m-type* (mixed) otherwise.

We write $T(F) \in \{\mathrm{G}, \mathrm{U}, \mathrm{M}\}$ for its type.

For each $n \in \mathbb{N}$ we define:

- n is a *g-number* if $f_n(x)$ is of g-type,

- n is a *u-number* if $f_n(x)$ is of u-type,
- n is an *m-number* otherwise.

A *g-prime* (resp. u-prime, m-prime) is a prime p which is a g-number (resp. u-number, m-number).

Every polynomial F can be written uniquely as

$$F(x) = E_F(x) + O_F(x),$$

with E_F even and O_F odd. Then

$$T(F) = \begin{cases} \text{G}, & O_F = 0, \\ \text{U}, & E_F = 0 \neq O_F, \\ \text{M}, & E_F \neq 0 \neq O_F. \end{cases}$$

3.2 Type tables for sums and products

We first prove the tables stated in the MO post.

Lemma 3.3 (Sum table)**.** *Let $F, G \in \mathbb{R}[x]$ with types in $\{\text{G}, \text{U}, \text{M}\}$. Assuming neither F nor G is the zero polynomial, the type of $F + G$ is given by*

+	G	U	M
G	G	M	M
U	M	U	M
M	M	M	M

(i.e. this is exactly the table written in the question).

Proof. Write $F = E_F + O_F$, $G = E_G + O_G$. Then

$$F + G = (E_F + E_G) + (O_F + O_G),$$

where the first bracket is even and the second odd.

If both F, G are even, then $O_F = O_G = 0$ and $F + G$ is even, giving G+G=G. If both are odd, then $E_F = E_G = 0$ and $F + G$ is odd, giving U+U=U.

If F is even and G odd, then $E_F \neq 0, O_F = 0, E_G = 0, O_G \neq 0$. Thus both the even and odd parts of $F + G$ are nonzero, so $F + G$ is mixed: G+U = M, and by symmetry U+G = M.

If one summand is mixed, then both its even and odd parts are nonzero; adding any nonzero polynomial leaves at least one of those parts nonzero, hence the sum is mixed. This yields all the entries involving M. □

Lemma 3.4 (Product table)**.** *Let $F, G \in \mathbb{R}[x]$ be nonzero. Then the type of FG is*

*	G	U	M
G	G	U	M
U	U	G	M
M	M	M	M

again exactly as in the question.

Proof. Using $F = E_F + O_F$, $G = E_G + O_G$, we have

$$FG = E_F E_G \ + \ E_F O_G + O_F E_G \ + \ O_F O_G.$$

Even*even and odd*odd are even; even*odd and odd*even are odd. Thus the even part is $E_F E_G + O_F O_G$, the odd part is $E_F O_G + O_F E_G$.

- If both F, G are even, then $O_F = O_G = 0$, so FG is even (G*G=G).
- If both are odd, then $E_F = E_G = 0$, so FG is even (U*U=G).
- If exactly one is odd and the other even, then exactly one of $E_F O_G, O_F E_G$ is nonzero and both $E_F E_G, O_F O_G$ vanish, so FG is odd (G*U=U and U*G=U).
- If at least one factor is mixed, it has nonzero even and odd parts. Multiplying by any nonzero polynomial produces both a nonzero even and a nonzero odd part, so the product is mixed. This covers all cases involving M.

□

3.3 Classification of g- and u-numbers in terms of primes

We now express the type of n in terms of the types of its prime divisors.

Lemma 3.5. *Let $n = \prod_p p^{v_p(n)}$. Then*

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

In particular,

- *if some prime factor $p \mid n$ is an m-prime, then n is an m-number,*
- *otherwise, all odd primes dividing n are g-primes and the only possible non-g-prime factor is 2.*

Proof. The displayed factorisation is one of the axioms. If some factor f_p with $p \mid n$ is of type M, then by Lemma 3.4 every product containing it is of type M, so f_n is mixed and n an m-number.

If no prime factor is of type M, then every odd prime factor is of type G (since Lemma 3.1(3) shows that no odd prime can be of u-type, see below), and the only prime which can be of type U is 2. □

We now sharpen this and obtain an exact description of g- and u-numbers.

Lemma 3.6 (The only u-prime)**.** *The only u-prime is 2.*

Proof. For $p = 2$ we have $f_2(x) = x$, which is odd, so 2 is a u-prime.

Let $p > 2$ be an odd prime. By Lemma 3.1(3), $f_p(0) = 1 \neq 0$. An odd polynomial must vanish at 0; therefore $f_p(x)$ cannot be odd. Hence no odd prime is a u-prime. □

Proposition 3.7 (Structure of g- and u-numbers)**.** *Let $n \in \mathbb{N}$. Write $a = v_2(n)$. Assume that no prime divisor $p \mid n$ is an m-prime. Then:*

1. *If a is even, then n is a g-number.*

2. If a is odd, then n is a u-number.

Equivalently, if we let $\mathbb{G} \subset \mathbb{N}$ denote the set of g-numbers, then for all n with no m-prime factor we have

$$n \in \mathbb{G} \iff n = 2^{2k} \prod_{\substack{p \neq 2 \\ p \mid n}} p^{v_p(n)} \quad \text{for some } k \geq 0,$$

and

$$n \text{ a u-number} \iff n = 2^{2k+1} \prod_{\substack{p \neq 2 \\ p \mid n}} p^{v_p(n)} \quad \text{for some } k \geq 0.$$

Proof. By assumption, every odd prime divisor $p \mid n$ is a g-prime, so each factor $f_p(x)$ is even (type G). Write $n = 2^a m$ with m odd. Then

$$f_n(x) = f_{2^a}(x)\, f_m(x), \qquad f_m(x) = \prod_{p \mid m} f_p(x)^{v_p(m)}$$

is a product of even polynomials, hence even. On the other hand $f_{2^a}(x) = x^a$ (because $f_2 = x$ and $f_{2^a} = f_2^a$), so f_{2^a} is odd iff a is odd and even iff a is even.

Now apply Lemma 3.4 to the product $f_{2^a} \cdot f_m$. If a is even, then both factors are even and f_n is even (a g-number). If a is odd, then one factor is odd and the other even, so the product is odd (a u-number).

The displayed characterisations follow by spelling out the condition "no prime divisor is an m-prime" and the parity of $a = v_2(n)$. □

Combining Lemma 3.5 and Proposition 3.7 we obtain exactly statement (3) from the MO question:

Corollary 3.8 (Characterisation of g-numbers)**.** *Let $\mathbb{G}$ denote the set of g-numbers. Then*

$$n \in \mathbb{G} \iff n = 2^{2k} \prod_{\substack{p \neq 2 \\ p \mid n,\, p \in \mathbb{G}}} p^{v_p(n)} \quad \text{for some } k \geq 0.$$

3.4 g-primes and factorisation of $p - 1$

We now relate the type of a prime p to that of $p - 1$.

Lemma 3.9. *Let $p > 2$ be prime. Then*

$$f_p(x) = 1 + f_{p-1}(x).$$

Proof. By definition,

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

But the right-hand product is exactly the defining factorisation of $f_{p-1}(x)$. Hence the identity. □

The constant polynomial 1 is even, so adding it to a polynomial preserves evenness and never creates evenness from an odd polynomial.

Lemma 3.10. *Let $F(x)$ be a polynomial. Then $1 + F$ is even if and only if F is even.*

Proof. If F is even, then $1+F$ is the sum of two even polynomials and hence even. Conversely, if $1+F$ is even, then

$$F = (1+F) - 1$$

is a difference of even polynomials and hence even. □

Proposition 3.11 (g-primes via $p-1$)**.** *Let $p > 2$ be prime. Then*

$$p \text{ is a g-prime} \iff p-1 \text{ is a g-number.}$$

Equivalently, if $\mathbb{G}$ is the set of g-numbers, then

$$p \text{ is a g-prime} \iff p-1 = 2^{2k} \prod_{\substack{q \neq 2 \\ q \mid p-1,\, q \in \mathbb{G}}} q^{v_q(p-1)} \quad \text{for some } k \geq 0.$$

This is precisely statement (2) *in the MO question.*

Proof. By Lemma 3.9 and Lemma 3.10, f_p is even if and only if f_{p-1} is even. Thus p is a g-prime iff $p-1$ is a g-number.

The explicit factorisation condition follows by applying Corollary 3.8 to the integer $n = p-1$. □

3.5 m-primes from primes $p \equiv 1 \pmod 3$

We now justify the statement (due to Jonathan Love) that all primes $p \equiv 1 \pmod 3$ are m-primes.

First we compute $f_3(x)$. Since $3-1=2$, we have

$$f_3(x) = 1 + f_2(x)^{v_2(2)} = 1 + x = x + 1.$$

Lemma 3.12. *Let $p \equiv 1 \pmod 3$, so $p-1 = 3k$ for some $k \in \mathbb{N}$. Then*

$$f_p(x) = f_{3k}(x) + 1 = f_3(x) f_k(x) + 1 = (x+1) f_k(x) + 1.$$

Proof. From Lemma 3.9 we have $f_p(x) = 1 + f_{p-1}(x)$ and $p-1 = 3k$. Using the multiplicativity of f_n,

$$f_{3k}(x) = f_3(x) f_k(x),$$

and substituting $f_3(x) = x+1$ gives the claimed formula. □

Lemma 3.13. *For every n, $f_n(1) \geq 1$.*

Proof. By Lemma 3.1(1), all coefficients of $f_n(x)$ are nonnegative. Hence $f_n(1)$ is a sum of nonnegative integers. For $n \geq 1$ there is at least one nonzero coefficient, so $f_n(1) \geq 1$. □

Proposition 3.14 (Primes $p \equiv 1 \pmod 3$ are m-primes)**.** *Let $p \equiv 1 \pmod 3$ be prime. Then p is an m-prime.*

Proof. By Lemma 3.12,

$$f_p(1) = (1+1) f_k(1) + 1 = 2 f_k(1) + 1 > 1$$

by Lemma 3.13, while

$$f_p(-1) = ((-1)+1) f_k(-1) + 1 = 0 \cdot f_k(-1) + 1 = 1.$$

Thus

$$f_p(1) > 1 = f_p(-1).$$

In particular,

$$f_p(1) \neq f_p(-1) \quad \text{and} \quad f_p(1) \neq -f_p(-1),$$

so f_p is neither even nor odd. Hence p is an m-prime. □

Combining this with Dirichlet's theorem on primes in arithmetic progressions (which asserts that there are infinitely many primes $p \equiv 1 \pmod 3$), one obtains:

Corollary 3.15 (Infinitely many m-primes, conditional on Dirichlet)**.** *Assuming Dirichlet's theorem, there are infinitely many m-primes.*

Proof. Dirichlet's theorem gives infinitely many primes $p \equiv 1 \pmod 3$, and Proposition 3.14 shows that each such prime is an m-prime. □

3.6 The set S_4 and its multiplicativity

We now discuss the auxiliary set S_4 and its relation to g-primes, as in the MO question.

Definition 3.16. Define

$$S_4 := \{\, n \in \mathbb{N} : f_{f_n(4)}(x) = f_n(x^2) \text{ for all real } x \,\}.$$

Lemma 3.17. *The set S_4 is multiplicative: if $a, b \in S_4$, then $ab \in S_4$.*

Proof. Assume $a, b \in S_4$. Then

$$f_{f_a(4)}(x) = f_a(x^2), \qquad f_{f_b(4)}(x) = f_b(x^2).$$

By multiplicativity of f_n,

$$f_{ab}(x) = f_a(x) f_b(x),$$

and therefore

$$f_{ab}(x^2) = f_a(x^2) f_b(x^2) = f_{f_a(4)}(x)\, f_{f_b(4)}(x).$$

On the other hand,

$$f_{f_{ab}(4)}(x) = f_{\,f_a(4)\, f_b(4)}(x) = f_{f_a(4)}(x)\, f_{f_b(4)}(x),$$

again by multiplicativity, since $f_{mn} = f_m f_n$ for all m, n. Thus

$$f_{f_{ab}(4)}(x) = f_{ab}(x^2),$$

so $ab \in S_4$. □

Hence S_4 is multiplicative in the standard sense of multiplicative number theory. This justifies step (2) in the Euler-product strategy sketched in the MO post.

