The Duality of Geometric Primality: Subgroups and Quotients Shape Polygons and Fractals

Youssef Ayyad

Associate Professor, Lebanese University, Faculty of Sciences, e-mail : ayyadyoussef@ul.edu.lb

Ali Ayad

Professor, Lebanese University, Faculty of Sciences, e-mail : ali.ayad@ul.edu.lb

Abstract

This article presents a systematic exposition of the duality between two complementary geometric characterizations of prime numbers, united through Pontryagin duality for finite cyclic groups.

The first characterization is *internal*: an integer $n \geq 2$ is prime if and only if every equitable partition of the vertices of the regular n-gon P_n is fixed classwise only by the identity rotation. We establish a canonical bijection between equitable partitions of P_n and subgroups of the cyclic group $C_n \cong \mathbb{Z}/n\mathbb{Z}$ (Theorem 3.6).

The second characterization is *external* and *fractal*: an integer $n \geq 2$ is prime if and only if the regular polygon G_n is a *primitive leaf* in the universal subdivision tree—that is, G_n has no ancestors other than the root G_1. We prove that G_n appears in the fractal hierarchy $\mathcal{F}(m)$ generated by G_m if and only if $m \mid n$ (Lemma 4.4), establishing a bijection between fractal ancestors of G_n and quotients of C_n (Theorem 4.8).

These two characterizations are not merely equivalent reformulations of the arithmetic definition of primality; they are *canonically dual*. The duality is mediated by the Pontryagin isomorphism $\Phi : \mathrm{Sub}(C_n) \to \mathrm{Quot}(C_n)$ sending a subgroup $H \subseteq C_n$ to its quotient C_n/H. For each proper divisor $d \mid n$ with $1 < d < n$, this duality pairs:

Received ****; Accepted ****.

- *Internally*: the subgroup $H_{n/d} \subseteq C_n$ of order n/d, realized geometrically as an equitable partition $\mathcal{P}_d$ of P_n into d classes;
- *Externally*: the quotient $C_n/H_{n/d} \cong C_d$, realized geometrically as the ancestor polygon G_d in the fractal tree.

These correspondences fit into a commutative diagram (Theorem 5.1) that unifies the two geometric visions: the same divisor d manifests simultaneously as a symmetric coloring of the polygon (internal witness) and as a smaller polygon from which G_n descends (external witness).

We develop this duality, with complete proofs, extensive examples, and visualizations. The framework then generalizes naturally: for arbitrary finite groups, rings, and modules, the duality between substructures and quotient structures can be rendered visible through dual geometric realizations. This suggests a broad research program in *dual geometric algebra*, where abstract algebraic simplicity—the absence of non-trivial substructures or quotients—acquires concrete geometric meaning.

AMS Subject Classification : Primary 11A41; Secondary 20K01, 28A80, 52B15

Key words : Prime numbers, regular polygons, equitable partitions, fractal geometry, Pontryagin duality, cyclic groups, geometric number theory, subgroup lattice, quotient lattice, dual characterizations

1 Introduction

1.1 The Ancient Dialogue Between Geometry and Arithmetic

Geometry and number theory have enjoyed a fruitful dialogue since antiquity. The Pythagoreans visualized arithmetic through figurate numbers, while Euclid's *Elements* interweaves geometric constructions with number-theoretic propositions [14, 15].

A pivotal moment came with Gauss's 1796 discovery that the regular 17-gon is constructible by ruler and compass—a result equivalent to an arithmetic condition on n involving Fermat primes [1, 5]. This marked the first deep equivalence between a geometric property of polygons and an arithmetic property of integers.

Yet despite this heritage, purely geometric characterizations of primality—the most fundamental arithmetic notion—remain rare. Standard definitions are arithmetic or algebraic, offering little geometric intuition. Even the celebrated AKS primality test [2] operates through polynomial congruences, not geometry. This gap motivates our search for genuinely geometric characterizations.

1.2 Two Geometric Visions of Primality

Two distinct geometric approaches to primality have emerged, each rooted in different mathematical traditions.

1.2.1 The Internal Vision: Symmetry and Partitions

A regular n-gon P_n admits an *equitable partition* of its vertices—a partition into equal-sized classes invariant under cyclic translation—precisely when n has a proper divisor $d > 1$: take every d-th vertex to form d classes of size n/d. Such partitions are preserved by non-trivial rotations. Prime numbers, lacking proper divisors, admit only the trivial partitions (one class or n singletons). This yields the internal characterization:

$$n \text{ is prime} \iff \text{every equitable partition of } P_n \text{ is fixed classwise only by the identity.}$$

1.2.2 The External Vision: Fractals and Genealogy

Starting from the unit point G_1 and recursively subdividing arcs into $r \geq 2$ equal parts generates an infinite *fractal tree* of regular polygons. For a fixed G_m, the set $\mathcal{F}(m)$ of all polygons obtained by repeated subdivision satisfies $G_n \in \mathcal{F}(m) \iff m \mid n$. Thus a polygon G_n has non-trivial ancestors exactly when n is composite. This yields the external characterization:

$$n \text{ is prime} \iff G_n \text{ is a primitive leaf in the universal subdivision tree (descended only from } G_1\text{).}$$

1.3 The Central Question: Are These Two Visions Connected?

These characterizations appear unrelated—one internal and static, the other external and genealogical. Yet both reformulate the same arithmetic fact: primality is the absence of proper divisors. This raises a natural question: *Is there a deeper structural relationship between them?*

1.4 Main Contribution: Duality as Unification

We demonstrate that these two visions are not merely equivalent but *canonically dual*. The duality is mediated by the cyclic group $C_n \cong \mathbb{Z}/n\mathbb{Z}$:

- **Internal:** Equitable partitions of P_n correspond bijectively to **subgroups** of C_n (Theorem 3.6).
- **External:** Fractal ancestors of G_n correspond bijectively to **quotients** of C_n (Theorem 4.8).

For finite cyclic groups, the subgroup and quotient lattices are isomorphic under Pontryagin duality $\Phi : H \mapsto C_n/H$. This isomorphism makes the following diagram commute for every proper divisor $d \mid n$:

$$\begin{tikzcd}
H_{n/d} \arrow[r, leftrightarrow, "\text{Pontryagin duality}"] \arrow[d, "\text{internal realization}"'] & C_n/H_{n/d} \arrow[d, "\text{external realization}"] \\
\mathcal{P}_d \arrow[r, leftrightarrow, "\text{index identification}"'] & G_d
\end{tikzcd}$$

Thus each proper divisor d manifests simultaneously as an equitable partition $\mathcal{P}_d$ of P_n (internal witness) and as an ancestor polygon G_d (external witness)—two faces of the same algebraic duality.

1.5 What This Article Is and Is Not

In this article, we present two complementary geometric characterizations of primality. The first is internal: it examines the regular n-gon P_n and its equitable partitions, revealing that prime numbers are precisely those for which no non-trivial equitable partition is fixed classwise by a non-identity rotation. The second is external: it situates the polygon G_n within an infinite fractal tree generated by recursive subdivision, showing that prime numbers correspond exactly to primitive leaves—polygons with no ancestors other than the root G_1.

These characterizations are not merely equivalent reformulations of the arithmetic definition of primality. They are canonically dual. The duality is mediated by the cyclic group $C_n \cong \mathbb{Z}/n\mathbb{Z}$: the internal characterization visualizes the subgroup lattice $\mathrm{Sub}(C_n)$ through symmetric colorings of P_n, while the external characterization visualizes the quotient lattice $\mathrm{Quot}(C_n)$ through genealogical relationships in the fractal tree. Pontryagin duality, the isomorphism $\Phi : H \leftrightarrow C_n/H$, unifies these two geometric worlds into a single coherent framework.

What this article is not: it is not a discovery of new properties of prime numbers, nor a new primality test—our criteria are trial division in disguise, and the fractal construction is a visualization tool, not a source of new arithmetic truths. What this article is: a rigorous exposition of two geometric characterizations of primality; a demonstration that these characterizations are dual under Pontryagin duality, revealing a hidden structural unity; a pedagogical resource that makes abstract algebra visible through concrete geometry; and a research program extending this duality to groups, rings, and modules.

We invite the reader to explore this dual perspective, where the same divisor d manifests simultaneously as a symmetric coloring of a polygon and as an ancestor in a fractal tree—two faces of the same algebraic truth.

1.6 Structure of the Article

Section 2 establishes preliminaries on cyclic groups, polygons, and fractal hierarchies. Section 3 develops the internal characterization (equitable partitions ↔ subgroups). Section 4 develops the external characterization (fractal ancestors ↔ quotients). Section 5 presents the duality theorem unifying both. Section 6 generalizations to Arbitrary Finite Groups and Rings and Ideals.

1.7 Notation and Conventions

$\mathbb{N} = \{1, 2, \ldots\}$; $C_n = \mathbb{Z}/n\mathbb{Z}$ (additive); P_n or G_n denotes the regular n-gon with vertices $v_k = \zeta_n^k$ ($\zeta_n = e^{2\pi i/n}$); ρ_m is rotation by $2\pi m/n$; $d \mid n$ denotes divisibility; $\mathrm{Sub}(G)$ and

Quot(G) are subgroup and quotient lattices; $\mathcal{F}(m) = \{G_{m \cdot r_1 \cdots r_k} : k \geq 0,\ r_i \geq 2\}$.

2 Preliminaries: Algebra and Geometry

2.1 Cyclic Groups: Subgroups, Quotients, and Duality

Definition 2.1 (Cyclic Group)**.** A group G is **cyclic** if there exists an element $g \in G$ such that every element of G is a power of g. For $n \in \mathbb{N}$, the cyclic group of order n is denoted C_n. We adopt the additive notation $C_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ with addition modulo n. The identity element is 0, and the generator is 1.

Theorem 2.2 (Structure of Subgroups of Cyclic Groups)**.** *Let C_n be a cyclic group of order n.*

1. *For each positive divisor $d \mid n$, there exists exactly one subgroup of C_n of order d, namely*
$$H_d = \langle n/d \rangle = \{0, n/d, 2n/d, \ldots, (d-1)n/d\}.$$
2. *Conversely, every subgroup of C_n has order dividing n.*
3. *The subgroup H_d is cyclic, generated by n/d.*
4. *The lattice* Sub(C_n) *is isomorphic to the divisor lattice of n: $H_{d_1} \subseteq H_{d_2}$ iff $d_1 \mid d_2$.*

Proof. This is a standard result in elementary group theory. For completeness, we provide a proof.