Proposition 3.18 (Euler product over S_4)**.** *For any real $s > 0$ such that the series*

$$\sum_{n \in S_4} \frac{1}{n^s}$$

converges absolutely, we have the Euler product identity

$$\sum_{n \in S_4} \frac{1}{n^s} = \prod_{\substack{p \in S_4 \\ p \text{ prime}}} \frac{1}{1 - p^{-s}}.$$

Proof. Because S_4 is multiplicative (Lemma 3.17), every $n \in S_4$ admits a factorisation

$$n = \prod_p p^{e_p},$$

where the product is over primes $p \in S_4$ and all but finitely many exponents e_p are zero. (Primes not in S_4 necessarily have exponent zero, since otherwise their product with $1 \in S_4$ would lie in S_4, contradiction.)

Absolute convergence allows us to rearrange terms, giving

$$\sum_{n \in S_4} \frac{1}{n^s} = \prod_{\substack{p \in S_4 \\ p \text{ prime}}} \left(\sum_{e=0}^{\infty} p^{-es} \right) = \prod_{\substack{p \in S_4 \\ p \text{ prime}}} \frac{1}{1 - p^{-s}}.$$

□

Proposition 3.19 (Divergence ⇒ infinitely many primes in S_4)**.** *If for some $s > 0$ the series*

$$\sum_{n \in S_4} \frac{1}{n^s}$$

diverges, then S_4 contains infinitely many primes.

Proof. Suppose, for contradiction, that only finitely many primes lie in S_4. Then the Euler product in Proposition 3.18 is a finite product of convergent geometric series, hence convergent for all $s > 0$. Therefore the series $\sum_{n \in S_4} n^{-s}$ would converge for that s, contradicting the assumed divergence. □

Finally, we connect S_4 back to g-numbers.

Lemma 3.20. *If $n \in S_4$, then $m := f_n(4)$ is a g-number.*

Proof. By definition of S_4, we have

$$f_m(x) = f_{f_n(4)}(x) = f_n(x^2).$$

The polynomial $f_n(x^2)$ is a function of x^2 only, hence even:

$$f_n((-x)^2) = f_n(x^2).$$

Thus $f_m(x)$ is even, so m is a g-number. □

In particular, if one knows (from prior results on the family $f_n(x)$) that whenever $n = p > 2$ is prime and $p \in S_4$ the integer $q := f_p(4)$ is itself prime, then Lemma 3.20 shows that q is in fact a g-prime. Combining this with Proposition 3.19 gives the final step of the MO strategy: divergence of $\sum_{n \in S_4} n^{-s}$ for some $s > 0$ would imply infinitely many g-primes.

To summarise, all purely algebraic statements in the MathOverflow discussion about g- and m-primes follow from the axioms of the polynomials $f_n(x)$ and the parity-type analysis above:

- the sum and product type tables,
- the classification of g-numbers and u-numbers,

- the characterisation of g-primes via the factorisation of $p-1$,
- the uniqueness of the u-prime 2,
- the fact that primes $p \equiv 1 \pmod 3$ are m-primes,
- and the multiplicativity and Euler-product framework for the set S_4.

The only genuinely analytic ingredient in the MO post is Dirichlet's theorem (primes in arithmetic progressions) and the conjectural divergence of the Dirichlet series over S_4, which we have used only as external input where explicitly indicated.

3.7 Data tables for small $f_n(x)$ and selected factorizations

4 Non-solvable Galois groups forced by k-perfect numbers

Recall that a positive integer N is called k-perfect if

$$\sigma(N) \;=\; k\,N$$

for some integer $k \geq 2$. We work with the polynomials $f_n(x)$ as in the previous section, so that in particular

$$f_n(x) \;=\; \prod_{p \mid n} f_p(x)^{v_p(n)}, \qquad f_p(x) \in \mathbb{Z}[x] \text{ irreducible for primes } p.$$

Define

$$m := \operatorname{rad}(\sigma(N)).$$

Then every prime divisor of $\sigma(N)$ divides m, and

$$f_m(x) \;=\; f_{\operatorname{rad}(\sigma(N))}(x) \;=\; \prod_{p \mid m} f_p(x).$$

Let K_m be the splitting field of $f_m(x)$ over $\mathbb{Q}$ and

$$G_m := \operatorname{Gal}\big(K_m/\mathbb{Q}\big)$$

its Galois group.

Proposition 4.1. *Let $k \geq 2$ and suppose there exists a k-perfect number N, i.e. $\sigma(N) = kN$. Assume that k is divisible by a prime p such that*

$$G_p := \operatorname{Gal}\big(f_p(x)/\mathbb{Q}\big)$$

is non-solvable. Then the Galois group

$$G_m = \operatorname{Gal}\big(f_{\operatorname{rad}(\sigma(N))}(x)/\mathbb{Q}\big)$$

is also non-solvable.

Proof. From $\sigma(N) = kN$ and $p \mid k$ we obtain $p \mid \sigma(N)$, hence $p \mid m = \operatorname{rad}(\sigma(N))$. By multiplicativity,

$$f_m(x) = f_{\operatorname{rad}(\sigma(N))}(x) = \prod_{q \mid m} f_q(x),$$

and in particular $f_p(x)$ divides $f_m(x)$ in $\mathbb{Z}[x]$.

Let K_p be the splitting field of $f_p(x)$ over $\mathbb{Q}$. Every root of f_p is a root of f_m, hence

$$K_p \subseteq K_m.$$

Thus we have a tower of fields

$$\mathbb{Q} \subseteq K_p \subseteq K_m.$$

Passing to Galois groups, set

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

The restriction map

$$\mathrm{res} : G_m \longrightarrow G_p, \qquad \sigma \mapsto \sigma|_{K_p},$$

is a surjective group homomorphism with kernel $\ker(\mathrm{res}) = \mathrm{Gal}(K_m/K_p)$. Hence

$$G_m/\,\mathrm{Gal}(K_m/K_p) \;\cong\; G_p.$$

Now G_p is non-solvable by assumption. A quotient of a solvable group is always solvable; therefore, if G_m were solvable, then every quotient of G_m would be solvable. This contradicts the fact that $G_m/\,\mathrm{Gal}(K_m/K_p) \cong G_p$ is non-solvable. Thus G_m itself must be non-solvable. □

Table 3: Galois groups $\mathrm{Gal}(f_p(x)/\mathbb{Q})$ for primes p

p	$\lvert\mathrm{Gal}(f_p)\rvert$	disc sign	ID	structure
2	1	1	1	S1
3	1	1	1	S1
5	2	-1	1	S2
7	2	-1	1	S2
11	6	-1	1	S3
13	6	-1	1	S3
17	4	1	1	E(4) = 2[x]2
19	6	-1	1	S3
23	24	-1	1	S4
29	24	-1	1	S4
31	4	-1	1	C(4) = 4
37	8	-1	1	D(4)
41	120	-1	1	S5
43	8	-1	1	D(4)
47	120	-1	1	S5
53	120	-1	1	S5
59	120	-1	1	S5
61	120	-1	1	S5
67	120	-1	1	S5
71	120	-1	1	S5
73	120	-1	1	S5
79	120	-1	1	S5
83	720	-1	1	S6
89	720	-1	1	S6

p	$\lvert \mathrm{Gal}(f_p) \rvert$	disc sign	ID	structure
97	720	-1	1	S6
101	12	-1	1	D(6) = S(3)[x]2
103	720	-1	1	S6
107	48	-1	1	2S_4(6) = [2^3]S(3) = 2 wr S(3)
109	120	-1	1	S5
113	720	-1	1	S6
127	10	1	1	D(5) = 5:2
131	720	-1	1	S6
137	5040	-1	1	S7
139	720	-1	1	S6
149	720	-1	1	S6
151	720	-1	1	S6
157	72	-1	1	F_36(6):2 = [S(3)^2]2 = S(3) wr 2
163	120	-1	1	S5
167	5040	-1	1	S7
173	720	-1	1	S6
179	5040	-1	1	S7
181	720	-1	1	S6
191	72	-1	1	F_36(6):2 = [S(3)^2]2 = S(3) wr 2
193	5040	-1	1	S7
197	72	-1	1	F_36(6):2 = [S(3)^2]2 = S(3) wr 2
199	72	-1	1	F_36(6):2 = [S(3)^2]2 = S(3) wr 2
211	72	-1	1	F_36(6):2 = [S(3)^2]2 = S(3) wr 2
223	48	-1	1	2S_4(6) = [2^3]S(3) = 2 wr S(3)
227	5040	-1	1	S7
229	720	-1	1	S6
233	5040	-1	1	S7
239	5040	-1	1	S7
241	5040	-1	1	S7
251	5040	-1	1	S7
257	8	1	2	4[x]2
263	5040	-1	1	S7
269	5040	-1	1	S7
271	48	-1	1	2S_4(6) = [2^3]S(3) = 2 wr S(3)
277	5040	-1	1	S7
281	5040	-1	1	S7
283	5040	-1	1	S7
293	5040	-1	1	S7
307	5040	-1	1	S7
311	5040	-1	1	S7
313	5040	-1	1	S7
317	5040	-1	1	S7
331	5040	-1	1	S7
337	5040	-1	1	S7
347	5040	-1	1	S7
349	5040	-1	1	S7
353	40320	-1	50	S8
359	40320	-1	50	S8

p	$\lvert \mathrm{Gal}(f_p) \rvert$	disc sign	ID	structure
367	5040	-1	1	S7
373	5040	-1	1	S7
379	720	-1	1	S6
383	5040	-1	1	S7
389	40320	-1	50	S8
397	5040	-1	1	S7
401	64	1	29	E(8):D_8=[2^3]D(4)
409	40320	-1	50	S8
419	5040	-1	1	S7
421	5040	-1	1	S7
431	5040	-1	1	S7
433	5040	-1	1	S7
439	5040	-1	1	S7
443	384	-1	44	[2^4]S(4)
449	40320	-1	50	S8
457	5040	-1	1	S7
461	40320	-1	50	S8
463	5040	-1	1	S7
467	40320	-1	50	S8
479	40320	-1	50	S8
487	720	-1	1	S6
491	5040	-1	1	S7
499	40320	-1	50	S8
503	40320	-1	50	S8
509	5040	-1	1	S7
521	40320	-1	50	S8
523	5040	-1	1	S7
541	5040	-1	1	S7
547	5040	-1	1	S7
557	40320	-1	50	S8
563	40320	-1	50	S8
569	40320	-1	50	S8
571	5040	-1	1	S7
577	1152	-1	47	[S(4)^2]2
587	40320	-1	50	S8
593	40320	-1	50	S8
599	40320	-1	50	S8
601	40320	-1	50	S8
607	40320	-1	50	S8
613	40320	-1	50	S8
617	40320	-1	50	S8
619	40320	-1	50	S8
631	5040	-1	1	S7
641	362880	-1	34	S9
643	40320	-1	50	S8
647	40320	-1	50	S8
653	5040	-1	1	S7
659	40320	-1	50	S8

p	$\lvert \mathrm{Gal}(f_p) \rvert$	disc sign	ID	structure
661	40320	-1	50	S8
673	40320	-1	50	S8
677	1152	-1	47	[S(4)^2]2
683	40320	-1	50	S8
691	384	-1	44	[2^4]S(4)
701	40320	-1	50	S8
709	1152	-1	47	[S(4)^2]2
719	362880	-1	34	S9
727	1152	-1	47	[S(4)^2]2
733	40320	-1	50	S8
739	128	-1	35	[2^4]D(4)
743	40320	-1	50	S8
751	40320	-1	50	S8
757	5040	-1	1	S7
761	40320	-1	50	S8
769	362880	-1	34	S9
773	362880	-1	34	S9
787	40320	-1	50	S8
797	40320	-1	50	S8
809	362880	-1	34	S9
811	5040	-1	1	S7
821	362880	-1	34	S9
823	362880	-1	34	S9
827	40320	-1	50	S8
829	40320	-1	50	S8
839	40320	-1	50	S8
853	40320	-1	50	S8
857	362880	-1	34	S9
859	40320	-1	50	S8
863	40320	-1	50	S8
877	40320	-1	50	S8
881	362880	-1	34	S9
883	5040	-1	1	S7
887	362880	-1	34	S9
907	40320	-1	50	S8
911	40320	-1	50	S8
919	40320	-1	50	S8
929	362880	-1	34	S9
937	40320	-1	50	S8
941	362880	-1	34	S9
947	40320	-1	50	S8
953	362880	-1	34	S9
967	40320	-1	50	S8
971	362880	-1	34	S9
977	362880	-1	34	S9
983	40320	-1	50	S8
991	40320	-1	50	S8
997	362880	-1	34	S9

5 Basic results on cyclotomic polynomials and perfect numbers

Let $\Phi_d(x)$ denote the dth cyclotomic polynomial. We briefly recall the standard properties we will use; see any text on algebraic number theory.