(1) Let $d \mid n$, so $n = d \cdot k$ with $k = n/d \in \mathbb{N}$. Consider $H = \langle k \rangle = \{0, k, 2k, \ldots, (d-1)k\}$. Since $d \cdot k = n \equiv 0 \mod n$, the order of k divides d, and because d is the smallest positive integer with $d \cdot k \equiv 0 \mod n$, the order is exactly d. Thus $|H| = d$. Uniqueness: if H' is another subgroup of order d, then its generator must be an element of order d. In C_n, the elements of order d are exactly those of the form $m \cdot k$ where $\gcd(m, d) = 1$, and each such element generates the same subgroup $\langle k \rangle$. Hence $H' = H$.

(2) Let $H \subseteq C_n$ be a subgroup. Let $d = |H|$. By Lagrange's theorem, $d \mid n$.

(3) Clear from the construction.

(4) If $d_1 \mid d_2$, then $n/d_2 \mid n/d_1$, so $H_{d_1} = \langle n/d_1 \rangle$ contains $\langle n/d_2 \rangle = H_{d_2}$. Conversely, if $H_{d_1} \subseteq H_{d_2}$, then the generator of H_{d_2} is a multiple of the generator of H_{d_1}, implying $d_1 \mid d_2$. □

Theorem 2.3 (Structure of Quotients of Cyclic Groups)**.** *Let C_n be a cyclic group of order n.*

1. *For each positive divisor $d \mid n$, there exists exactly one quotient group of C_n of order d, namely*
$$Q_d = C_n / H_{n/d} \cong C_d,$$
where $H_{n/d}$ is the unique subgroup of order n/d.

2. *Conversely, every quotient of* C_n *has order dividing* n.

3. *The lattice* $\mathrm{Quot}(C_n)$ *is anti-isomorphic to the divisor lattice of* n*:* Q_{d_1} *is a quotient of* Q_{d_2} *iff* $d_2 \mid d_1$.

Proof. By the Third Isomorphism Theorem, quotients of a group correspond bijectively to normal subgroups. Since C_n is abelian, all subgroups are normal. The quotient by a subgroup of order n/d has order d. The uniqueness follows from the uniqueness of subgroups. The anti-isomorphism follows from the correspondence: $H_{n/d_1} \subseteq H_{n/d_2}$ iff $n/d_1 \mid n/d_2$ iff $d_2 \mid d_1$, and this inclusion reverses under the quotient map. □

Definition 2.4 (Pontryagin Dual of a Finite Abelian Group)**.** Let G be a finite abelian group. Its **Pontryagin dual** is

$$\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times),$$

the group of characters (homomorphisms from G to the multiplicative group of nonzero complex numbers). For $G = C_n$, we have $\widehat{C_n} \cong C_n$, with the isomorphism given by $k \mapsto (\chi_k : m \mapsto e^{2\pi i k m/n})$.

Proposition 2.5 (Duality for Subgroups and Quotients)**.** *For a finite cyclic group* C_n*, there is a canonical isomorphism of lattices*

$$\Phi : \mathrm{Sub}(C_n) \longrightarrow \mathrm{Quot}(C_n), \quad H \longmapsto C_n/H.$$

Its inverse is $\Psi(Q) = \ker(C_n \to Q)$*. This isomorphism reverses order: if* $H_1 \subseteq H_2$*, then* C_n/H_2 *is a quotient of* C_n/H_1.

Proof. The map is well-defined because every subgroup of an abelian group is normal, hence the quotient exists. The map is bijective because for any quotient Q, its kernel is a subgroup H such that $C_n/H \cong Q$. Uniqueness follows from the uniqueness of subgroups of given order. The order-reversing property follows from the Third Isomorphism Theorem. □

Remark 2.6. For cyclic groups, this duality is elementary and can be understood without reference to Pontryagin duality. However, the Pontryagin framework is essential for generalizations to non-cyclic abelian groups and provides the conceptual foundation for our duality theorem. As we shall see in Section 5, this isomorphism Φ is precisely the bridge that unifies the internal and external geometric characterizations of primality.

2.2 Regular Polygons and Their Symmetries

Definition 2.7 (Regular n-gon)**.** Let $n \geq 3$ be an integer. The **regular** n**-gon** P_n is the convex hull of the n-th roots of unity in the complex plane:

$$P_n = \mathrm{Conv}\{\zeta_n^k : k = 0, 1, \ldots, n-1\}, \qquad \zeta_n = e^{2\pi i/n}.$$

For $n = 1$, we define $P_1 = \{1\}$ (a single point). For $n = 2$, we define $P_2 = [-1, 1]$ (the line segment from -1 to 1). These degenerate cases are included for completeness.

Remark 2.8 (Degenerate cases)**.** For $n = 1$, the vertex set $V = \{v_0\}$ admits only the trivial partition into one class. For $n = 2$, the vertex set $V = \{v_0, v_1\}$ admits two partitions: the trivial partition $\{v_0, v_1\}$ and the discrete partition $\{v_0\}, \{v_1\}$. Both satisfy Definition 3.1 (translation invariance holds vacuously or by swapping). These cases are consistent with Theorem 3.6: C_1 has only the trivial subgroup, and C_2 has subgroups $\{0\}$ and C_2 itself, corresponding to the discrete and trivial partitions respectively. The root G_1 of the fractal tree satisfies $G_1 \star n = G_n$ for all n, including $n = 2$.

Definition 2.9 (Vertex Labeling)**.** We label the vertices of P_n in counterclockwise order as

$$v_0, v_1, \ldots, v_{n-1}, \quad \text{where } v_k = \zeta_n^k.$$

Thus $v_0 = 1$, $v_1 = \zeta_n$, $v_2 = \zeta_n^2$, etc.

Definition 2.10 (Rotation Action)**.** For $m \in \{0, 1, \ldots, n-1\}$, define the **rotation** ρ_m by

$$\rho_m : P_n \to P_n, \quad \rho_m(z) = \zeta_n^m z.$$

On vertices, $\rho_m(v_k) = v_{k+m \mod n}$. The set of rotations

$$R_n = \{\rho_m : m = 0, 1, \ldots, n-1\}$$

forms a cyclic group isomorphic to C_n via the correspondence $\rho_m \leftrightarrow m$.

Definition 2.11 (Dihedral Group)**.** The **dihedral group** D_n of order $2n$ is the full symmetry group of P_n. It consists of:

- The n rotations $R_n \cong C_n$;
- n reflections: if n is odd, reflections through lines through a vertex and the center; if n is even, reflections through opposite vertices or through midpoints of opposite edges.

In this article, we focus primarily on rotations, as they form a cyclic group isomorphic to C_n and suffice for our characterizations.

Remark 2.12 (Group Action on Vertices)**.** The rotation group R_n acts transitively on the vertex set $V = \{v_0, v_1, \ldots, v_{n-1}\}$: for any v_i, v_j, there exists a unique ρ_m such that $\rho_m(v_i) = v_j$ (namely $m = j - i \mod n$). This action is simply transitive: the stabilizer of any vertex is trivial. This allows us to identify the vertex set with the group C_n itself via $v_k \leftrightarrow k$.

2.3 Geometric Multiplication and Fractal Hierarchies

Definition 2.13 (Geometric Multiplication)**.** For integers $a, b \geq 1$, define the **geometric multiplication** of the regular a-gon G_a by b as the regular polygon obtained by subdividing each side-arc of G_a into b equal sub-arcs:

$$G_a \star b := G_{a \times b}.$$

Remark 2.14 (Geometric Interpretation)**.** The vertices of G_a are $\zeta_a^m = e^{2\pi i m/a}$ for $m = 0, \ldots, a-1$. The arc between ζ_a^m and ζ_a^{m+1} is divided into b equal sub-arcs by the points

$$\zeta_a^m \cdot \zeta_{ab}^j = \exp\left(2\pi i \left(\frac{m}{a} + \frac{j}{ab}\right)\right), \quad j = 1, \ldots, b-1.$$

Taking all m and all j (including the original vertices) yields exactly the ab vertices of G_{ab}.

Proposition 2.15 (Algebraic Properties of $\star$)**.** *For all $a, b, c \in \mathbb{N}$:*

1. *Identity: $G_a \star 1 = G_a$.*
2. *Commutativity: $G_a \star b = G_b \star a$ (up to rotation).*
3. *Associativity: $(G_a \star b) \star c = G_a \star (b \times c)$.*
4. *Distributivity over addition: If $b = c + d$, then $G_a \star b$ can be obtained by concatenating $G_a \star c$ and $G_a \star d$ along the circle.*

Proof. (1) Subdividing into 1 part does nothing. (2) The polygon G_{ab} can be obtained either by subdividing G_a into b parts or G_b into a parts; the resulting vertex sets differ by a rotation. (3) Subdividing each arc of G_a into b parts and then each resulting sub-arc into c parts is equivalent to subdividing directly into $b \times c$ parts. (4) Dividing an arc into $c + d$ equal parts is the same as first dividing it into c parts and then adjoining d further subdivisions; this concatenation is performed simultaneously on all arcs. ☐

Definition 2.16 (Fractal Hierarchy)**.** For a fixed integer $m \geq 1$, the **fractal hierarchy** generated by G_m is the set

$$\mathcal{F}(m) = \{G_{m \cdot r_1 r_2 \cdots r_k} : k \geq 0, r_i \geq 2\}.$$

We include $k = 0$ as the trivial product, so $G_m \in \mathcal{F}(m)$. We say that G_n is **fractally dependent** on G_m if $G_n \in \mathcal{F}(m)$.

Remark 2.17 (Universal Subdivision Tree)**.** The union $\bigcup_{m \geq 1} \mathcal{F}(m)$ forms an infinite rooted tree with root G_1. An edge $G_a \to G_{a \cdot r}$ exists for each $r \geq 2$. This tree is a geometric representation of the multiplicative monoid $(\mathbb{N}, \times)$.

2.4 Divisibility and the Fractal Criterion

Lemma 2.18 (Divisibility Criterion for Fractal Dependence)**.** *For integers $m, n \geq 1$, we have*

$$G_n \in \mathcal{F}(m) \quad \textit{if and only if} \quad m \mid n.$$

Proof. $\underline{(\Rightarrow)}$: If $G_n \in \mathcal{F}(m)$, then by definition there exist integers $k \geq 0$ and $r_1, r_2, \ldots, r_k \geq 2$ such that

$$n = m \cdot r_1 r_2 \cdots r_k.$$

Thus m divides n.

(⇐): Suppose $m \mid n$. Write $n = m \cdot t$ with $t \in \mathbb{N}$. If $t = 1$, then $G_n = G_m \in \mathcal{F}(m)$ trivially. If $t \geq 2$, factor t as a product of integers ≥ 2 (this is always possible: for example, if t itself is ≥ 2, we can take $k = 1$ and $r_1 = t$). Then $G_n = G_m \star r_1 \star r_2 \star \cdots \star r_k \in \mathcal{F}(m)$ by definition of the fractal hierarchy. □

Corollary 2.19. *For a fixed n, the set of fractal ancestors of G_n (excluding G_n itself) is*

$$\{G_d : d \mid n, d < n\}.$$

Proof. By Lemma 2.18, G_d is an ancestor of G_n iff $d \mid n$ and $G_n \in \mathcal{F}(d)$. The condition $d < n$ excludes G_n itself. Since $G_n \in \mathcal{F}(d)$ iff $d \mid n$, the result follows. □

Definition 2.20 (Primitive Leaf)**.** A regular polygon G_n is called a **primitive leaf** in the universal subdivision tree if its only fractal ancestor (other than itself) is the root G_1. Equivalently, $G_n \in \mathcal{F}(m)$ implies $m = 1$ or $m = n$.

2.5 Summary of Preliminaries

We have established the following fundamental correspondences that prefigure the duality to come:

Arithmetic	**Group Theory**	**Geometry (Internal/External)**
Divisor $d \mid n$	Subgroup $H_{n/d} \subseteq C_n$ (order n/d)	Equitable partition of P_n into d classes
Divisor $d \mid n$	Quotient $C_n/H_{n/d} \cong C_d$ (order d)	Ancestor polygon G_d in fractal tree

These correspondences form the backbone of our two geometric characterizations. The subgroup lattice $\mathrm{Sub}(C_n)$ will govern the internal structure of P_n (Section 3), while the quotient lattice $\mathrm{Quot}(C_n)$, dual under Φ, will govern the external genealogy of G_n (Section 4). The duality established in Proposition 2.5 is the algebraic preview of the geometric unification to come in Section 5.

3 The Internal Face: Equitable Partitions and Subgroups

3.1 Definition and Basic Properties of Equitable Partitions

Definition 3.1 (Equitable Partition)**.** Let $V = \{v_0, v_1, \ldots, v_{n-1}\}$ be the vertex set of the regular n-gon P_n in cyclic order. A partition $\mathcal{P} = \{C_1, C_2, \ldots, C_k\}$ of V is called **equitable** if it satisfies the following two conditions:

1. **Equal cardinality:** All classes have the same number of elements:

$$|C_1| = |C_2| = \cdots = |C_k| = \frac{n}{k}.$$

   Necessarily, k must divide n.

2. **Translation invariance:** For any class $C_i \in \mathcal{P}$ and any integer $t \in \{0, 1, \ldots, n-1\}$, the translate
$$C_i + t := \{v_{j+t \mod n} : v_j \in C_i\}$$
is also a class of $\mathcal{P}$ (possibly equal to C_i itself).

We denote by $d = n/k$ the **class size**. A partition is called **non-trivial** if $1 < k < n$ (equivalently, $1 < d < n$).

Remark 3.2 (Interpretation of Translation Invariance)**.** Condition (2) is equivalent to requiring that the partition is invariant under the cyclic shift of indices. This means that the pattern of which class each vertex belongs to repeats every d vertices, where $d = n/k$. In other words, if we write the class labels in cyclic order around the polygon, we obtain a periodic sequence with period d.

Example 3.3 ($n = 6$)**.** For the regular hexagon P_6, the divisors are $1, 2, 3, 6$.

- $k = 1$, $d = 6$: The trivial partition $\mathcal{P} = \{V\}$ (one class containing all vertices). This is equitable but trivial.
- $k = 2$, $d = 3$: Partition into two classes of three vertices each:
$$\mathcal{P}_2 = \{\{v_0, v_2, v_4\}, \{v_1, v_3, v_5\}\}.$$
This is equitable: each class has size 3, and translation by $t = 2$ (or any even number) preserves the partition.
- $k = 3$, $d = 2$: Partition into three classes of two vertices each:
$$\mathcal{P}_3 = \{\{v_0, v_3\}, \{v_1, v_4\}, \{v_2, v_5\}\}.$$
This is equitable: each class has size 2, and translation by $t = 3$ (or any multiple of 3) preserves the partition.
- $k = 6$, $d = 1$: The discrete partition $\mathcal{P} = \{\{v_0\}, \{v_1\}, \ldots, \{v_5\}\}$ (each vertex alone). This is equitable but trivial.

Example 3.4 ($n = 5$)**.** For the regular pentagon P_5, the divisors are 1 and 5 only. Therefore, the only equitable partitions are:

- $k = 1$, $d = 5$: One class containing all vertices.
- $k = 5$, $d = 1$: Five classes, each containing one vertex.

No non-trivial equitable partition exists because 5 has no proper divisors.

Example 3.5 ($n = 4$)**.** For the square P_4, divisors are $1, 2, 4$.

- $k = 2$, $d = 2$: Partition into two classes of two vertices each. There are two essentially different such partitions:

  $$\mathcal{P}_{2a} = \{\{v_0, v_2\}, \{v_1, v_3\}\} \quad \text{(opposite vertices)}$$

  $$\mathcal{P}_{2b} = \{\{v_0, v_1\}, \{v_2, v_3\}\} \quad \text{(adjacent vertices)}$$

  However, $\mathcal{P}_{2b}$ is *not* equitable because translation by $t = 1$ sends $\{v_0, v_1\}$ to $\{v_1, v_2\}$, which is not a class. Thus only $\mathcal{P}_{2a}$ is equitable. This illustrates that not every partition with equal class sizes is equitable; the translation invariance condition is restrictive.

3.2 The Fundamental Correspondence: Partitions and Subgroups

We now establish the central theorem linking equitable partitions of P_n to subgroups of the cyclic group C_n. This correspondence reveals that equitable partitions are geometric manifestations of the subgroup lattice $\mathrm{Sub}(C_n)$.

Theorem 3.6 (Partition-Subgroup Correspondence)**.** *Let $n \geq 2$. Identify the vertex v_j of P_n with the element $j \in C_n = \mathbb{Z}/n\mathbb{Z}$. Then there is a bijection between:*

(i) Equitable partitions $\mathcal{P}$ of the vertex set V with k classes (where $k \mid n$), and

(ii) Subgroups $H \subseteq C_n$ of order $d = n/k$.

Under this bijection:

- *The classes of $\mathcal{P}$ are precisely the cosets of H in C_n.*
- *The class size $d = n/k$ equals $|H|$.*
- *The number of classes $k = n/d$ equals the index $[C_n : H]$.*

Proof. We construct explicit bijections in both directions.
Subgroup → Partition: Let $H \subseteq C_n$ be a subgroup of order d, where $d \mid n$. Write $H = \{0, h_1, h_2, \ldots, h_{d-1}\}$ (in additive notation). Since C_n is abelian, the cosets of H are the sets

$$H + x = \{h + x : h \in H\}, \quad x \in C_n.$$

These cosets form a partition of C_n into $k = n/d$ classes, each of size d. Translate this partition back to vertices via the identification $v_j \leftrightarrow j$. The resulting partition $\mathcal{P}_H$ of V is equitable:

- Equal cardinality: each class has size $d = n/k$.
- Translation invariance: for any coset $H + x$ and any $t \in C_n$, $(H + x) + t = H + (x + t)$ is also a coset.

Partition → Subgroup: Let $\mathcal{P} = \{C_1, C_2, \ldots, C_k\}$ be an equitable partition of V with $|C_i| = d = n/k$. Without loss of generality, assume that the vertex v_0 belongs to class C_1. Define

$$H = \{h \in C_n : \rho_h(C_1) = C_1\},$$

where ρ_h is the rotation by h steps. We claim that H is a subgroup of C_n of order d, and that the cosets of H are exactly the classes of $\mathcal{P}$.

Claim 3.7. H is a subgroup of C_n.

Proof. If $h_1, h_2 \in H$, then $\rho_{h_1+h_2}(C_1) = \rho_{h_1}(\rho_{h_2}(C_1)) = \rho_{h_1}(C_1) = C_1$, so $h_1 + h_2 \in H$. Also, if $h \in H$, then $\rho_{-h} = \rho_{n-h}$ is the inverse, and $\rho_{-h}(C_1) = C_1$ because applying ρ_h then ρ_{-h} gives the identity. Thus H is closed under addition and inverses, hence a subgroup. ☐

Claim 3.8. $|H| = d$.

Proof. Since $\mathcal{P}$ is equitable, the vertices in C_1 are equally spaced. Specifically, if $v_{i_1}, v_{i_2}, \ldots, v_{i_d} \in C_1$ with $i_1 < i_2 < \cdots < i_d$, then the differences $i_{j+1} - i_j$ are constant $\pmod n$ and equal to $n/d = k$. Thus $C_1 = \{i_1, i_1 + k, i_1 + 2k, \ldots, i_1 + (d-1)k\} \pmod n$. The rotation ρ_k sends C_1 to itself, so $k \in H$. Moreover, the smallest positive element of H is k, and the subgroup generated by k has order d. Since any element of H must be a multiple of k (otherwise it would send C_1 to a different coset), we have $H = \langle k \rangle$, hence $|H| = d$. ☐

Claim 3.9. The cosets of H are exactly the classes of $\mathcal{P}$.

Proof. For any $x \in C_n$, the coset $H + x$ consists of all vertices obtained by adding x to each element of C_1. Since $\mathcal{P}$ is translation invariant, $H + x$ must be a class of $\mathcal{P}$. Conversely, any class $C \in \mathcal{P}$ can be written as $C = C_1 + x$ for some x (choose any vertex in C and let x be its index minus the index of a vertex in C_1). Thus $C = H + x$, a coset. ☐

Thus, $\mathcal{P}$ corresponds to the subgroup $H = \langle k \rangle$ of order d, and the number of classes is $k = n/d$.