Proposition 5.1 (Basic properties of Φ_d)**.** *For each integer $n \geq 1$ there exist unique monic polynomials $\Phi_d(x) \in \mathbb{Z}[x]$ $(d \mid n)$ such that*

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

Moreover:

1. $\Phi_1(x) = x - 1$.
2. *For each $d \geq 1$, $\Phi_d(x)$ is irreducible over $\mathbb{Q}$.*
3. *For every $n \geq 1$ and every integer a we have the identity*

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

obtained by substituting $x = a$ in the factorisation above.

We now prove the factorisation used in Section 2 of the paper.

Proposition 5.2. *Let N be a perfect number with prime factorisation*

$$N = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Then

$$2N = \sigma(N) = \prod_{i=1}^{k} \sigma\big(p_i^{\alpha_i}\big) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} = \prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i).$$

Proof. First, by definition of a perfect number, $\sigma(N) = 2N$.

Since σ is multiplicative and the prime powers $p_i^{\alpha_i}$ are pairwise coprime, we have

$$\sigma(N) = \sigma\Big(\prod_{i=1}^{k} p_i^{\alpha_i}\Big) = \prod_{i=1}^{k} \sigma\big(p_i^{\alpha_i}\big).$$

For a prime power p^{α} one has the well-known formula

$$\sigma(p^{\alpha}) = 1 + p + \cdots + p^{\alpha} = \frac{p^{\alpha+1} - 1}{p - 1},$$

so

$$\sigma(N) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Now we express each factor $\dfrac{p_i^{\alpha_i+1}-1}{p_i-1}$ via cyclotomic polynomials. Fix i and set $n=\alpha_i+1$. By the cyclotomic factorisation we have

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

Evaluating at $x=p_i$ yields

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

Separating the factor with $d=1$ and using $\Phi_1(x)=x-1$ gives

$$p_i^n-1=(p_i-1)\prod_{\substack{d\mid n\\ d>1}}\Phi_d(p_i).$$

Dividing by p_i-1 we obtain

$$\frac{p_i^n-1}{p_i-1}=\prod_{\substack{d\mid n\\ d>1}}\Phi_d(p_i).$$

Recalling that $n=\alpha_i+1$, this becomes

$$\frac{p_i^{\alpha_i+1}-1}{p_i-1}=\prod_{\substack{d\mid \alpha_i+1\\ d>1}}\Phi_d(p_i).$$

Substituting this expression into the product for $\sigma(N)$, we obtain

$$\sigma(N)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}=\prod_{i=1}^{k}\prod_{\substack{d\mid \alpha_i+1\\ d>1}}\Phi_d(p_i),$$

which, together with $\sigma(N)=2N$, is exactly the desired identity. □

6 A cyclotomic factorisation of $\sigma(n)$ and of $\mathrm{rad}(\sigma(n))$

In this section we derive, for an arbitrary positive integer

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

a cyclotomic factorisation of the divisor sum $\sigma(n)$ and a corresponding description of its radical $\mathrm{rad}(\sigma(n))$.

6.1 Cyclotomic factorisation of $\sigma(n)$

Recall the basic properties of cyclotomic polynomials $\Phi_d(x)\in\mathbb{Z}[x]$:

- For each $n\geq 1$,

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

- $\Phi_1(x) = x - 1$.
- For any integer a and $n \geq 1$,

$$a^n - 1 = \prod_{d|n} \Phi_d(a)$$

(obtained by evaluating the first identity at $x = a$).

For a prime power p^α one has

$$\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Writing $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, multiplicativity of σ gives

$$\sigma(n) = \sigma\Big(\prod_{i=1}^{k} p_i^{\alpha_i}\Big) = \prod_{i=1}^{k} \sigma\big(p_i^{\alpha_i}\big) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

We now express each factor via cyclotomic polynomials.

Proposition 6.1. *Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. For each i we have*

$$\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} = \prod_{\substack{d|\alpha_i+1 \\ d>1}} \Phi_d(p_i),$$

and hence

$$\sigma(n) = \prod_{i=1}^{k} \prod_{\substack{d|\alpha_i+1 \\ d>1}} \Phi_d(p_i).$$

Proof. Fix i and set $m := \alpha_i + 1$. From the cyclotomic factorisation $x^m - 1 = \prod_{d|m} \Phi_d(x)$ we obtain, after substituting $x = p_i$,

$$p_i^m - 1 = \prod_{d|m} \Phi_d(p_i).$$

Separating the factor $d = 1$ and using $\Phi_1(x) = x - 1$ gives

$$p_i^m - 1 = (p_i - 1) \prod_{\substack{d|m \\ d>1}} \Phi_d(p_i).$$

Dividing by $p_i - 1$ and recalling $m = \alpha_i + 1$ yields

$$\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} = \prod_{\substack{d|\alpha_i+1 \\ d>1}} \Phi_d(p_i),$$

as claimed. Multiplying over $i = 1, \ldots, k$ gives the formula for $\sigma(n)$. □

6.2 A description of $\mathrm{rad}(\sigma(n))$

Recall that for a nonzero integer M the radical is

$$\mathrm{rad}(M) := \prod_{p \mid M} p,$$

the product of the distinct prime divisors of M.

Corollary 6.2. *For $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ we have*

$$\mathrm{rad}(\sigma(n)) = \mathrm{rad}\left(\prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i) \right).$$

Equivalently, a prime ℓ divides $\mathrm{rad}(\sigma(n))$ if and only if there exist an index i and a divisor $d > 1$ of $\alpha_i + 1$ such that $\ell \mid \Phi_d(p_i)$.

Proof. The first statement is just the definition of the radical applied to the factorisation of $\sigma(n)$ in Proposition 6.1. By definition of rad, a prime ℓ divides $\mathrm{rad}(\sigma(n))$ if and only if ℓ divides $\sigma(n)$, and hence if and only if ℓ divides one of the integer factors $\Phi_d(p_i)$ appearing in that product. □

We can refine this using a standard property of cyclotomic polynomials at prime arguments.

Lemma 6.3. *Let p and ℓ be distinct primes, and let $d \geq 1$. If $\ell \mid \Phi_d(p)$, then the multiplicative order of p modulo ℓ is exactly d. In particular, $d \mid (\ell - 1)$ and so $\ell \equiv 1 \pmod{d}$.*

Proof. From $x^d - 1 = \prod_{e \mid d} \Phi_e(x)$ we get

$$p^d - 1 = \prod_{e \mid d} \Phi_e(p).$$

If $\ell \mid \Phi_d(p)$, then $\ell \mid p^d - 1$, so the order f of p modulo ℓ satisfies $f \mid d$. On the other hand, $\Phi_d(p) \equiv 0 \pmod{\ell}$ means that p modulo ℓ is a primitive d-th root of unity; this is well known to be equivalent to $f = d$ (see, for example, any standard reference on cyclotomic polynomials). It follows that $d \mid (\ell - 1)$, because the order of an element of the group $(\mathbb{Z}/\ell\mathbb{Z})^\times$ always divides the group order $\ell - 1$. □

Together with the above corollary we obtain an arithmetic characterisation of the prime divisors of $\sigma(n)$.

Proposition 6.4 (Primes in the radical of $\sigma(n)$)**.** *Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ and let ℓ be a prime with $\ell \nmid p_i$ for all i. Then*

$$\ell \mid \mathrm{rad}(\sigma(n))$$

if and only if there exist i and a divisor $d > 1$ of $\alpha_i + 1$ such that the multiplicative order of p_i modulo ℓ is d. Equivalently,

$$\ell \mid \mathrm{rad}(\sigma(n)) \quad \Longleftrightarrow \quad \exists\, i,\ d > 1,\ d \mid \alpha_i + 1 \ \text{ with } \ \ell \equiv 1 \pmod{d} \text{ and } \ell \mid \Phi_d(p_i).$$

Proof. By Corollary 6.2, ℓ divides $\mathrm{rad}(\sigma(n))$ exactly when $\ell \mid \Phi_d(p_i)$ for some i and some $d \mid \alpha_i + 1$ with $d > 1$. For such i, d it follows from Lemma 6.3 that the order of p_i modulo ℓ is equal to d. Conversely, $\mathrm{ord}_\ell(p_i) = d$ with $d \mid \alpha_i + 1$ implies $\ell \mid \Phi_d(p_i)$, again by the standard theory of cyclotomic polynomials. This gives the desired equivalence. □

In summary, for general n the divisor sum $\sigma(n)$ factorises as a finite product of cyclotomic values $\Phi_d(p_i)$, and the radical $\mathrm{rad}(\sigma(n))$ is precisely the product of the distinct primes which divide these values. Each such prime ℓ is characterised by the existence of a prime factor p_i of n whose multiplicative order modulo ℓ divides $\alpha_i + 1$ and is > 1.

7 Multiplicative Cyclotomic Polynomials

For every integer $n \geq 1$ we define the *multiplicative cyclotomic polynomial*

$$g_n(x) \;:=\; \prod_{p \mid n} \Phi_p(x)^{v_p(n)} \in \mathbb{Z}[x],$$

where the product runs over all prime divisors p of n, and $v_p(n)$ denotes the p–adic valuation of n. We also set $g_1(x) = 1$. These polynomials are built purely from cyclotomic factors, but still encode the full prime factorization of n.

Throughout the section we denote by

$$\mathrm{rad}(n) := \prod_{p \mid n} p$$

the radical of n.

7.1 Basic properties

Theorem 7.1 (Evaluation)**.** *For all $n \geq 1$ one has*

$$g_n(1) = n.$$

Proof. For a prime p we have $\Phi_p(1) = p$, since $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Therefore

$$g_n(1) = \prod_{p \mid n} \Phi_p(1)^{v_p(n)} = \prod_{p \mid n} p^{v_p(n)} = n.$$

□

Theorem 7.2 (Multiplicativity)**.** *If $\gcd(m, n) = 1$, then*

$$g_{mn}(x) = g_m(x)\, g_n(x).$$

Proof. Write $m = \prod_{p \mid m} p^{a_p}$ and $n = \prod_{q \mid n} q^{b_q}$. If $\gcd(m, n) = 1$, then the sets of primes dividing m and n are disjoint. Hence

$$g_{mn}(x) = \prod_{r \mid mn} \Phi_r(x)^{v_r(mn)} = \prod_{p \mid m} \Phi_p(x)^{a_p} \prod_{q \mid n} \Phi_q(x)^{b_q} = g_m(x)\, g_n(x).$$

□

Theorem 7.3 (Irreducibility at prime argument)**.** *If $n = p$ is prime, then $g_p(x) = \Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. The polynomial $\Phi_p(x)$ is the minimal polynomial of a primitive pth root of unity over $\mathbb{Q}$, hence irreducible. □

Theorem 7.4 (Radical)**.**

$$g_{\mathrm{rad}(n)}(x) = \prod_{p \mid n} \Phi_p(x).$$

Proof. Since $v_p(\mathrm{rad}(n)) = 1$ for every $p \mid n$, the claim follows directly from the definition of g_n. □

7.2 Polynomial gcd structure

Theorem 7.5 (Greatest common divisor)**.** *For all $m, n \geq 1$ we have*

$$\gcd\big(g_m(x), g_n(x)\big) = g_{\gcd(m,n)}(x).$$

Proof. Using the unique factorization

$$g_m(x) = \prod_{p \mid m} \Phi_p(x)^{v_p(m)}, \qquad g_n(x) = \prod_{p \mid n} \Phi_p(x)^{v_p(n)},$$

and the fact that the Φ_p for distinct primes are pairwise coprime irreducible polynomials, we obtain

$$\gcd(g_m, g_n) = \prod_{p \mid m,n} \Phi_p(x)^{\min(v_p(m), v_p(n))} = \prod_{p \mid \gcd(m,n)} \Phi_p(x)^{v_p(\gcd(m,n))} = g_{\gcd(m,n)}.$$

□

7.3 Radical of a multiplicative cyclotomic polynomial

Theorem 7.6 (Polynomial radical)**.**

$$\mathrm{rad}\big(g_n(x)\big) = g_{\mathrm{rad}(n)}(x).$$

Proof. The radical of a polynomial is defined as the product of its distinct irreducible factors. Since

$$g_n(x) = \prod_{p \mid n} \Phi_p(x)^{v_p(n)},$$

and each $\Phi_p(x)$ is irreducible, it follows that

$$\mathrm{rad}(g_n) = \prod_{p \mid n} \Phi_p(x) = g_{\mathrm{rad}(n)}(x).$$

□

7.4 Splitting fields

Theorem 7.7 (Splitting field of $g_{\mathrm{rad}(n)}$)**.** *Let $K_{\mathrm{rad}(n)}$ be the splitting field of $g_{\mathrm{rad}(n)}(x)$. Then*

$$K_{\mathrm{rad}(n)} = \mathbb{Q}\big(\zeta_{\mathrm{rad}(n)}\big)\,.$$

Proof. The polynomial

$$g_{\mathrm{rad}(n)}(x) = \prod_{p \mid n} \Phi_p(x)$$

has as its roots all primitive pth roots of unity, for all primes $p \mid n$. Hence its splitting field is

$$K_{\mathrm{rad}(n)} = \mathbb{Q}\big(\zeta_p : p \mid n\big) = \mathbb{Q}\Big(\zeta_{\prod_{p \mid n} p}\Big) = \mathbb{Q}(\zeta_{\mathrm{rad}(n)}).$$

□

Theorem 7.8 (Splitting field of $g_n(x)$)**.** *For all $n \geq 1$,*

$$K_n := \mathrm{SplittingField}(g_n/\mathbb{Q}) = \mathbb{Q}(\zeta_{\mathrm{rad}(n)}).$$

Proof. Changing the exponents $v_p(n)$ does not change the set of roots of the polynomial. Thus g_n and $g_{\mathrm{rad}(n)}$ have the same splitting field. □

7.5 Galois groups

Theorem 7.9 (Galois group)**.**

$$\mathrm{Gal}(g_n/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathrm{rad}(n)})/\mathbb{Q}) \cong (\mathbb{Z}/\operatorname{rad}(n)\mathbb{Z})^\times.$$

Proof. The Galois group of a cyclotomic field $\mathbb{Q}(\zeta_m)$ is well known to be isomorphic to the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ via $\sigma_a(\zeta_m) = \zeta_m^a$. The previous theorem shows that the splitting field of g_n is $\mathbb{Q}(\zeta_{\mathrm{rad}(n)})$, which yields the claim. □

7.6 Adjoining a new prime

Theorem 7.10 (Adjunction of a new prime)**.** *Let q be a prime with $q \nmid n$, and set $n' = nq$. Then:*

(i) ***Polynomial level:***

$$g_{n'}(x) = g_n(x)\, \Phi_q(x).$$

(ii) ***Field level:***

$$K_{n'} = K_n(\zeta_q) = \mathbb{Q}(\zeta_{\mathrm{rad}(n)q}).$$

(iii) ***Galois groups:***

$$\mathrm{Gal}(K_{n'}/\mathbb{Q}) \cong \mathrm{Gal}(K_n/\mathbb{Q}) \times (\mathbb{Z}/q\mathbb{Z})^\times.$$

Proof. (i) Since $v_q(n') = 1$ and the other valuations are unchanged,

$$g_{n'}(x) = \prod_{p \mid n'} \Phi_p(x)^{v_p(n')} = \Phi_q(x)\, g_n(x).$$

(ii) As $\operatorname{rad}(n') = \operatorname{rad}(n) \cdot q$, the splitting field is

$$K_{n'} = \mathbb{Q}(\zeta_{\mathrm{rad}(n)q}) = K_n(\zeta_q).$$

(iii) Cyclotomic fields corresponding to distinct primes are linearly disjoint, so

$$\mathrm{Gal}(K_{n'}/\mathbb{Q}) \cong \mathrm{Gal}(K_n/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/\operatorname{rad}(n)\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times.$$

□

Summary

The multiplicative cyclotomic polynomials $g_n(x)$ satisfy:

- $g_n(1) = n$;
- multiplicativity: $g_{mn} = g_m g_n$ for $\gcd(m,n) = 1$;
- $\gcd(g_m, g_n) = g_{\gcd(m,n)}$;
- $\mathrm{rad}(g_n) = g_{\mathrm{rad}(n)}$;
- $\mathrm{SplittingField}(g_n) = \mathbb{Q}(\zeta_{\mathrm{rad}(n)})$;
- $\mathrm{Gal}(g_n/\mathbb{Q}) \cong (\mathbb{Z}/\,\mathrm{rad}(n)\mathbb{Z})^\times$;
- adjoining a new prime behaves exactly as adjoining a cyclotomic factor.

7.7 Galois group via adjoining prime cyclotomic fields

We now justify in detail the description

$$\mathrm{Gal}\big(g_n/\mathbb{Q}\big) \;\cong\; \big(\mathbb{Z}/\,\mathrm{rad}(n)\mathbb{Z}\big)^\times.$$

Recall that the splitting field of g_n equals the splitting field of $g_{\mathrm{rad}(n)}$, namely

$$K_n = \mathbb{Q}(\zeta_{\mathrm{rad}(n)}).$$

Since $\mathrm{rad}(n)$ is squarefree, we may write

$$\mathrm{rad}(n) = \prod_{p \mid n} p,$$

and it is convenient to work with the compositum of the prime cyclotomic fields.

For a finite set S of primes, define

$$K_S := \mathbb{Q}\big(\zeta_p : p \in S\big).$$

If S is the set of prime divisors of n, then $K_S = \mathbb{Q}(\zeta_{\mathrm{rad}(n)}) = K_n$.

Lemma 7.11. *Let $p \neq q$ be distinct primes. Then*

$$\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}.$$

Proof. Both fields are Galois over $\mathbb{Q}$ with degrees $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ and $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q-1$. Their compositum is contained in the cyclotomic field $\mathbb{Q}(\zeta_{pq})$, which has degree

$$[\mathbb{Q}(\zeta_{pq}) : \mathbb{Q}] = \varphi(pq) = (p-1)(q-1).$$

On the other hand

$$[\mathbb{Q}(\zeta_p)\,\mathbb{Q}(\zeta_q) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]\,[\mathbb{Q}(\zeta_q) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) : \mathbb{Q}]} = \frac{(p-1)(q-1)}{[\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) : \mathbb{Q}]}.$$

Since the compositum is contained in $\mathbb{Q}(\zeta_{pq})$, whose degree is already $(p-1)(q-1)$, we must have

$$[\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) : \mathbb{Q}] = 1,$$

hence the intersection is exactly $\mathbb{Q}$. □

Lemma 7.12. *Let S be a finite set of primes and $q \notin S$ another prime. Set $S' := S \cup \{q\}$. Then*

$$\mathrm{Gal}(K_{S'}/\mathbb{Q}) \;\cong\; \mathrm{Gal}(K_S/\mathbb{Q}) \times \mathrm{Gal}\big(\mathbb{Q}(\zeta_q)/\mathbb{Q}\big).$$

Proof. We have $K_{S'} = K_S(\zeta_q)$ and $\mathbb{Q}(\zeta_q) \subseteq K_{S'}$. By Lemma 7.11 and induction on $|S|$ we obtain

$$\mathbb{Q}(\zeta_q) \cap K_S = \mathbb{Q}.$$

Thus the extensions $K_S/\mathbb{Q}$ and $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ are linearly disjoint. For finite Galois extensions, linear disjointness implies

$$\mathrm{Gal}(K_S\,\mathbb{Q}(\zeta_q)/\mathbb{Q}) \;\cong\; \mathrm{Gal}(K_S/\mathbb{Q}) \times \mathrm{Gal}\big(\mathbb{Q}(\zeta_q)/\mathbb{Q}\big),$$

and $K_S\,\mathbb{Q}(\zeta_q) = K_{S'}$, which gives the claim. □

Theorem 7.13 (Galois group of K_n)**.** *Let $n \geq 1$ and let S be the (finite) set of prime divisors of n. Then*

$$\mathrm{Gal}(K_n/\mathbb{Q}) \;\cong\; \prod_{p \in S} \big(\mathbb{Z}/p\mathbb{Z}\big)^{\times} \;\cong\; \big(\mathbb{Z}/\operatorname{rad}(n)\mathbb{Z}\big)^{\times}.$$

Proof. We argue by induction on $|S|$.

If $S = \varnothing$ (i.e. $n = 1$), then $K_n = \mathbb{Q}$ and the Galois group is trivial, which is the empty product.

If $S = \{p\}$ consists of a single prime, then $K_n = \mathbb{Q}(\zeta_p)$ and

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$$

is the usual cyclotomic result.

Assume now that $|S| \geq 2$ and write $S = T \cup \{q\}$ with $q \notin T$. By induction,

$$\mathrm{Gal}(K_T/\mathbb{Q}) \cong \prod_{p \in T} (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

Using Lemma 7.12 we obtain

$$\mathrm{Gal}(K_S/\mathbb{Q}) \;\cong\; \mathrm{Gal}(K_T/\mathbb{Q}) \times \mathrm{Gal}\big(\mathbb{Q}(\zeta_q)/\mathbb{Q}\big) \;\cong\; \Big(\prod_{p \in T} (\mathbb{Z}/p\mathbb{Z})^{\times}\Big) \times (\mathbb{Z}/q\mathbb{Z})^{\times} = \prod_{p \in S} (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

Finally, for a squarefree integer $m = \prod_{p \in S} p$ the Chinese remainder theorem yields a canonical isomorphism

$$\big(\mathbb{Z}/m\mathbb{Z}\big)^{\times} \;\cong\; \prod_{p \in S} (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

Taking $m = \operatorname{rad}(n)$ proves the theorem. □

Corollary 7.14. *For every $n \geq 1$,*

$$\mathrm{Gal}(g_n/\mathbb{Q}) \;\cong\; \big(\mathbb{Z}/\operatorname{rad}(n)\mathbb{Z}\big)^{\times}.$$

Proof. The splitting field of g_n equals $K_n = \mathbb{Q}(\zeta_{\operatorname{rad}(n)})$, and Theorem 7.13 applies. □

8 Galois action on the values $f_q(\alpha)$ for $q \mid p-1$

We work with the polynomials $f_n(x) \in \mathbb{Z}[x]$ as in the MathOverflow discussion, in particular 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, and let

$$K_p := \mathrm{Spl}\big(f_p(x)/\mathbb{Q}\big)$$

be the splitting field of f_p over $\mathbb{Q}$, with

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

its Galois group. Let $R_p \subset K_p$ denote the set of roots of $f_p(x)$ in a fixed algebraic closure $\overline{\mathbb{Q}}$.

Lemma 8.1 (Transitivity on the roots)**.** *For each prime p, the Galois group G_p acts transitively on the set R_p of roots of f_p.*

Proof. Since $f_p(x)$ is irreducible over $\mathbb{Q}$, its roots are all Galois conjugate. Equivalently, for any two roots $\alpha, \beta \in R_p$ there exists $\sigma \in G_p$ with $\sigma(\alpha) = \beta$. This is exactly transitivity of the action of G_p on R_p. □

Now fix a prime divisor $q \mid (p-1)$. For each root $\alpha \in R_p$ we consider the value $f_q(\alpha) \in K_p$. Using multiplicativity we have

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

so for every root $\alpha \in R_p$ the identity

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

implies

$$f_{p-1}(\alpha) = -1 = \prod_{r|p-1} f_r(\alpha)^{v_r(p-1)}. \tag{8.1}$$

Definition 8.2. Define

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

for each prime divisor $q \mid p-1$, and let

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

Note that $\Omega_{p,q}$ is a subset of K_p; different primes q may in principle produce overlapping subsets $\Omega_{p,q} \subset K_p$, so the union is not a disjoint union as sets in general.