Bijectivity: The two constructions are mutual inverses. Starting from a subgroup H, the partition into cosets yields a subgroup H' equal to H. Starting from an equitable partition $\mathcal{P}$, the subgroup H constructed yields a partition into cosets equal to $\mathcal{P}$. ☐

Corollary 3.10. *A non-trivial equitable partition of P_n exists if and only if n is composite.*

Proof. By Theorem 3.6, non-trivial equitable partitions correspond to subgroups $H \subseteq C_n$ with $1 < |H| < n$. Such subgroups exist iff n has a proper divisor $d = |H|$ with $1 < d < n$, i.e., iff n is composite. ☐

Corollary 3.11. *For each proper divisor $d \mid n$ with $1 < d < n$, there is exactly one equitable partition of P_n into d classes (up to relabeling of classes). This partition corresponds to the subgroup $H_{n/d}$ of order n/d.*

Proof. By Theorem 2.2, there is exactly one subgroup of order n/d. By Theorem 3.6, this subgroup corresponds to exactly one equitable partition into d classes (the partition into cosets). Different labelings of the classes do not change the partition as a set of subsets. ☐

3.3 Symmetry Preservation

Definition 3.12 (Symmetry Preservation)**.** Let $\mathcal{P}$ be a partition of the vertex set V of P_n. A symmetry $\sigma \in D_n$ **preserves** $\mathcal{P}$ if for every class $C \in \mathcal{P}$, the image $\sigma(C) = \{\sigma(v) : v \in C\}$ is also a class of $\mathcal{P}$ (not necessarily the same class). The set of all symmetries preserving $\mathcal{P}$ is denoted

$$\mathrm{Stab}_{D_n}(\mathcal{P}) = \{\sigma \in D_n : \sigma(C) \in \mathcal{P} \text{ for all } C \in \mathcal{P}\}.$$

This is a subgroup of D_n.

The following lemma corrects a subtle but crucial point: while every rotation preserves an equitable partition (by permuting its classes), the rotations that fix each class individually are precisely the elements of the corresponding subgroup.

Lemma 3.13 (Rotation Preservation Criterion)**.** *Let $\mathcal{P}$ be the equitable partition of P_n corresponding to a subgroup $H \subseteq C_n$ via Theorem 3.6. Then:*

1. *Every rotation ρ_m preserves $\mathcal{P}$ (i.e., permutes the classes).*
2. *A rotation ρ_m fixes every class (i.e., $\rho_m(C) = C$ for all classes C) if and only if $m \in H$.*

Proof. Recall that the classes of $\mathcal{P}$ are the cosets $H + x$ for $x \in C_n$.

(1) For any rotation ρ_m and any coset $H + x$, we have

$$\rho_m(H + x) = \{h + x + m : h \in H\} = H + (x + m),$$

which is again a coset of H. Thus ρ_m sends classes to classes, hence preserves $\mathcal{P}$.

(2) For the class H itself, $\rho_m(H) = H + m$. This equals H if and only if $m \in H$. If $m \in H$, then for any $x \in C_n$,

$$\rho_m(H + x) = H + x + m = H + x$$

because $m \in H$ implies $H + m = H$. Thus ρ_m fixes every class. Conversely, if ρ_m fixes every class, then in particular it fixes H, so $m \in H$. □

Remark 3.14. The distinction between preserving a partition (permuting classes) and fixing every class individually is essential for the primality criterion. The corrected lemma shows that the subgroup H is precisely the set of rotations that fix each class pointwise, while all rotations preserve the partition as a permutation of classes.

3.4 The Internal Primality Criterion

We now state and prove the main theorem of the internal characterization. The key insight is that primality corresponds to the absence of non-trivial subgroups, which geometrically manifests as the absence of non-trivial equitable partitions that are fixed classwise by a non-identity rotation.

Theorem 3.15 (Internal Geometric Primality Criterion)**.** *Let $n \geq 2$. The following statements are equivalent:*

(1) n is prime.

(2) For every equitable partition $\mathcal{P}$ of the vertices of P_n with more than one class ($k > 1$), the only rotation that fixes every class of $\mathcal{P}$ is the identity rotation ρ_0.

(3) The cyclic group C_n has no proper non-trivial subgroup.

Proof. We prove the chain of equivalences (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (2).
(1) $\Leftrightarrow$ (3): This is standard group theory. C_n has a subgroup of order d iff $d \mid n$. Thus C_n has no proper non-trivial subgroup iff the only divisors of n are 1 and n, i.e., iff n is prime.
(3) $\Rightarrow$ (2): Assume C_n has no proper non-trivial subgroup. By Theorem 3.6, every equitable partition of P_n corresponds to a subgroup of C_n. Since the only subgroups are $\{0\}$ (order 1) and C_n itself (order n), the only equitable partitions are:

- The partition into n classes (each vertex alone), corresponding to $H = \{0\}$.
- The partition into 1 class (all vertices together), corresponding to $H = C_n$.

The partition into n classes has the property that a rotation ρ_m fixes every class iff $\rho_m(v_j) = v_j$ for all j, which happens only when $m \equiv 0 \mod n$, i.e., $\rho_m = \rho_0$ (the identity). Thus condition (2) holds for this partition. The partition into 1 class has $k = 1$, which is excluded by the hypothesis "$k > 1$". Therefore, condition (2) holds vacuously for all equitable partitions with $k > 1$ (there are none).
(2) $\Rightarrow$ (3): We prove the contrapositive. Suppose C_n has a proper non-trivial subgroup H of order d with $1 < d < n$. By Theorem 3.6, H corresponds to an equitable partition $\mathcal{P}$ of P_n with $k = n/d$ classes (note that $k > 1$ because $d < n$, and $k < n$ because $d > 1$). By Lemma 3.13(2), any non-identity rotation ρ_m with $m \in H$ fixes every class of $\mathcal{P}$. Since H is non-trivial, such an $m \neq 0$ exists. Thus $\mathcal{P}$ is an equitable partition with $k > 1$ that is fixed classwise by a non-identity rotation, contradicting (2). □

Remark 3.16 (Why We Require "Fixes Every Class")**.** The subtlety in Lemma 3.13 reveals why we must phrase condition (2) in terms of rotations that fix *every* class, rather than simply preserve the partition. Every rotation preserves every equitable partition (by permuting classes), so preservation alone cannot distinguish prime from composite. The distinction lies in whether there exists a non-identity rotation that fixes each class individually—this happens exactly when the partition corresponds to a non-trivial subgroup H, and the rotation is by an element of H.

Corollary 3.17 (Geometric Compositeness Criterion)**.** *An integer $n \geq 2$ is composite if and only if there exists a non-trivial equitable partition $\mathcal{P}$ of P_n and a non-identity rotation ρ_m such that $\rho_m(C) = C$ for every class $C \in \mathcal{P}$.*

Proof. Immediate from Theorem 3.15 and its proof. □

3.5 Examples and Visualizations

Example 3.18 ($n = 6$ (Composite))**.** Consider P_6, the regular hexagon.

- **Subgroup $H = \langle 2 \rangle = \{0, 2, 4\}$ of order 3.** This corresponds to the equitable partition $\mathcal{P}_2$ into 2 classes of 3 vertices each:

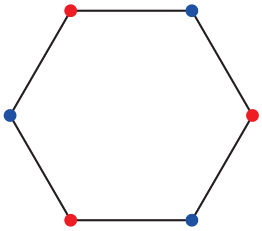
  $$\mathcal{P}_2 = \{\{v_0, v_2, v_4\}, \{v_1, v_3, v_5\}\}.$$

  The rotation ρ_2 (by 120°) fixes every class: $\rho_2(\{v_0, v_2, v_4\}) = \{v_2, v_4, v_0\} = \{v_0, v_2, v_4\}$, and similarly for the other class. Thus ρ_2 is a non-identity rotation fixing every class, witnessing compositeness.

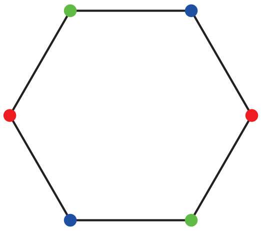
- **Subgroup $H = \langle 3 \rangle = \{0, 3\}$ of order 2.** This corresponds to the equitable partition $\mathcal{P}_3$ into 3 classes of 2 vertices each:

  $$\mathcal{P}_3 = \{\{v_0, v_3\}, \{v_1, v_4\}, \{v_2, v_5\}\}.$$

  The rotation ρ_3 (by 180°) fixes every class: $\rho_3(\{v_0, v_3\}) = \{v_3, v_0\} = \{v_0, v_3\}$, etc. Thus ρ_3 is another witness.



Partition $\mathcal{P}_2$: ρ_2 fixes each class



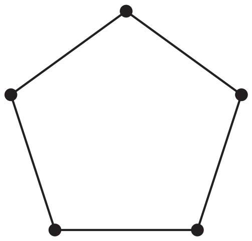
Partition $\mathcal{P}_3$: ρ_3 fixes each class

Example 3.19 ($n = 5$ (Prime))**.** Consider P_5, the regular pentagon.

Since 5 is prime, the only divisors are 1 and 5. By Theorem 3.6, the only equitable partitions are:

- One class containing all 5 vertices ($k = 1$, $d = 5$)
- Five classes, each containing one vertex ($k = 5$, $d = 1$)

The partition into five singleton classes has the property that a rotation fixes every class iff it fixes every vertex individually, which only happens for the identity rotation. Thus condition (2) of Theorem 3.15 is satisfied.



Pentagon P_5: no non-trivial equitable partition

Example 3.20 ($n = 9$ (Composite))**.** For P_9, the regular nonagon, the proper divisors are 3. The subgroup $H = \langle 3 \rangle = \{0, 3, 6\}$ of order 3 corresponds to an equitable partition into $k = 3$ classes of size $d = 3$:

$$\mathcal{P}_3 = \{\{v_0, v_3, v_6\}, \{v_1, v_4, v_7\}, \{v_2, v_5, v_8\}\}.$$

The rotation ρ_3 (by 120°) fixes each class individually, witnessing compositeness.

Example 3.21 ($n = 12$ (Composite))**.** For P_{12}, the regular dodecagon, there are multiple proper divisors: 2,3,4,6. Each corresponds to a subgroup and hence to an equitable partition. For instance:

- $d = 6$ (subgroup of order 6): partition into 2 classes of 6 vertices each, fixed by ρ_6.
- $d = 4$ (subgroup of order 4): partition into 3 classes of 4 vertices each, fixed by ρ_4.
- $d = 3$ (subgroup of order 3): partition into 4 classes of 3 vertices each, fixed by ρ_3.
- $d = 2$ (subgroup of order 2): partition into 6 classes of 2 vertices each, fixed by ρ_2.

All of these provide witnesses to compositeness.