Proposition 8.3 (Galois action on Ω_p)**.** *The Galois group G_p acts on Ω_p via*

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

Moreover, for each fixed prime $q \mid p-1$ the subset $\Omega_{p,q}$ is stable under the action of G_p.

Proof. First we check that the formula

$$\sigma \cdot f_q(\alpha) := f_q(\sigma(\alpha))$$

is well-defined on Ω_p. If $f_q(\alpha) = f_q(\beta)$ for two roots $\alpha, \beta \in R_p$, then

$$f_q(\sigma(\alpha)) = \sigma(f_q(\alpha)) = \sigma(f_q(\beta)) = f_q(\sigma(\beta)),$$

since σ is a field automorphism fixing $\mathbb{Q}$ and hence the coefficients of f_q. Thus the image depends only on the value $f_q(\alpha)$, not on the choice of α.

Secondly, for fixed q we have by definition

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

If $x \in \Omega_{p,q}$, say $x = f_q(\alpha)$, then

$$\sigma(x) = \sigma(f_q(\alpha)) = f_q(\sigma(\alpha)) \in \Omega_{p,q}.$$

Thus $\Omega_{p,q}$ is invariant under G_p, and the action preserves the decomposition of Ω_p into the subsets $\Omega_{p,q}$. □

The transitivity of G_p on the root set R_p (Lemma 8.1) and the definition of $\Omega_{p,q}$ immediately give:

Corollary 8.4. *For each prime divisor $q \mid p-1$, the action of G_p on $\Omega_{p,q}$ is given by the permutation representation induced from the map*

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

In particular, $\Omega_{p,q}$ is a union of G_p-orbits, and every orbit in $\Omega_{p,q}$ is the image of the full G_p-orbit of some root $\alpha \in R_p$.

Proof. The map $\alpha \mapsto f_q(\alpha)$ is G_p–equivariant:

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

Since G_p acts transitively on R_p, its orbits in $\Omega_{p,q}$ are exactly the images of R_p under this map, modulo possible identifications when two distinct roots yield the same value $f_q(\alpha)$. □

The multiplicative relation (8.1) is preserved under the Galois action. Indeed, for each $\sigma \in G_p$ and each root $\alpha \in R_p$, we have

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

so the family of values

$$\Big(f_q(\alpha)\Big)_{\substack{q \mid p-1 \\ q \text{ prime}}}$$

satisfies a G_p–stable multiplicative relation with coefficients in $\mathbb{Q}$.

In particular, for each prime $q \mid p-1$ and each choice of a root $\alpha \in R_p$, the element $f_q(\alpha)$ lies in K_p and its Galois conjugates over $\mathbb{Q}$ are precisely the elements of the G_p–orbit of $f_q(\alpha)$ inside $\Omega_{p,q}$. If we denote by

$$L_{p,q} := \mathbb{Q}\big(f_q(\alpha)\big)^{\mathrm{gal}}$$

the Galois closure of $\mathbb{Q}(f_q(\alpha))$ inside K_p, then $L_{p,q} \subseteq K_p$ and

$$\mathrm{Gal}(L_{p,q}/\mathbb{Q}) \cong G_p/\operatorname{Stab}_{G_p}\big(f_q(\alpha)\big),$$

so each prime divisor $q \mid p-1$ gives rise to a natural quotient of G_p together with a distinguished permutation representation on $\Omega_{p,q}$.

Example 8.5 (The case $p = 11$)**.** *We illustrate the general construction for the prime $p = 11$. From the defining recursion one computes*

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

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

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

so $G_{11} := \mathrm{Gal}(K_{11}/\mathbb{Q})$ has order 6 and is (as one easily checks) isomorphic to S_3.

Let $\alpha \in K_{11}$ be a root of $f_{11}(x)$, so that

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

The prime divisors of $p - 1 = 10$ are 2 and 5, hence we consider $q \in \{2, 5\}$.

***The set** $\Omega_{11,2}$. Here $f_2(x) = x$, so*

$$\Omega_{11,2} = \{f_2(\sigma(\alpha)) : \sigma \in G_{11}\} = \{\sigma(\alpha) : \sigma \in G_{11}\}$$

is just the G_{11}–orbit of α. A computation in Sage shows:

- *$|\Omega_{11,2}| = 3$, so this is precisely the set of the three roots of $f_{11}(x)$;*
- *for every $\beta \in \Omega_{11,2}$ we have $\mathrm{minpoly}(\beta/\mathbb{Q}) = x^3 + x + 1$.*

Thus

$$L_{11,2} := \mathbb{Q}(\beta)$$

is a cubic subfield of K_{11} with $[L_{11,2} : \mathbb{Q}] = 3$, and K_{11} is the Galois closure of this field. The stabiliser of an element $\beta \in \Omega_{11,2}$ is a subgroup of order 2 in $G_{11} \cong S_3$, so the orbit–stabiliser formula gives

$$|\Omega_{11,2}| = \frac{|G_{11}|}{|\operatorname{Stab}_{G_{11}}(\beta)|} = \frac{6}{2} = 3.$$

***The set** $\Omega_{11,5}$. Here $f_5(x) = x^2 + 1$, and we consider*

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

An explicit computation (again for example in Sage) shows:

- *$|\Omega_{11,5}| = 3$;*
- *every $\gamma \in \Omega_{11,5}$ has minimal polynomial*

$$\mathrm{minpoly}(\gamma/\mathbb{Q}) = x^3 - x^2 - 1,$$

again of degree 3, but distinct from $f_{11}(x)$.

Thus

$$L_{11,5} := \mathbb{Q}(\gamma)$$

is a different *cubic subfield of* K_{11} *with* $[L_{11,5} : \mathbb{Q}] = 3$. *As in a typical* S_3*–extension, the field* K_{11} *has exactly two proper intermediate fields of degree* 3, *namely* $\mathbb{Q}(\alpha)$ *and* $\mathbb{Q}(f_5(\alpha))$, *and both arise from the sets* $\Omega_{11,2}$ *and* $\Omega_{11,5}$.

Finally,

$$\Omega_{11} := \Omega_{11,2} \cup \Omega_{11,5}$$

is a set of 6 *elements in* K_{11}, *decomposing into two* G_{11}*–orbits of size* 3, *corresponding exactly to the two cubic subfields* $L_{11,2}$ *and* $L_{11,5}$.

Example 8.6 (The case $p = 127$)**.** *We now consider the prime* $p = 127$. *From the defining recursion one obtains*

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

which is irreducible over $\mathbb{Q}$. *Its splitting field* K_{127} *has*

$$[K_{127} : \mathbb{Q}] = 10,$$

so $G_{127} := \mathrm{Gal}(K_{127}/\mathbb{Q})$ *has order* 10. *Computations (and the group table in Section 3.7) show that* G_{127} *is isomorphic to the dihedral group* D_5 *of order* 10.

Let $\alpha \in K_{127}$ *be a root of* $f_{127}(x)$, *so that*

$$\mathrm{minpoly}(\alpha/\mathbb{Q}) = x^5 + 3x^4 + 4x^3 + 3x^2 + x + 1.$$

The prime divisors of $p - 1 = 126$ *are* $2, 3, 7$, *so we consider* $q \in \{2, 3, 7\}$ *and the sets* $\Omega_{127,q}$ *as before.*

The set $\Omega_{127,2}$**.** *Here* $f_2(x) = x$, *so*

$$\Omega_{127,2} = \{f_2(\sigma(\alpha)) : \sigma \in G_{127}\} = \{\sigma(\alpha) : \sigma \in G_{127}\}$$

is the G_{127}*–orbit of* α. *A computation in* Sage *shows:*

- $|\Omega_{127,2}| = 5$, *so we see all five Galois conjugates of* α*;*
- *for every* $\beta \in \Omega_{127,2}$ *we have*

$$\mathrm{minpoly}(\beta/\mathbb{Q}) = x^5 + 3x^4 + 4x^3 + 3x^2 + x + 1.$$

Thus

$$L_{127,2} := \mathbb{Q}(\beta)$$

is a quintic subfield of K_{127} *with* $[L_{127,2} : \mathbb{Q}] = 5$, *and* K_{127} *is its Galois closure.*

The sets $\Omega_{127,3}$ ***and*** $\Omega_{127,7}$**.** *For* $q = 3$ *we have* $f_3(x) = x + 1$, *and we consider*

$$\Omega_{127,3} = \{f_3(\sigma(\alpha)) : \sigma \in G_{127}\} = \{\sigma(\alpha) + 1 : \sigma \in G_{127}\}.$$

Similarly, for $q = 7$ *we have* $f_7(x) = x^2 + x + 1$ *and*

$$\Omega_{127,7} = \{f_7(\sigma(\alpha)) : \sigma \in G_{127}\} = \{\sigma(\alpha)^2 + \sigma(\alpha) + 1 : \sigma \in G_{127}\}.$$

Explicit computations in Sage *give:*

- $|\Omega_{127,3}| = 5$ *and every* $\gamma \in \Omega_{127,3}$ *has*

$$\mathrm{minpoly}(\gamma/\mathbb{Q}) = x^5 - 2x^4 + 2x^3 - x^2 + 1;$$

- $|\Omega_{127,7}| = 5$ *and every* $\delta \in \Omega_{127,7}$ *has*

$$\mathrm{minpoly}(\delta/\mathbb{Q}) = x^5 - 3x^4 + 3x^3 - 2x^2 + x - 1.$$

In particular,

$$L_{127,3} := \mathbb{Q}(\gamma), \qquad L_{127,7} := \mathbb{Q}(\delta)$$

are two further quintic subfields of K_{127}*, both of degree* 5*, but with different minimal polynomials than* $f_{127}(x)$*.*

Altogether we obtain three distinct quintic subfields

$$L_{127,2},\ L_{127,3},\ L_{127,7} \subset K_{127},$$

each generated by any element of the corresponding orbit $\Omega_{127,q}$*. From the Galois-theoretic point of view,* $G_{127} \cong D_5$ *has subgroups of order* 2 *(the reflections), each of index* 5*; these subgroups correspond exactly to the degree-*5 *subfields of* K_{127}*. The sets*

$$\Omega_{127,q} = \{f_q(\sigma(\alpha)) : \sigma \in G_{127}\}, \quad q \in \{2, 3, 7\},$$

realise three such orbits of size 5*, and*

$$\Omega_{127} := \Omega_{127,2} \cup \Omega_{127,3} \cup \Omega_{127,7}$$

is a union of three G_{127}*–orbits of size* 5*, corresponding to the three quintic subfields* $L_{127,2}, L_{127,3}, L_{127,7}$*.*

Lemma 8.7. *Let* $f_p(x) \in \mathbb{Q}[x]$ *be irreducible of degree* d*, let* $\alpha \in \mathbb{C}$ *be a root of* f_p*, and let* K_p *be the splitting field of* f_p *over* $\mathbb{Q}$*. Set*

$$G_p := \mathrm{Gal}(K_p/\mathbb{Q}), \qquad |G_p| = d \cdot r.$$

For each prime $q \mid (p-1)$ *let* $f_q(x)$ *be defined as in the MO construction and set*

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

and let $\Omega_{p,q}$ *be its* G_p*–orbit:*

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

Then:

1. $\beta_q \in \mathbb{Q}(\alpha)$*;*
2. $|\Omega_{p,q}|$ *divides* d*;*
3. *with* $L_{p,q} := \mathbb{Q}(\beta_q)$ *we have*

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

4. the natural quotient

$$G_p/\operatorname{Gal}(K_p/L_{p,q})$$

has order $|\Omega_{p,q}|$, hence this "nontrivial quotient coming from $q \mid (p-1)$" always has size dividing d (and of course also dividing $|G_p| = d \cdot r$).

Proof. (1) By construction $f_q(x) \in \mathbb{Q}[x]$, so $f_q(\alpha)$ is obtained by substituting α into a polynomial with rational coefficients. Hence

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

(2) Consider the tower of fields

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

Since f_p is irreducible of degree d, we have

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

Because $K_p/\mathbb{Q}$ is Galois, the subgroup

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

is normal in G_p, and by the fundamental theorem of Galois theory

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

Now let $\beta_q := f_q(\alpha) \in \mathbb{Q}(\alpha)$ as above. Since every $\tau \in N$ fixes α, it also fixes any polynomial in α with rational coefficients. In particular, for all $\tau \in N$,

$$\tau(\beta_q) = \tau\big(f_q(\alpha)\big) = f_q\big(\tau(\alpha)\big) = f_q(\alpha) = \beta_q.$$

Thus every element of N fixes β_q, i.e.

$$N \subseteq \operatorname{Stab}_{G_p}(\beta_q),$$

where

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

is the stabiliser of β_q in G_p.

By the orbit–stabiliser theorem,

$$|\Omega_{p,q}| = |G_p \cdot \beta_q| = [G_p : \operatorname{Stab}_{G_p}(\beta_q)].$$

Combining this with $N \subseteq \operatorname{Stab}_{G_p}(\beta_q)$ we obtain

$$[G_p : \operatorname{Stab}_{G_p}(\beta_q)] = \frac{[G_p : N]}{[\operatorname{Stab}_{G_p}(\beta_q) : N]},$$

and the denominator $[\operatorname{Stab}_{G_p}(\beta_q) : N]$ is a positive integer. Hence

$$|\Omega_{p,q}| = [G_p : \operatorname{Stab}_{G_p}(\beta_q)] \mid [G_p : N] = d.$$

In particular $|\Omega_{p,q}|$ divides d (and trivially divides $|G_p| = d \cdot r$).

(3) and (4) Let $L_{p,q} := \mathbb{Q}(\beta_q)$. Because $K_p/\mathbb{Q}$ is Galois, K_p is also the splitting field of the minimal polynomial of β_q over $\mathbb{Q}$, and we have

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

Therefore

$$|G_p/\,\mathrm{Gal}(K_p/L_{p,q})| = [G_p : \mathrm{Stab}_{G_p}(\beta_q)] = |\Omega_{p,q}|.$$

On the other hand, the conjugates of β_q over $\mathbb{Q}$ are precisely the elements of its G_p–orbit, so

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

This shows both (3) and (4). □

Example 8.8 (Non-disjoint orbits for $p = 31$)**.** *We give an explicit example showing that, in general, the orbits $\Omega_{p,q}$ for different primes $q \mid (p-1)$ need not be disjoint.*

Recall that for each prime divisor $q \mid p-1$ we define

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

where R_p is the set of roots of $f_p(x)$ in a fixed algebraic closure and K_p is the splitting field of f_p over $\mathbb{Q}$.

For the prime $p = 31$ one computes

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

which is irreducible over $\mathbb{Q}$. Its splitting field K_{31} has $[K_{31} : \mathbb{Q}] = 4$, so

$$G_{31} := \mathrm{Gal}(K_{31}/\mathbb{Q})$$

has order 4 and in fact is isomorphic to the cyclic group C_4. In particular, there are only three intermediate fields: $\mathbb{Q}$, a unique quadratic subfield, and K_{31} itself; any element of degree 4 over $\mathbb{Q}$ generates the full field K_{31}.

The prime divisors of $p - 1 = 30$ are $2, 3, 5$, and for each of these we form the corresponding set $\Omega_{31,q}$.

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

$$\Omega_{31,2} = \{\alpha : \alpha \in R_{31}\} = R_{31}$$

is just the set of the four roots of $f_{31}(x)$. A computation in Sage yields, up to reordering,

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

each element having minimal polynomial $\mathrm{minpoly}(\,\cdot\,/\mathbb{Q}) = x^4+x^3+x^2+x+1$. *Thus every element of $\Omega_{31,2}$ generates K_{31}.*

***The sets** $\Omega_{31,3}$ **and** $\Omega_{31,5}$. For $q = 3$ we have $f_3(x) = x + 1$, and for $q = 5$ we have $f_5(x) = x^2 + 1$. Using the same root α as above, one finds*

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

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, only in different order. Moreover, each of these elements has the same minimal polynomial

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

so they are Galois-conjugate and all generate the same quartic field

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

In particular, for $p = 31$ we have:

- *$\Omega_{31,2} = R_{31}$ is the G_{31}–orbit of a root of f_{31} and consists of four elements of degree 4 over $\mathbb{Q}$, each generating K_{31};*
- *$\Omega_{31,3} = \Omega_{31,5}$ is a* single *G_{31}–orbit of size 4, consisting of four other elements of degree 4 over $\mathbb{Q}$, which again all generate the same field K_{31}.*

Thus the union

$$\Omega_{31} := \bigcup_{\substack{q|30 \\ q \text{ prime}}} \Omega_{31,q} = \Omega_{31,2} \cup \Omega_{31,3} \cup \Omega_{31,5}$$

is a union of only two *distinct G_{31}–orbits, not three: the orbits for $q = 3$ und $q = 5$ coincide. Equivalently, the two elements $f_3(\alpha)$ und $f_5(\alpha)$ are Galois-conjugate. This shows that the naive expectation that the sets $\Omega_{p,q}$ for different primes $q \mid (p-1)$ should always be disjoint is, in general,* ***false****, even though they may all generate the same splitting field K_p.*

Lemma 8.9. *Let $p > 2$ be a prime, let K_p be the splitting field of $f_p(x)$ over $\mathbb{Q}$, and let $G_p := \mathrm{Gal}(K_p/\mathbb{Q})$. Fix a root $\alpha \in K_p$ of $f_p(x)$, and for each prime divisor $q \mid (p-1)$ set*

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

Then, for two primes $q, r \mid (p-1)$, we have

$$\Omega_{p,q} = \Omega_{p,r} \quad \Longleftrightarrow \quad \beta_q \text{ and } \beta_r \text{ are Galois-conjugate under } G_p,$$

i.e. there exists $\sigma \in G_p$ with $\sigma(\beta_q) = \beta_r$.

Proof. First recall that G_p acts transitively on the set R_p of roots of $f_p(x)$ in K_p, and by definition

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

If we fix one root $\alpha \in R_p$, then every other root has the form $\sigma(\alpha)$ for some $\sigma \in G_p$, and

$$f_q(\sigma(\alpha)) = \sigma\big(f_q(\alpha)\big) = \sigma(\beta_q),$$

because σ is a field automorphism and f_q has rational coefficients. Hence

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

and similarly $\Omega_{p,r} = G_p \cdot \beta_r$. Thus each $\Omega_{p,q}$ is a single G_p-orbit.

($\Rightarrow$) Suppose $\Omega_{p,q} = \Omega_{p,r}$. Then in particular $\beta_q \in \Omega_{p,r} = G_p \cdot \beta_r$, so there exists $\sigma \in G_p$ with

$$\beta_q = \sigma(\beta_r).$$

Equivalently, $\beta_r = \sigma^{-1}(\beta_q)$, so β_q and β_r lie in the same G_p-orbit and are therefore Galois-conjugate.

(⇐) Conversely, suppose there exists $\sigma \in G_p$ with $\sigma(\beta_q) = \beta_r$. Then

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

so $\Omega_{p,q} \cap \Omega_{p,r} \neq \varnothing$. But G_p-orbits in K_p are either disjoint or equal: if $G_p \cdot x$ and $G_p \cdot y$ have a common element, then

$$G_p \cdot x = G_p \cdot y.$$

Applying this to $x = \beta_q$ and $y = \beta_r$ yields

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

as claimed. □

Lemma 8.10. *Reminder:*

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

and let

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

Then we have the standard Orbit-Stabilizer-connection:

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

Let $p > 2$ be prime and keep the above notation. For primes $q, r \mid (p-1)$ the following are equivalent:

1. *β_q and β_r are Galois-conjugate under G_p, i.e. there exists $\sigma \in G_p$ with $\sigma(\beta_q) = \beta_r$.*
2. *The orbits coincide: $\Omega_{p,q} = \Omega_{p,r}$.*
3. *The stabilizers H_q and H_r are conjugate subgroups of G_p:*

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

Proof. (1) ⇒ (2): If $\sigma(\beta_q) = \beta_r$, then

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

(2) ⇒ (1): If $\Omega_{p,q} = \Omega_{p,r}$, then in particular $\beta_r \in \Omega_{p,q} = G_p \cdot \beta_q$, so there is $\sigma \in G_p$ with $\sigma(\beta_q) = \beta_r$.

(1) ⇒ (3): Suppose $\sigma(\beta_q) = \beta_r$. Then for any $\tau \in H_q$ we have

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

so $\sigma H_q \sigma^{-1} \subseteq H_r$. Conversely, if $\rho \in H_r$, then $\sigma^{-1}\rho\sigma(\beta_q) = \beta_q$, so $\sigma^{-1}\rho\sigma \in H_q$ and thus $\rho \in \sigma H_q \sigma^{-1}$. Hence $H_r = \sigma H_q \sigma^{-1}$.

(3) ⇒ (1): If $H_r = \sigma H_q \sigma^{-1}$ for some σ, then H_r fixes β_r, and H_q fixes β_q. But $H_r = \sigma H_q \sigma^{-1}$ fixes $\sigma(\beta_q)$, so both β_r and $\sigma(\beta_q)$ are fixed by H_r. In a transitive action of G_p on the orbit $G_p \cdot \beta_q$, the stabilizer fixes exactly one point, so necessarily $\beta_r = \sigma(\beta_q)$. Thus β_q and β_r are Galois-conjugate. □

9 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.

9.1 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 $(\mathbb{Z}/r\mathbb{Z})^\times$.

9.2 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.

9.3 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:

- $|\Omega_{q,r}| = [G_q : H_r] = [L_{q,r} : \mathbb{Q}]$,
- β_r and β_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
$$\Omega_q := \bigcup_{r \mid (q-1)} \Omega_{q,r}$$
is a union of G_q-orbits, and all the structure is encoded in the family of stabilisers $\{H_r\}_{r \mid (q-1)}$.

For Mersenne primes $q = 2^p - 1$ the family $\{H_r\}_{r \mid (q-1)}$ 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 $f_n(2) = n$.

9.4 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 $p = 11, 13, 19, \dots$),
  - 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.

9.5 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 $\{H_r\}_{r \mid (q-1)}$, 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 β_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.

9.6 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.

9.6.1 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 9.1 (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 9.2 (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 $\mathcal{E}^*$:

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

9.6.2 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 9.3. 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 $d > 1$.

9.6.3 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.

10 Cyclotomic primes and Zsigmondy's theorem

In this section we connect the cyclotomic factorisation of $\sigma(n)$ from Section **??** with Zsigmondy's theorem on primitive prime divisors. This allows us to isolate primes q that divide a specific cyclotomic factor $\Phi_d(p)$ and do *not* divide any smaller factor $\Phi_e(p)$ with $e < d$.

10.1 Cyclotomic primes $q \mid \Phi_d(p)$

Let p be a prime and $d \geq 1$ an integer. A prime q with

$$q \mid \Phi_d(p)$$

will be called a *cyclotomic prime* for the pair (p, d).

By the basic theory of cyclotomic polynomials we have

$$x^d - 1 = \prod_{e \mid d} \Phi_e(x),$$

and therefore, after evaluating at $x = p$,

$$p^d - 1 = \prod_{e \mid d} \Phi_e(p).$$

Hence, $q \mid \Phi_d(p)$ if and only if q divides $p^d - 1$ but does not divide any $\Phi_e(p)$ with $e < d$.

Equivalently, q is a prime factor of $p^d - 1$ such that the multiplicative order of p modulo q is exactly d.

Lemma 10.1. *Let p and q be distinct primes and $d \geq 1$. If $q \mid \Phi_d(p)$, then the multiplicative order of p modulo q is d, i.e.*

$$\mathrm{ord}_q(p) = d.$$

In particular, $d \mid (q - 1)$ and hence $q \equiv 1 \pmod{d}$.

Proof. From $x^d-1=\prod_{e\mid d}\Phi_e(x)$ we obtain $p^d-1=\prod_{e\mid d}\Phi_e(p)$. If $q\mid\Phi_d(p)$, then $q\mid p^d-1$, so the order $f:=\mathrm{ord}_q(p)$ divides d. On the other hand $\Phi_d(p)\equiv 0 \pmod q$ means that the residue of p modulo q is a primitive d-th root of unity, which forces $f=d$. Since the order of an element in $(\mathbb{Z}/q\mathbb{Z})^\times$ always divides the group order $q-1$, we get $d\mid(q-1)$ and $q\equiv 1 \pmod d$. □

Thus each cyclotomic prime $q\mid\Phi_d(p)$ carries a strong congruence constraint $q\equiv 1 \pmod d$ and sits naturally in the arithmetic of $(\mathbb{Z}/q\mathbb{Z})^\times$ via $\mathrm{ord}_q(p)=d$.