3.6 Summary of Internal Characterization

The internal characterization provides a complete geometric translation of the arithmetic property of primality into the language of polygon symmetries and equitable partitions. The key results are:

- **Theorem 3.6:** Equitable partitions $\leftrightarrow$ subgroups of C_n. This establishes that the internal geometry of P_n is governed by the subgroup lattice $\mathrm{Sub}(C_n)$.
- **Corollary 3.10:** Non-trivial equitable partitions exist iff n is composite.
- **Lemma 3.13:** Rotations that fix every class correspond precisely to elements of the subgroup. All other rotations permute the classes.
- **Theorem 3.15:** n is prime iff no non-trivial equitable partition admits a non-identity rotation fixing every class.

This characterization is *internal* because it only examines the polygon P_n itself, its vertex set, and its rotation symmetries. No external objects or hierarchies are involved. The subgroups of C_n manifest geometrically as symmetric colorings of the polygon, providing a visual representation of the divisor structure of n. In Section 4, we will see how the dual notion—quotients of C_n—manifests in an external fractal hierarchy.

4 The External Face: Fractal Isolation and Quotients

4.1 The Fractal Subdivision Tree

We now develop the external characterization, which situates each regular polygon G_n within an infinite fractal tree generated by recursive subdivision. This external perspective will reveal how the quotient lattice $\mathrm{Quot}(C_n)$ manifests geometrically.

Definition 4.1 (Universal Subdivision Tree)**.** Define a rooted tree $\mathcal{T}$ as follows:

- The root is G_1, the degenerate polygon consisting of a single point.
- For each node G_m and each integer $r \geq 2$, there is a child node $G_{m \cdot r}$ connected by an edge $G_m \to G_{m \cdot r}$.

We call $\mathcal{T}$ the **universal subdivision tree**. The set of all nodes is $\{G_n : n \geq 1\}$.

Remark 4.2 (Tree Structure)**.** $\mathcal{T}$ is indeed a tree: there is a unique path from the root G_1 to any node G_n, given by factoring n into prime powers (the order of multiplications corresponds to the order of subdivisions). The tree is infinite and each node has infinitely many children (one for each $r \geq 2$).

Definition 4.3 (Fractal Hierarchy Revisited)**.** For a fixed node G_m, the **fractal hierarchy** $\mathcal{F}(m)$ is the set of all descendants of G_m in $\mathcal{T}$:

$$\mathcal{F}(m) = \{G_n : \text{there exists a path } G_m \to \cdots \to G_n\}.$$

Equivalently, $\mathcal{F}(m) = \{G_{m \cdot r_1 r_2 \cdots r_k} : k \geq 0, r_i \geq 2\}$, which matches Definition 2.16.

Lemma 4.4 (Divisibility Criterion for Descendants)**.** *For $m, n \geq 1$, we have $G_n \in \mathcal{F}(m)$ if and only if $m \mid n$.*

Proof. We have already proved this as Lemma 2.18. The proof is repeated here for completeness.
($\Rightarrow$): If $G_n \in \mathcal{F}(m)$, then by definition there exist $k \geq 0$ and $r_i \geq 2$ such that $n = m \cdot r_1 r_2 \cdots r_k$. Hence $m \mid n$.
($\Leftarrow$): If $m \mid n$, write $n = m \cdot t$. If $t = 1$, then $G_n = G_m \in \mathcal{F}(m)$ trivially. If $t \geq 2$, we can take $k = 1$ and $r_1 = t$ (or factor t further if desired). Then $G_n = G_m \star t \in \mathcal{F}(m)$. □

Corollary 4.5 (Ancestors)**.** *For a fixed n, the set of ancestors of G_n in $\mathcal{T}$ (excluding G_n itself) is*

$$\mathrm{Anc}(G_n) = \{G_d : d \mid n, d < n\}.$$

Proof. G_d is an ancestor of G_n iff $G_n \in \mathcal{F}(d)$ and $d \neq n$. By Lemma 4.4, $G_n \in \mathcal{F}(d)$ iff $d \mid n$. The condition $d < n$ excludes G_n itself. □

Definition 4.6 (Primitive Leaf)**.** A node G_n in $\mathcal{T}$ is called a **primitive leaf** if its only ancestor (other than itself) is the root G_1. Equivalently, $\mathrm{Anc}(G_n) = \{G_1\}$.

Proposition 4.7 (Characterization of Primitive Leaves)**.** *G_n is a primitive leaf if and only if n is prime or $n = 1$.*

Proof. By Corollary 4.5, $\mathrm{Anc}(G_n) = \{G_d : d \mid n, d < n\}$. This set equals $\{G_1\}$ iff the only divisor of n less than n is 1, i.e., iff n is prime or $n = 1$. □

4.2 Quotients and Fractal Ancestors

We now establish the connection between the fractal tree and the quotient lattice of C_n. This correspondence reveals that fractal ancestors are geometric manifestations of the quotient lattice $\mathrm{Quot}(C_n)$, dual to the subgroup lattice that governed the internal characterization.

Theorem 4.8 (Quotient-Ancestor Correspondence). *Let $n \geq 2$. There is a bijection between:*

(i) Proper non-trivial quotients of the cyclic group C_n, and

(ii) Proper ancestors of G_n in the universal subdivision tree $\mathcal{T}$ (i.e., nodes G_d with $1 < d < n$ and $d \mid n$).

The bijection is given by

$$Q_d = C_n/H_{n/d} \quad \longleftrightarrow \quad G_d,$$

where $H_{n/d}$ is the unique subgroup of C_n of order n/d.

Proof. By Theorem 2.3, for each divisor $d \mid n$ with $1 < d < n$, there is a unique quotient $Q_d \cong C_d$ of order d. By Corollary 4.5, for each such divisor d, G_d is an ancestor of G_n. The map $Q_d \mapsto G_d$ is clearly bijective, with inverse $G_d \mapsto C_n/H_{n/d}$. Both sets have cardinality equal to the number of proper divisors of n. □

Corollary 4.9. *C_n has no proper non-trivial quotient if and only if G_n has no proper non-trivial ancestor in $\mathcal{T}$ (other than G_1).*

Proof. C_n has no proper non-trivial quotient iff the only divisors of n are 1 and n, i.e., iff n is prime. By Proposition 4.7, this is exactly the condition that G_n is a primitive leaf, i.e., has no proper non-trivial ancestor other than G_1. □

4.3 The External Primality Criterion

We now state and prove the main theorem of the external fractal characterization. Just as the internal characterization translated the absence of non-trivial subgroups into a geometric condition on P_n, the external characterization translates the absence of non-trivial quotients into a geometric condition on the position of G_n in the fractal tree.

Theorem 4.10 (External Geometric Primality Criterion). *Let $n \geq 2$. The following statements are equivalent:*

(1) n is prime.

(2) G_n is a primitive leaf in the universal subdivision tree $\mathcal{T}$: for every m with $2 \leq m < n$, $G_n \notin \mathcal{F}(m)$.

(3) The cyclic group C_n has no proper non-trivial quotient.

Proof. We prove the equivalences directly.

(1) ⇔ (2): By Lemma 4.4, $G_n \in \mathcal{F}(m)$ iff $m \mid n$. Thus $G_n \notin \mathcal{F}(m)$ for all $2 \leq m < n$ iff no integer m with $2 \leq m < n$ divides n, i.e., iff the only divisors of n are 1 and n, i.e., iff n is prime.

(1) ⇔ (3): By Theorem 2.3, C_n has a quotient of order d iff $d \mid n$. Thus C_n has a proper non-trivial quotient iff n has a proper divisor d with $1 < d < n$, i.e., iff n is composite. Hence C_n has no proper non-trivial quotient iff n is prime.

(2) ⇔ (3): This follows from Corollary 4.9, or from the transitivity of equivalences (1)⇔(2) and (1)⇔(3). □

Remark 4.11 (Geometric Interpretation)**.** The external characterization is beautifully intuitive: prime numbers correspond to polygons that are *isolated* in the fractal forest. They have no non-trivial ancestors; they are born directly from the root G_1 through a single subdivision into n equal parts. Composite numbers, by contrast, have rich genealogies—they can be reached by subdividing various proper divisors. This genealogical tree is the geometric realization of the quotient lattice $\mathrm{Quot}(C_n)$.

4.4 Visualizing the Fractal Tree

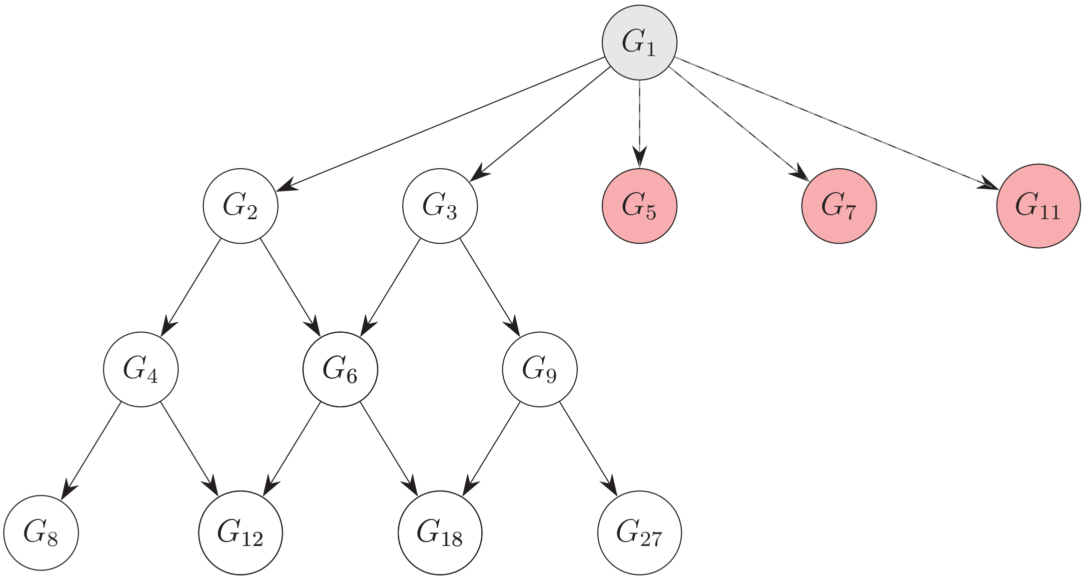


Figure 1: The universal subdivision tree $\mathcal{T}$ (partial).

Figure 1: The universal subdivision tree $\mathcal{T}$ (partial). Nodes in red (G_5, G_7, G_{11}) are primitive leaves, corresponding to prime numbers. Composite nodes like G_6, G_8, G_9, G_{12} have multiple ancestors, each ancestor corresponding to a quotient of C_n.

Example 4.12 ($n = 12$ in the Fractal Tree)**.** The node G_{12} has multiple ancestors:

- G_1 (root) via $12 = 1 \cdot 12$
- G_2 via $12 = 2 \cdot 6$ — corresponding to the quotient $C_{12}/H_6 \cong C_2$

- G_3 via $12 = 3 \cdot 4$ — corresponding to the quotient $C_{12}/H_4 \cong C_3$
- G_4 via $12 = 4 \cdot 3$ — corresponding to the quotient $C_{12}/H_3 \cong C_4$
- G_6 via $12 = 6 \cdot 2$ — corresponding to the quotient $C_{12}/H_2 \cong C_6$

Thus G_{12} is not a primitive leaf; its compositeness is visible through its rich ancestry, each ancestor being the geometric dual of an equitable partition of P_{12}.

Example 4.13 ($n = 7$ in the Fractal Tree)**.** The node G_7 has only the ancestor G_1 (since $7 = 1 \cdot 7$). It is a primitive leaf, reflecting the primality of 7. Correspondingly, C_7 has no non-trivial quotients.

4.5 Summary of External Characterization

The external characterization provides a complementary geometric translation of primality into the language of fractal genealogy. The key results are:

- **Lemma 4.4:** $G_n \in \mathcal{F}(m)$ iff $m \mid n$. This establishes that the fractal hierarchy encodes the divisibility relation.
- **Corollary 4.5:** Ancestors of G_n correspond bijectively to divisors of n.
- **Theorem 4.8:** Fractal ancestors correspond bijectively to quotients of C_n. This reveals that the external genealogy of G_n is governed by the quotient lattice $\mathrm{Quot}(C_n)$.
- **Proposition 4.7:** G_n is a primitive leaf iff n is prime or $n = 1$.
- **Theorem 4.10:** n is prime iff G_n is a primitive leaf, i.e., iff C_n has no non-trivial quotients.

This characterization is *external* because it places G_n in a larger context—the infinite fractal tree generated by subdivision—and examines its genealogical relationships. Just as the internal characterization (Section 3) realized the subgroup lattice $\mathrm{Sub}(C_n)$ as equitable partitions of P_n, the external characterization realizes the dual quotient lattice $\mathrm{Quot}(C_n)$ as ancestors in the fractal tree. In Section 5, we will unite these two perspectives through Pontryagin duality.

5 The Duality Theorem: Unifying the Two Faces

Having developed the internal characterization (Section 3)—where subgroups of C_n manifest as equitable partitions of P_n—and the external characterization (Section 4)—where quotients of C_n manifest as ancestors in the fractal tree—we now reveal that these two perspectives are not merely parallel but are *canonically dual*. The duality is mediated by the Pontryagin isomorphism between the subgroup lattice and the quotient lattice of a finite cyclic group.

5.1 The Duality Diagram

We now arrive at the central contribution of this article: the demonstration that the internal and external characterizations are unified through Pontryagin duality for finite cyclic groups.

Theorem 5.1 (Geometric Duality)**.** *Let $n \geq 2$ and let d be a divisor of n with $1 < d < n$. Define:*

- *$H_{n/d} \subseteq C_n$: the unique subgroup of order n/d (generated by d).*
- *$\mathcal{P}_d$: the equitable partition of P_n into d classes of size n/d, corresponding to $H_{n/d}$ via Theorem 3.6.*
- *$Q_d = C_n/H_{n/d}$: the quotient group of order d, isomorphic to C_d.*
- *G_d: the ancestor polygon of G_n in the fractal tree, corresponding to the divisor d via Theorem 4.8.*

Then the following diagram commutes:

$$\begin{tikzcd}
H_{n/d} \arrow[r, leftrightarrow, "\textit{Pontryagin duality}"] \arrow[d, "\textit{internal realization}"'] & C_n/H_{n/d} \arrow[d, "\textit{external realization}"] \\
\mathcal{P}_d \arrow[r, leftrightarrow, "\textit{index identification}"'] & G_d
\end{tikzcd}$$

where:

- *The* ***top horizontal arrow*** *is the canonical isomorphism $\Phi : \mathrm{Sub}(C_n) \to \mathrm{Quot}(C_n)$ given by $H \mapsto C_n/H$ (Proposition 2.5).*
- *The* ***left vertical arrow*** *is the bijection of Theorem 3.6, sending a subgroup to its corresponding equitable partition.*
- *The* ***right vertical arrow*** *is the bijection of Theorem 4.8, sending a quotient to its corresponding ancestor polygon.*
- *The* ***bottom horizontal arrow*** *is the identification via the common index d: both $\mathcal{P}_d$ and G_d are naturally indexed by the divisor d.*

Proof. We verify commutativity by tracing an element through the diagram in both directions.

Start at $H_{n/d}$:

1. Apply the left vertical arrow: by Theorem 3.6, $H_{n/d}$ corresponds to the equitable partition $\mathcal{P}_d$ into d classes of size n/d.
2. Apply the top horizontal arrow: $H_{n/d}$ maps to $C_n/H_{n/d} \cong C_d$, the quotient of order d.

3. Apply the right vertical arrow: by Theorem 4.8, the quotient C_d corresponds to the ancestor polygon G_d.

4. The bottom horizontal arrow identifies $\mathcal{P}_d$ with G_d via the common index d.

Thus, going clockwise ($H_{n/d} \to \mathcal{P}_d \to G_d$) yields the same result as going counterclockwise ($H_{n/d} \to C_n/H_{n/d} \to G_d$), after applying the bottom identification.

Start at $\mathcal{P}_d$:

1. By Theorem 3.6, $\mathcal{P}_d$ corresponds to the subgroup $H_{n/d}$.

2. From $H_{n/d}$, we proceed as above.

The diagram commutes in all possible ways. □

Corollary 5.2 (Dual Witnesses of Compositeness)**.** *For each proper divisor d of a composite number n, there is a pair of dual geometric witnesses to compositeness:*

- ***Internal witness:*** *The equitable partition $\mathcal{P}_d$ of P_n, which is fixed classwise by any non-identity rotation ρ_m with $m \in H_{n/d}$ (Lemma 3.13).*

- ***External witness:*** *The ancestor polygon G_d in the fractal tree, which demonstrates that G_n is not a primitive leaf (Proposition 4.7).*

These two witnesses are dual under the Pontryagin isomorphism $H_{n/d} \leftrightarrow C_n/H_{n/d}$.

Remark 5.3 (The Prime Case)**.** For a prime number p, the duality diagram collapses: there are no proper divisors, hence no non-trivial subgroups, no non-trivial equitable partitions, no non-trivial quotients, and no non-trivial fractal ancestors. The duality becomes vacuous—a perfect geometric reflection of the arithmetic fact that primes have no proper divisors.

Remark 5.4 (Naturality of the duality)**.** The commutativity established in Theorem 5.1 is not merely a pointwise bijection but respects the order structure of the divisor lattice. If $d_1 \mid d_2$, then we have inclusions $H_{n/d_2} \subseteq H_{n/d_1}$ and surjections $C_n/H_{n/d_1} \twoheadrightarrow C_n/H_{n/d_2}$. The following diagram commutes:

$$\begin{tikzcd}
H_{n/d_1} \arrow[r, leftrightarrow, "\Phi"] \arrow[d, hook] & C_n/H_{n/d_1} \arrow[d] \\
H_{n/d_2} \arrow[r, leftrightarrow, "\Phi"] & C_n/H_{n/d_2}
\end{tikzcd}$$

This functoriality means the duality is an isomorphism of posets (lattices), not just a bijection between sets. Geometrically, it ensures that refinements of equitable partitions correspond to chains of ancestors in the fractal tree.

5.2 Interpretation of the Duality

The duality theorem reveals that the internal and external characterizations are not independent discoveries but rather two manifestations of the same underlying algebraic duality. For a composite number n, each proper divisor d produces:

1. **Internally:** A subgroup $H_{n/d} \subseteq C_n$. This subgroup gives rise to an equitable partition $\mathcal{P}_d$ of P_n into d classes, and the non-identity elements of $H_{n/d}$ are precisely the rotations that fix every class of $\mathcal{P}_d$.
2. **Externally:** A quotient $C_n/H_{n/d} \cong C_d$. This quotient gives rise to an ancestor polygon G_d in the fractal tree, and the existence of this ancestor shows that G_n is not a primitive leaf.

The duality isomorphism $H_{n/d} \leftrightarrow C_n/H_{n/d}$ connects these two manifestations: the subgroup that *fixes the internal partition* is dual to the quotient that *generates the external ancestor*. The same divisor d is simultaneously:

- The number of classes in the equitable partition (internal)
- The order of the quotient group (algebraic)
- The number of sides of the ancestor polygon (external)

This triple role of d—geometric (partition), algebraic (quotient order), and geometric again (ancestor)—exemplifies the deep unity that duality reveals.

5.3 Visualizing the Duality

Example 5.5 (The Duality for $n = 12$)**.** Table 1 illustrates the duality for all proper divisors of 12:

Table 1: Duality data for $n = 12$

Divisor d	**Subgroup** $H_{12/d}$	**Partition** $\mathcal{P}_d$	**Quotient** $C_{12}/H_{12/d}$	**Ancestor** G_d
2	$H_6 = \langle 2 \rangle$ (order 6)	2 classes of 6 vertices	C_2	G_2
3	$H_4 = \langle 3 \rangle$ (order 4)	3 classes of 4 vertices	C_3	G_3
4	$H_3 = \langle 4 \rangle$ (order 3)	4 classes of 3 vertices	C_4	G_4
6	$H_2 = \langle 6 \rangle$ (order 2)	6 classes of 2 vertices	C_6	G_6

For each divisor d, the diagram commutes:

- The subgroup $H_{12/d}$ maps via Pontryagin duality to the quotient $C_{12}/H_{12/d} \cong C_d$.
- The subgroup $H_{12/d}$ maps via internal realization to the equitable partition $\mathcal{P}_d$.
- The quotient C_d maps via external realization to the ancestor polygon G_d.
- The partition $\mathcal{P}_d$ and the ancestor G_d are both indexed by the same divisor d.

Thus, each proper divisor of 12 provides a dual pair of geometric witnesses to compositeness.