10.2 Primitive prime divisors and Zsigmondy's theorem

We now recall Zsigmondy's theorem in a form adapted to our situation.

Definition 10.2. Let $a>b>0$ be coprime integers and $n\geq 1$. A prime q is called a *primitive prime divisor* of a^n-b^n if

$$q\mid(a^n-b^n)\quad\text{and}\quad q\nmid(a^k-b^k)\ \text{ for all } 1\leq k<n.$$

Theorem 10.3 (Zsigmondy)**.** *Let $a>b>0$ be coprime integers and $n>1$. Then, with the following explicit exceptions, a^n-b^n has a primitive prime divisor:*

- $(a,b,n)=(2,1,6)$*, in which case* $2^6-1=63=3^2\cdot 7$ *and both* 3 *and* 7 *already divide some* 2^k-1 *with* $k<6$*;*
- $(a+b)$ *is a power of* 2 *and* $n=2$*, in which case all prime divisors of* $a^2-b^2=(a-b)(a+b)$ *already divide* $a-b$*.*

In all other cases there exists a prime q which divides a^n-b^n but does not divide a^k-b^k for any $k<n$.

We shall only apply this theorem with $b=1$ and $a=p$ a prime. In this special case the exceptional triples reduce to:

- $(p,n)=(2,6)$, where $2^6-1=63$ has no primitive prime divisor;
- $(p,n)=(M,2)$ with $M+1$ a power of 2, i.e. M a Mersenne prime, where $M^2-1=(M-1)(M+1)$ has only prime divisors of $M-1$ and $M+1$.

Corollary 10.4 (Zsigmondy for p^d-1)**.** *Let p be a prime and $d>1$. Then p^d-1 has a primitive prime divisor q except in the following cases:*

- $(p,d)=(2,6)$*;*
- $(p,d)=(M,2)$ *with M a Mersenne prime (so $M+1$ is a power of 2).*

In particular, for any prime p and any $d\geq 3$ with $(p,d)\neq(2,6)$ there exists a prime q dividing p^d-1 such that $q\nmid p^k-1$ for all $1\leq k<d$.

Combining this with Lemma 10.1 we obtain:

Corollary 10.5 (Primitive cyclotomic primes)**.** *Let p be a prime and $d>1$. Suppose (p,d) is not one of the Zsigmondy exceptional pairs listed in Corollary 10.4. Then there exists a prime q such that*

$$q\mid\Phi_d(p)\quad\textit{and}\quad q\nmid\Phi_e(p)\ \textit{ for all } e\mid d,\ e<d.$$

Equivalently, there exists a prime q with

$$\mathrm{ord}_q(p) = d,$$

which divides $\Phi_d(p)$ but does not divide any $\Phi_e(p)$ with $e < d$. We call such a prime q a primitive cyclotomic prime *for (p, d).*

Proof. By Corollary 10.4 there is a prime q dividing $p^d - 1$ which does not divide $p^k - 1$ for any $k < d$. Factorising $p^d - 1 = \prod_{e|d} \Phi_e(p)$, this implies that q must divide $\Phi_d(p)$ and cannot divide any $\Phi_e(p)$ for $e < d$, since $p^e - 1 = \prod_{f|e} \Phi_f(p)$. Lemma 10.1 then yields $\mathrm{ord}_q(p) = d$. □

10.3 Application to the cyclotomic factorisation of $\sigma(n)$

Recall from Proposition 6.1 that if

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

is the prime factorisation of n, then

$$\sigma(n) = \prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i),$$

and hence

$$\mathrm{rad}(\sigma(n)) = \mathrm{rad}\left(\prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i) \right).$$

Zsigmondy's theorem allows us to identify, for each pair (p_i, d) with $d \mid \alpha_i + 1$ and $d > 1$, primes q that occur *for the first time* in the factor $\Phi_d(p_i)$ and do not divide any $\Phi_e(p_i)$ with $e < d$.

Proposition 10.6 (Primitive primes in $\sigma(p^\alpha)$)**.** *Let p be a prime and $\alpha \geq 1$. Write $m := \alpha + 1$. For each divisor $d \mid m$ with $d > 1$ and (p, d) not in the Zsigmondy exception list of Corollary 10.4, there exists a prime q such that:*

- *$q \mid \Phi_d(p)$, hence $q \mid \sigma(p^\alpha)$;*
- *$q \nmid \Phi_e(p)$ for any $e \mid m$ with $1 < e < d$;*
- *$\mathrm{ord}_q(p) = d$ and therefore $d \mid (q - 1)$.*

In particular, whenever m has at least one divisor $d > 1$ with (p, d) non-exceptional, the radical $\mathrm{rad}(\sigma(p^\alpha))$ contains at least one primitive *prime q arising at the level d.*

Proof. Fix $d \mid m$ with $d > 1$ and assume (p, d) is not exceptional. By Corollary 10.5 there exists a prime q with $q \mid \Phi_d(p)$ and $q \nmid \Phi_e(p)$ for any $e \mid d$, $e < d$. Since $d \mid m$, the factor $\Phi_d(p)$ appears in the product $\sigma(p^\alpha) = \prod_{e|m, e>1} \Phi_e(p)$, so $q \mid \sigma(p^\alpha)$. The non-divisibility for smaller e shows that q appears for the first time at the level d, and Lemma 10.1 gives $\mathrm{ord}_q(p) = d$. □

For a general integer

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

we can combine the contributions from each prime power $p_i^{\alpha_i}$.

Corollary 10.7 (Primitive primes in $\mathrm{rad}(\sigma(n))$)**.** *Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ and, for each i, set $m_i := \alpha_i + 1$. For each index i and each divisor $d \mid m_i$ with $d > 1$ and (p_i, d) not Zsigmondy-exceptional, there exists a prime $q_{i,d}$ such that:*

- *$q_{i,d} \mid \Phi_d(p_i)$ and hence $q_{i,d} \mid \sigma(n)$,*
- *$q_{i,d}$ does not divide any $\Phi_e(p_i)$ with $e \mid m_i$, $1 < e < d$,*
- *$\mathrm{ord}_{q_{i,d}}(p_i) = d$, so $d \mid (q_{i,d} - 1)$.*

In particular, $\mathrm{rad}(\sigma(n))$ contains at least one such primitive prime $q_{i,d}$ for each non-exceptional pair (p_i, d); different pairs may of course yield the same prime, but Zsigmondy's theorem guarantees that, for fixed (p_i, d), there is at least one prime dividing $\sigma(n)$ whose first appearance for the base p_i occurs at the level d.

Remark 10.8. Combining Corollary 10.7 with the Galois-theoretic framework of the polynomials $f_n(x)$ from earlier sections, one can refine these statements as follows: for each primitive cyclotomic prime $q_{i,d} \mid \Phi_d(p_i)$, the order condition $d \mid (q_{i,d} - 1)$ forces the prime divisors of d to appear among the primes $r \mid (q_{i,d} - 1)$ used to define the orbits $\Omega_{q_{i,d},r}$ and the associated intermediate fields $L_{q_{i,d},r} \subset K_{q_{i,d}}$. Thus the cyclotomic structure of $\sigma(n)$, the Zsigmondy primitive primes $q_{i,d}$, and the Galois structure of the polynomials $f_q(x)$ are tightly interwoven.

10.4 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 α is a fixed root of f_q in K_q.

Example 10.9 (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 8.5) 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* α *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* α. *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 10.10 (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 α 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 10.11 (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 α *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 β_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* β_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 β_r and β_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 σ 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 β_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 β_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 β_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 β_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 β_r, and the image of β_r must be a Galois-conjugate of β_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 β_r is Galois-conjugate to β_s. Conversely, if β_r and β_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 β_r and β_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 10.12. 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.

11 Perfect numbers, Zsigmondy primes, and Galois data

We now connect the cyclotomic factorisation of $\sigma(n)$ and Zsigmondy primitive primes with the Galois theory of the MO–polynomials $f_q(x)$. Throughout, q will denote a prime, and $f_q(x) \in \mathbb{Z}[x]$ the associated irreducible polynomial as in the previous sections.

11.1 Cyclotomic factorisation and Zsigmondy primes

Let

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

be the prime factorisation of a positive integer n. Recall from Proposition 6.1 that

$$\sigma(n) = \prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i).$$

Thus every prime divisor ℓ of $\sigma(n)$ arises as a prime divisor of some cyclotomic value $\Phi_d(p_i)$ with $d > 1$ and $d \mid (\alpha_i + 1)$.

If $\ell \nmid p_i$, the following is a standard fact from cyclotomic theory.

Lemma 11.1. *Let p and ℓ be distinct primes, and $d \geq 1$. Then*

$$\ell \mid \Phi_d(p) \quad \Longleftrightarrow \quad \mathrm{ord}_\ell(p) = d.$$

In particular, if $\ell \mid \Phi_d(p)$ then $d \mid (\ell - 1)$ and $\ell \equiv 1 \pmod{d}$.

Proof. From $x^d - 1 = \prod_{e \mid d} \Phi_e(x)$ we get

$$p^d - 1 = \prod_{e \mid d} \Phi_e(p).$$

If $\ell \mid \Phi_d(p)$, then $\ell \mid p^d - 1$, so the order $f := \mathrm{ord}_\ell(p)$ divides d. Conversely, it is a standard fact that $\Phi_d(p) \equiv 0 \pmod{\ell}$ exactly when $p \bmod \ell$ is a primitive dth root of unity, i.e. when $\mathrm{ord}_\ell(p) = d$. The divisibility $d \mid (\ell - 1)$ follows because the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ divides $\ell - 1$. □

We now recall the Zsigmondy notion.

Definition 11.2 (Zsigmondy primitive prime)**.** Let p be a prime and $d > 1$ an integer. A prime q is called a *primitive prime divisor* of $p^d - 1$ if

$$q \mid p^d - 1 \quad \text{and} \quad q \nmid p^e - 1 \ \text{ for all } 1 \leq e < d.$$

Equivalently (by Lemma 11.1), q is primitive if and only if $\mathrm{ord}_q(p) = d$.

In this language, if q is a primitive divisor of $p^d - 1$ then

$$q \mid \Phi_d(p) \quad \text{and} \quad \mathrm{ord}_q(p) = d.$$

Thus in the cyclotomic factorisation of $\sigma(n)$, a Zsigmondy prime q appearing in some factor $\Phi_d(p_i)$ carries a very strong piece of multiplicative information: the order of p_i modulo q is exactly d.

11.2 Galois data attached to primes $q \mid \sigma(n)$

Let q be a prime divisor of $\sigma(n)$, and consider the associated MO–polynomial $f_q(x)$:

- $f_q(x) \in \mathbb{Z}[x]$ is irreducible by assumption,
- K_q is its splitting field over $\mathbb{Q}$,
- $G_q := \mathrm{Gal}(K_q/\mathbb{Q})$ is the Galois group.

For each prime divisor $r \mid (q-1)$ we define, with α a fixed root of f_q,

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

and put $L_{q,r} := \mathbb{Q}(\Omega_{q,r}) \subseteq K_q$.

The abstract Galois structure of these objects is summarised in Lemma 10.11: the stabiliser $H_r := \mathrm{Stab}_{G_q}(\beta_r) \leq G_q$ is a subgroup, and

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

and $L_{q,r} = K_q^{H_r}$ is the fixed field of H_r. Two primes $r, s \mid (q-1)$ give the same orbit $\Omega_{q,r} = \Omega_{q,s}$ if and only if β_r, β_s are Galois-conjugate, equivalently if H_r and H_s are conjugate subgroups in G_q.

Thus *every* prime divisor q of $\sigma(n)$ comes equipped with a finite family of Galois subfields $(L_{q,r})_{r \mid (q-1)}$, one for each prime $r \mid (q-1)$, and these in turn are encoded in the stabiliser subgroups $H_r \leq G_q$.