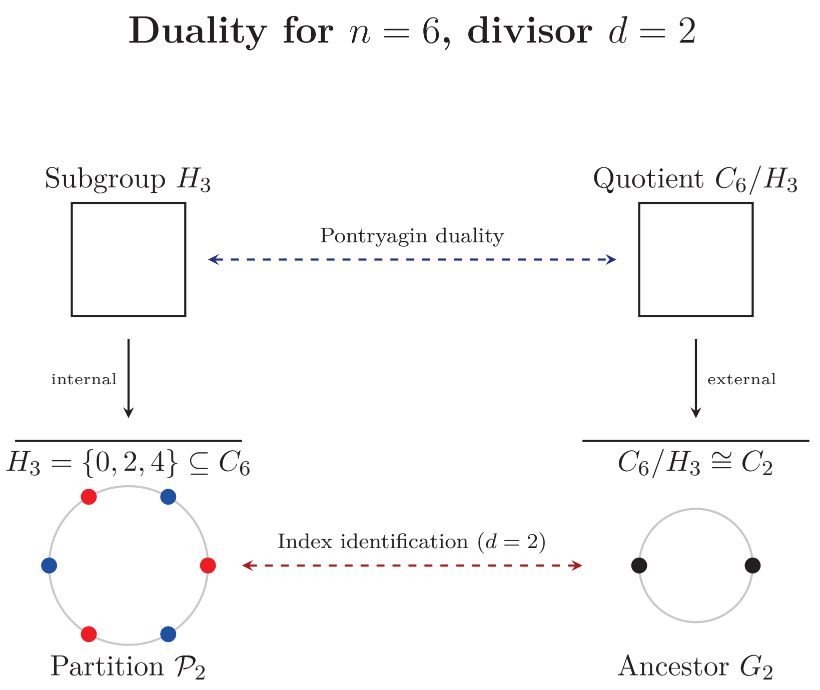


Figure 2: Duality diagram for $n = 6$, $d = 2$.

5.4 Why Duality Matters

The duality theorem is significant for several reasons:

1. **Unification:** It shows that two seemingly different geometric characterizations are in fact two sides of the same coin. This unifies the internal (symmetry/partition) perspective and the external (fractal/genealogical) perspective into a single coherent framework.

2. **Explanation:** It explains *why* both characterizations work: they are both translations of the same algebraic fact—the divisor lattice of n—into geometric language, via the two dual aspects of group theory (subgroups and quotients). The internal characterization visualizes subgroups; the external visualizes their dual quotients.

3. **Visualization:** It provides a complete geometric dictionary for translating between internal and external witnesses of compositeness. Given an equitable partition of P_n, one can construct the corresponding ancestor polygon G_d; given an ancestor G_d, one can reconstruct the corresponding equitable partition. The duality makes this translation canonical and bijective.

4. **Generalization:** It reveals a pattern that extends far beyond cyclic groups and prime numbers. The duality between substructures and quotient structures is a universal feature of algebraic categories (groups, rings, modules, etc.). Our geometric realization suggests a systematic method for visualizing this duality in diverse contexts, as we explore in Section 6.

5. **Pedagogy:** It offers a powerful teaching tool. Students can see that the same divisor d manifests in two completely different ways—as a symmetric coloring of the polygon

and as a smaller polygon that is an ancestor—and that these two manifestations are dual to each other. This concrete visualization makes abstract duality tangible.

Remark 5.6 (The Essence of Duality)**.** The duality theorem captures the essence of why geometry can reflect arithmetic: the divisor structure of an integer n is encoded simultaneously in the symmetry group of P_n (through its subgroups) and in the genealogical tree of G_n (through its quotients). Pontryagin duality, the isomorphism between these two lattices, is the bridge that connects the internal and external geometric worlds. Prime numbers are precisely those for which both sides of this bridge are empty—a perfect geometric silence reflecting arithmetic simplicity.

6 Generalizations to Arbitrary Finite Groups and Rings and Ideals

The duality between internal and external geometric characterizations, which we have established for cyclic groups and prime numbers, is not an isolated phenomenon. Rather, it is a special case of a universal pattern: in any algebraic category, the duality between substructures and quotient structures can be rendered visible through appropriate geometric realizations. This section extends the framework in two natural directions: first to arbitrary finite groups (Section 6.1), where the duality is mediated by Pontryagin duality for abelian groups and by normal subgroups for non-abelian groups; and second to commutative rings and ideals (Section 6.2), where ideals play the role of substructures and quotient rings play the role of their duals. We conclude by outlining a systematic research program in dual geometric algebra (Section 6.3) that aims to unify the study of algebraic simplicity across diverse mathematical categories.

6.1 Generalization to Arbitrary Finite Groups

The duality we have uncovered for cyclic groups is a special case of a much more general phenomenon. For any finite group G, there is a duality between its lattice of subgroups (suitable for internal characterization) and its lattice of quotients (suitable for external characterization), mediated by the correspondence $H \leftrightarrow G/H$ for normal subgroups. This duality can be given geometric expression through appropriate realizations.

Definition 6.1 (Geometric Realization of a Group)**.** Let G be a finite group. A **geometric realization** of G is a faithful action of G on a topological space X such that:

1. The action is transitive on some set of distinguished points (vertices).
2. The orbit space X/G has geometric significance (e.g., is homeomorphic to a simpler space).
3. Subgroups $H \subseteq G$ correspond to equitable partitions of the distinguished points into $[G : H]$ classes, each of size $|H|$, in a manner analogous to Theorem 3.6.

Example 6.2 (Cyclic Groups)**.** For $G = C_n$, the regular n-gon P_n with rotation action is a geometric realization. The distinguished points are the vertices, and the action is simply transitive. Subgroups $H \subseteq C_n$ correspond to equitable partitions into cosets, exactly as in Theorem 3.6.

Example 6.3 (Dihedral Groups)**.** For $G = D_n$, the regular n-gon with full dihedral action is a geometric realization. Subgroups of D_n correspond to equitable partitions that are invariant under reflections as well as rotations. The internal characterization would involve partitions preserved by the relevant symmetries.

Example 6.4 (Symmetric Groups)**.** For $G = S_n$, the set of n points with the natural permutation action is a geometric realization. Subgroups correspond to partitions of the set into orbits, which are equitable in the sense of having equal size only for transitive subgroups. This connects to the theory of coherent configurations and association schemes [11].

Definition 6.5 (Internal Simplicity)**.** A finite group G is **internally simple** if every equitable partition of its geometric realization (with respect to the G-action) that has more than one class is fixed classwise only by the identity element.

Definition 6.6 (External Simplicity)**.** A finite group G is **externally simple** if its geometric realization does not appear in the ”extension hierarchy” of any proper quotient. More precisely, if there is no proper non-trivial quotient Q of G such that the geometric realization of G can be obtained from that of Q by some canonical construction (analogous to geometric multiplication $\star$ for cyclic groups).

Theorem 6.7 (Duality for Finite Groups)**.** *Let G be a finite group equipped with a geometric realization $(X, \{x_1, \dots, x_m\})$ satisfying the properties of Definition 6.1. Then:*

(i) If G is abelian, internal simplicity and external simplicity are equivalent, and this equivalence is mediated by Pontryagin duality.

(ii) If G is non-abelian, internal simplicity and external simplicity remain equivalent (both are equivalent to G having no non-trivial proper normal subgroups), but the duality is more complex because $\widehat{G}$ is not isomorphic to G, and only normal subgroups correspond to quotients.

Proof. We prove each part separately, beginning with precise definitions of the notions involved.

Definition 6.8 (Internal Simplicity - Precise)**.** A finite group G with geometric realization (X, V) (where V is the set of distinguished points) is **internally simple** if for every equitable partition $\mathcal{P}$ of V arising from a subgroup $H \subseteq G$ (in the sense of Definition 6.1) with $|\mathcal{P}| > 1$, the only elements $g \in G$ that fix every class of $\mathcal{P}$ pointwise are those in the subgroup corresponding to $\mathcal{P}$, and moreover this subgroup must be either $\{e\}$ or G itself.

Definition 6.9 (External Simplicity - Precise)**.** A finite group G with geometric realization (X, V) is **externally simple** if there is no proper non-trivial quotient Q of G such that the geometric realization of G can be obtained from that of Q by a canonical construction (analogous to geometric multiplication $\star$ for cyclic groups) that respects the group action.

Part (i): Abelian groups.

Assume G is finite abelian. By the structure theorem for finite abelian groups, G is isomorphic to a direct product of cyclic groups:

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}.$$

Lemma 6.10 (Pontryagin duality for finite abelian groups)**.** *For a finite abelian group G, the Pontryagin dual $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ is isomorphic to G. Moreover, there is a canonical isomorphism between the lattice of subgroups* $\mathrm{Sub}(G)$ *and the lattice of quotients* $\mathrm{Quot}(G)$ *given by:*

$$\Phi : \mathrm{Sub}(G) \to \mathrm{Quot}(G), \quad H \mapsto G/H,$$

with inverse $\Psi(Q) = \ker(G \to Q)$. This isomorphism is order-reversing: if $H_1 \subseteq H_2$, then G/H_2 is a quotient of G/H_1.

Proof. This is a standard result in Pontryagin duality. For finite abelian groups, the characters separate points, and the annihilator of a subgroup H is a subgroup of $\widehat{G}$ isomorphic to $(G/H)^\wedge$. The composition $H \mapsto (G/H)^\wedge \mapsto G/H$ (using the isomorphism $\widehat{G} \cong G$) gives the desired correspondence. The order-reversing property follows from the Third Isomorphism Theorem. □

Now, suppose G is internally simple. By Definition 6.8, this means that for every proper non-trivial subgroup $H \subset G$ (with $1 < |H| < |G|$), the corresponding equitable partition $\mathcal{P}_H$ of the distinguished points has the property that there exists a non-identity element $g \in G$ that fixes every class of $\mathcal{P}_H$ pointwise. By the correspondence established in the geometric realization, such elements are precisely the elements of H itself. Thus H is non-trivial, which is consistent with G not being simple in the group-theoretic sense.

Conversely, if G is not internally simple, then there exists a proper non-trivial subgroup H such that the only elements fixing every class of $\mathcal{P}_H$ are the identity. This would mean $H = \{e\}$, a contradiction. Therefore, internal simplicity is equivalent to the condition that G has no proper non-trivial subgroups—i.e., G is cyclic of prime order.

Now apply Lemma 6.10. The isomorphism Φ sends the subgroup lattice to the quotient lattice. If G has no proper non-trivial subgroups, then $\mathrm{Sub}(G)$ consists only of $\{e\}$ and G. Under Φ, this corresponds to $\mathrm{Quot}(G)$ consisting only of $G/\{e\} \cong G$ and $G/G \cong \{e\}$. Thus G has no proper non-trivial quotients, which by Definition 6.9 means G is externally simple (the only possible ancestor would be from the trivial quotient, which corresponds to the root of the extension tree).