When q is *Zsigmondy primitive* for some pair (p_i, d) (so $q \mid \Phi_d(p_i)$ and $\mathrm{ord}_q(p_i) = d$) this q has extra arithmetic structure in the Pratt tree of the base prime p_i, and the fields $L_{q,r}$ may be viewed as Galois-theoretic refinements of that Pratt layer.

11.3 Perfect numbers: general picture

Let now n be a perfect number:

$$\sigma(n) = 2n.$$

Write $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. As before, we have

$$2n = \sigma(n) = \prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i).$$

Each prime divisor q of $2n$ (equivalently of $\sigma(n)$) arises as a prime divisor of some $\Phi_d(p_i)$. There are two cases for such a q:

(a) q already divides n; in this case q is one of the primes p_i in the factorisation of n;

(b) q does not divide n, and so is a *new* prime divisor of $\sigma(n)$.

In case (b), q must divide one of the cyclotomic values $\Phi_d(p_i)$ with $d > 1$ and $d \mid (\alpha_i + 1)$. If furthermore q is Zsigmondy primitive for $p_i^d - 1$, then $\mathrm{ord}_q(p_i) = d$ and q does not divide $p_i^e - 1$ for any $e < d$; such primes are "first seen" at the level d of the Pratt tree of p_i.

For *each* prime $q \mid \sigma(n)$ we can attach the Galois data (K_q, G_q) and the subfields $L_{q,r}$ for $r \mid (q-1)$ as above. All these fields sit inside the compositum

$$\mathcal{K}_n := \prod_{q \mid \sigma(n)} K_q,$$

which is itself a subfield of K_m, where $m := \mathrm{rad}(\sigma(n))$ and K_m is the splitting field of $f_m(x) = \prod_{q \mid m} f_q(x)$.

11.4 Even perfect numbers

Every even perfect number n has the classical form

$$n = 2^{p-1}(2^p - 1),$$

where p is prime and $M := 2^p - 1$ is a Mersenne prime. Then

$$\sigma(n) = 2n = 2^p M, \qquad \mathrm{rad}(\sigma(n)) = 2M.$$

On the cyclotomic side one has:

- For the prime 2 with exponent $\alpha_1 = p - 1$,

  $$\alpha_1 + 1 = p, \quad \Phi_p(2) = 2^p - 1 = M.$$

  Here M is the unique Zsigmondy primitive prime divisor of $2^p - 1$.

- For the Mersenne prime M with exponent $\alpha_2 = 1$ we have $\alpha_2 + 1 = 2$, and

  $$\Phi_2(M) = M + 1 = 2^p.$$

  All prime divisors of $\Phi_2(M)$ are equal to 2.

Thus *all* prime divisors of $\sigma(n)$ are already present in n: there are no new Zsigmondy primes beyond 2 and M in this situation. From the MO–polynomial viewpoint,

$$f_{\mathrm{rad}(\sigma(n))}(x) = f_2(x) f_M(x) = x\, f_M(x),$$

and $f_2(x) = x$ contributes no nontrivial Galois extension. Hence

$$K_{\mathrm{rad}(\sigma(n))} = K_M, \qquad G_{\mathrm{rad}(\sigma(n))} \cong G_M.$$

In particular, for an even perfect number the entire Galois-theoretic structure attached to $\sigma(n)$ is encoded in the single prime M and its Galois group G_M. The Zsigmondy-primitive role of M (as a primitive divisor of $2^p - 1$) is reflected purely at this top level.

11.5 Odd perfect numbers

If an odd perfect number n exists, it must satisfy

$$\sigma(n) = 2n, \qquad n \text{ odd}.$$

In particular,

$$\mathrm{rad}(\sigma(n)) = \mathrm{rad}(2n) = 2\ \mathrm{rad}(n),$$

so every prime divisor of $\sigma(n)$ is either 2 or an odd prime divisor of n; there are no "new" primes appearing in $\sigma(n)$.

Write $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with all p_i odd. Then

$$\sigma(n) = \prod_{i=1}^{k} \sigma\big(p_i^{\alpha_i}\big) = \prod_{i=1}^{k} \prod_{\substack{d \mid \alpha_i + 1 \\ d > 1}} \Phi_d(p_i).$$

For each pair (p_i, d) with $d > 1$ and $d \mid \alpha_i + 1$, Zsigmondy's theorem (apart from the usual small exceptional pairs) guarantees the existence of a primitive prime divisor q of $p_i^d - 1$, i.e. a prime q with

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

However, in the perfect case we must have $q \mid \sigma(n) = 2n$, hence necessarily q is either 2 or one of the primes p_j dividing n. Thus Zsigmondy-primitive primes for the various pairs (p_i, d) are "recycled" among the existing prime factors of n; this imposes strong arithmetical constraints on the exponents α_i and the allowed pairs (p_i, d).

For each such Zsigmondy prime q (now necessarily $q \in \{2, p_1, \ldots, p_k\}$) we still obtain a nontrivial Galois package:

- an irreducible MO–polynomial $f_q(x)$ and its Galois group $G_q = \mathrm{Gal}(K_q/\mathbb{Q})$,
- for each prime $r \mid (q-1)$, an orbit $\Omega_{q,r}$ and a Galois subfield $L_{q,r} \subseteq K_q$ as in Lemma 10.11.

All these fields embed into the compositum

$$\mathcal{K}_n := \prod_{q \mid \sigma(n)} K_q = \prod_{q \in \{2, p_1, \ldots, p_k\}} K_q,$$

which is a subfield of the splitting field of $f_m(x)$ with $m = \mathrm{rad}(\sigma(n)) = 2\,\mathrm{rad}(n)$. In other words, a hypothetical odd perfect number forces a large amount of Galois structure built entirely from the MO–polynomials attached to the prime divisors of n (and 2), with Zsigmondy-primitive behaviour appearing at specific cyclotomic layers $\Phi_d(p_i)$ but never introducing new primes beyond those dividing n.

12 Conclusion

The investigations in this paper show that the condition of being a perfect number can be fruitfully examined through the language of Galois theory. By attaching to divisor data certain carefully chosen polynomials, we obtain splitting fields whose Galois groups and discriminants appear to remember aspects of the underlying arithmetic. In particular, the examples studied here suggest that perfection, and more generally strong constraints on the divisor structure of an integer, can leave detectable traces in the algebraic structure of the associated extensions.

At the same time, our results are only a first step. Many of the phenomena we observe are supported by specific examples and computations rather than by complete general theorems. This underscores the need for a more systematic study of the Galois groups arising from divisor-based constructions, and for a better understanding of how classical questions about perfect and almost perfect numbers can be reformulated in field-theoretic terms.

We close by emphasising two directions that seem especially promising. First, there is the possibility of using Galois-theoretic constraints to rule out certain patterns that a hypothetical odd perfect number would have to satisfy. Second, one might hope to adapt ideas from inverse Galois theory to construct families of polynomials whose Galois groups encode prescribed arithmetic properties of their values, including perfection-type conditions. Both directions sit at a natural crossroads between algebraic number theory and classical multiplicative number theory, and we hope that the present work will stimulate further exploration of this interface.

13 Appendix

13.1 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:

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

Definition 13.1 (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 Σ_p denotes the permutation representation

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

Proposition 13.2 (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 Σ_p is a transitive permutation representation.*

(b) *The kernel of Σ_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,*

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

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

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

hence

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

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

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

(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*

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

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 Ω_p and $\Omega_{p,q}$.***

(a) *The formula*

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

defines a well-defined action of G_p on Ω_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:

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

(b) *The action of G_p on $\Omega_{p,q}$ is thus the permutation representation induced from Σ_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*

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

(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 α and hence every polynomial in α with rational coefficients; in particular,

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

(PG10) ***Location of β_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:*

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

(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*

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

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 Σ_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) *β_q and β_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 σ.*

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 Ω_p into orbits.***

(a) *The set Ω_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 8.8).*

Definition 13.3 (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*

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

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 13.2, 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 $L_{p,q}$.

13.2 Primitive element primes and local Galois quotients

Throughout, let p be a prime, and let

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

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 13.2 (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 13.4 (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 13.5 (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 13.4.

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 13.4 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.

13.2.1 Local structure at a primitive element prime

We first record the strengthening of PG10 that holds under Definition 13.4.

Proposition 13.6 (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 13.7 (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 13.8. When p is a primitive element prime, Proposition 13.6 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.

13.2.2 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

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

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 13.2(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.

13.3 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 Appendix **??**, and we fix a splitting field

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

together with a root α_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 13.9. 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 13.10 (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 13.11 (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 13.12. For all tested primes $2 \leq p \leq 37$ 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.

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.

n	Type	$f_n(x)$
1	G	1
2	U	x
3	M	$x+1$
4	G	x^2
5	G	x^2+1
6	M	x^2+x
7	M	x^2+x+1
8	U	x^3
9	M	x^2+2x+1
10	U	x^3+x
11	M	x^3+x+1
12	M	x^3+x^2
13	M	x^3+x^2+1
14	M	x^3+x^2+x
15	M	x^3+x^2+x+1
16	G	x^4
17	G	x^4+1
18	M	x^3+2x^2+x
19	M	x^3+2x^2+x+1
20	G	x^4+x^2
21	M	x^3+2x^2+2x+1
22	M	x^4+x^2+x
23	M	x^4+x^2+x+1
24	M	x^4+x^3
25	G	x^4+2x^2+1
26	M	x^4+x^3+x
27	M	x^3+3x^2+3x+1
28	M	$x^4+x^3+x^2$
29	M	$x^4+x^3+x^2+1$
30	M	$x^4+x^3+x^2+x$
31	M	$x^4+x^3+x^2+x+1$
32	U	x^5
33	M	$x^4+x^3+x^2+2x+1$
34	U	x^5+x
35	M	$x^4+x^3+2x^2+x+1$
36	M	$x^4+2x^3+x^2$
37	M	$x^4+2x^3+x^2+1$
38	M	$x^4+2x^3+x^2+x$
39	M	$x^4+2x^3+x^2+x+1$
40	U	x^5+x^3
41	M	x^5+x^3+1
42	M	$x^4+2x^3+2x^2+x$
43	M	$x^4+2x^3+2x^2+x+1$
44	M	$x^5+x^3+x^2$
45	M	$x^4+2x^3+2x^2+2x+1$
46	M	$x^5+x^3+x^2+x$
47	M	$x^5+x^3+x^2+x+1$
48	M	x^5+x^4
49	M	$x^4+2x^3+3x^2+2x+1$
50	U	x^5+2x^3+x
51	M	x^5+x^4+x+1
52	M	$x^5+x^4+x^2$
53	M	$x^5+x^4+x^2+1$
54	M	$x^4+3x^3+3x^2+x$
55	M	$x^5+2x^3+x^2+x+1$
56	M	$x^5+x^4+x^3$
57	M	$x^4+3x^3+3x^2+2x+1$
58	M	$x^5+x^4+x^3+x$
59	M	$x^5+x^4+x^3+x+1$
60	M	$x^5+x^4+x^3+x^2$
61	M	$x^5+x^4+x^3+x^2+1$
62	M	$x^5+x^4+x^3+x^2+x$
63	M	$x^4+3x^3+4x^2+3x+1$
64	G	x^6

Table 1: Small values of $f_n(x)$ together with their parity type (G = even, U = odd, M = mixed).

p	associated factorisation
5	2^2
17	2^4
101	$2^2 \cdot 5^2$
257	2^8
401	$2^4 \cdot 5^2$
1361	$2^4 \cdot 5 \cdot 17$
1601	$2^6 \cdot 5^2$
5441	$2^6 \cdot 5 \cdot 17$
6869	$2^2 \cdot 17 \cdot 101$
8081	$2^4 \cdot 5 \cdot 101$
8501	$2^2 \cdot 5^3 \cdot 17$
17477	$2^2 \cdot 17 \cdot 257$
25601	$2^{10} \cdot 5^2$
28901	$2^2 \cdot 5^2 \cdot 17^2$
32321	$2^6 \cdot 5 \cdot 101$
62501	$2^2 \cdot 5^6$
65537	2^{16}
82241	$2^6 \cdot 5 \cdot 257$
87041	$2^{10} \cdot 5 \cdot 17$

Table 2: Selected factorisations attached to g-primes (as in the data list).