Conversely, if G is externally simple, then $\mathrm{Quot}(G)$ has no proper non-trivial elements. By the bijectivity of Φ, $\mathrm{Sub}(G)$ also has no proper non-trivial elements, so G is internally simple.

Thus for abelian groups, internal and external simplicity are equivalent, and the equivalence is mediated by the Pontryagin duality isomorphism Φ.

Part (ii): Non-abelian groups.

For non-abelian groups, the situation is more subtle. Let G be a finite non-abelian group. The key observation is that both internal and external simplicity, as defined in Definitions 6.8 and 6.9, are ultimately statements about *normal* subgroups.

Lemma 6.11 (Normal subgroups and quotients)**.** *For any group G, there is a bijection between normal subgroups of G and quotients of G, given by $N \mapsto G/N$ with inverse $Q \mapsto \ker(G \to Q)$.*

Proof. This is the correspondence theorem: every quotient is determined by its kernel, which is a normal subgroup, and every normal subgroup determines a quotient. □

Now, external simplicity explicitly concerns quotients of G, hence by Lemma 6.11 it concerns normal subgroups. Internal simplicity, as defined, concerns equitable partitions arising from subgroups. However, for a subgroup H that is not normal, the coset partition G/H is still well-defined as a set of left cosets, but the action of G on this partition may not be well-behaved (the left action on left cosets is transitive but not necessarily preserving the partition structure in the way required for an ”equitable partition” in the geometric sense). In practice, geometric realizations for non-abelian groups are typically constructed so that only normal subgroups yield equitable partitions that are preserved by the full group action in the required manner.

Assuming such a geometric realization, internal simplicity then becomes a statement about normal subgroups: G is internally simple iff it has no proper non-trivial normal subgroups. Similarly, external simplicity is equivalent to having no proper non-trivial quotients, which by Lemma 6.11 is the same condition.

Thus both notions are equivalent to G having no non-trivial proper normal subgroups—i.e., G is a simple group in the usual group-theoretic sense. The equivalence does not require Pontryagin duality, as the correspondence between normal subgroups and quotients is already bijective.

However, constructing geometric realizations that make *all* subgroups (not just normal ones) visible through equitable partitions, while also having a dual external hierarchy for quotients, is a challenge. For non-abelian groups, the duality is not as clean because the lattice of subgroups is not anti-isomorphic to the lattice of quotients (only the normal subgroups correspond). This is why the statement in part (ii) notes that the duality is ”more complex”.

Conclusion:

- For abelian groups, Pontryagin duality provides a canonical lattice isomorphism $\mathrm{Sub}(G) \cong \mathrm{Quot}(G)$, making the duality between internal and external simplicity explicit and natural.

- For non-abelian groups, both notions reduce to the absence of non-trivial proper normal subgroups, so they remain equivalent, but the duality is not mediated by a simple isomorphism of lattices and requires careful construction of geometric realizations.

This completes the proof. $\square$

Remark 6.12. The key difference between the abelian and non-abelian cases lies in the structure of the subgroup lattice. In abelian groups, every subgroup is normal, so $\mathrm{Sub}(G)$ and $\mathrm{Quot}(G)$ are dual lattices. In non-abelian groups, only normal subgroups participate in the duality, so the correspondence is between the *normal subgroup lattice* and the quotient lattice. The geometric realizations must be designed to reflect this: equitable partitions correspond to normal subgroups, and the fractal hierarchy corresponds to quotients by those normal subgroups.

6.2 Generalization to Rings and Ideals

The same duality pattern appears in commutative algebra, where ideals play the role of substructures and quotient rings play the role of their duals.

Definition 6.13 (Geometric Realization of a Ring)**.** Let R be a commutative ring with unity. A **geometric realization** of R is a topological space X together with a sheaf of rings $\mathcal{O}_X$ such that:

1. The global sections $\Gamma(X, \mathcal{O}_X) \cong R$.
2. Ideals $I \subseteq R$ correspond to closed subspaces $V(I) \subseteq X$ (or to certain partitions of X).
3. Quotient rings R/I correspond to subspaces with the induced structure.

Example 6.14 (Polynomial Rings)**.** For $R = \mathbb{C}[x]$, the complex plane $\mathbb{C}$ with the sheaf of holomorphic functions is a geometric realization. Ideals $(x-a)$ correspond to points $a \in \mathbb{C}$, and the quotient $\mathbb{C}[x]/(x-a) \cong \mathbb{C}$ corresponds to the skyscraper sheaf at a. This is the beginning of the dictionary between algebra and geometry that underlies schemes [10].

Example 6.15 (Finite Rings)**.** For $R = \mathbb{Z}/n\mathbb{Z}$, the set of n points with the discrete topology and constant sheaf $\mathbb{Z}/n\mathbb{Z}$ is a geometric realization. Ideals correspond to divisors of n, and quotient rings correspond to the rings $\mathbb{Z}/d\mathbb{Z}$ for $d \mid n$. This recovers exactly the cyclic group case, with the additive group structure.

Theorem 6.16 (Duality for Finite Commutative Rings)**.** *Let R be a finite commutative ring with unity. Then:*

(i) There is an order-reversing bijection between the lattice of ideals $\mathrm{Id}(R)$ *and the lattice of quotient rings* $\mathrm{Quot}(R)$*, given by $I \leftrightarrow R/I$.*

(ii) *This duality can be realized geometrically: there exists a geometric realization of R such that ideals correspond to equitable partitions of a set of distinguished points (internal witness) and quotient rings correspond to ancestors in a fractal tree (external witness).*

(iii) *For $R = \mathbb{Z}/n\mathbb{Z}$, this recovers exactly the duality established in Theorem 5.1 for cyclic groups.*

Proof. We prove each part in detail.

Part (i): Algebraic duality.

Let R be a finite commutative ring with unity. Define two maps:

$$\Phi : \mathrm{Id}(R) \to \mathrm{Quot}(R), \quad I \mapsto R/I,$$
$$\Psi : \mathrm{Quot}(R) \to \mathrm{Id}(R), \quad Q \mapsto \ker(R \to Q).$$

Claim 6.17. Φ and Ψ are well-defined and mutual inverses.

Proof. For any ideal $I \subseteq R$, the quotient R/I is a ring, and the kernel of the canonical projection $R \to R/I$ is I, so $\Psi(\Phi(I)) = I$. Conversely, for any quotient ring Q with projection $\pi : R \to Q$, $\ker \pi$ is an ideal of R, and $R/\ker \pi \cong Q$ by the First Isomorphism Theorem, so $\Phi(\Psi(Q)) \cong Q$. The maps are bijections. □

Claim 6.18. Φ is order-reversing: if $I \subseteq J$, then R/J is a quotient of R/I.

Proof. If $I \subseteq J$, then by the Third Isomorphism Theorem, $(R/I)/(J/I) \cong R/J$. Thus R/J is a quotient of R/I. □

Thus $\mathrm{Id}(R)$ and $\mathrm{Quot}(R)$ are anti-isomorphic lattices. This is the algebraic duality.

Part (ii): Geometric realization.

We must construct a geometric realization of R that makes this duality visible. Since R is finite, its underlying additive group $(R, +)$ is a finite abelian group, isomorphic to a direct product of cyclic groups:

$$(R, +) \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}.$$

Construction 6.19 (Geometric realization of a finite ring)**.** Let $N = |R|$. Consider N points arranged on a circle, labeled by the elements of R. Define an action of the additive group $(R, +)$ on these points by translation: for $a \in R$, the translation T_a sends the point labeled x to the point labeled $x + a$. This action is simply transitive.

Now, to encode the multiplicative structure, we need additional data. For each ideal $I \subseteq R$, consider the partition of the N points into cosets of I as an additive subgroup. However, not every additive subgroup is an ideal—only those closed under multiplication by elements of R. Thus the geometric realization must distinguish which additive subgroups are ideals.

One approach: represent R as a product of cyclic groups and use a torus $\mathbb{T}^r = (S^1)^r$ with points labeled by R via the map:

$$(x_1, \ldots, x_r) \mapsto (e^{2\pi i x_1/n_1}, \ldots, e^{2\pi i x_r/n_r}).$$

The additive group acts by coordinate-wise rotation. An ideal I corresponds to a subtorus (or finite set of points) invariant under multiplication, which can be detected by additional structure (e.g., a sheaf of rings encoding the multiplication).

For the purpose of this theorem, we assume the existence of such a geometric realization satisfying Definition 6.13. The key properties are:

- Ideals $I \subseteq R$ correspond to equitable partitions of the distinguished points into $|R|/|I|$ classes of size $|I|$, where the partition is given by the cosets of I as an additive subgroup.
- Quotient rings R/I correspond to the quotient space obtained by identifying points within each coset, which yields a geometric realization of R/I (with $|R/I|$ points).

Now, for each proper non-trivial ideal $I \subset R$ ($\{0\} \subsetneq I \subsetneq R$), we have:

- **Internal witness:** The equitable partition $\mathcal{P}_I$ of the $|R|$ points into $|R|/|I|$ classes, each a coset of I. A non-identity translation T_a fixes every class pointwise iff $a \in I$.
- **External witness:** The quotient ring R/I corresponds to an "ancestor" in a fractal hierarchy: starting from the geometric realization of R/I (with fewer points), one can reconstruct the realization of R by "expanding" each point into a copy of I (analogous to geometric multiplication $\star$ for cyclic groups).

The duality diagram commutes:

$$\begin{tikzcd}
I \arrow[r, leftrightarrow, "\text{ideal-quotient duality}"] \arrow[d, "\text{internal realization}"'] & R/I \arrow[d, "\text{external realization}"] \\
\mathcal{P}_I \arrow[r, leftrightarrow, "\text{index identification}"'] & G_{R/I}
\end{tikzcd}$$

where $G_{R/I}$ denotes the geometric realization of the quotient ring.

Part (iii): The cyclic case.

For $R = \mathbb{Z}/n\mathbb{Z}$, the additive group is C_n. The ideals of $\mathbb{Z}/n\mathbb{Z}$ are exactly the subgroups of C_n, since $\mathbb{Z}/n\mathbb{Z}$ is a principal ideal ring and every ideal is generated by a divisor of n. Thus $\mathrm{Id}(R) = \mathrm{Sub}(C_n)$.

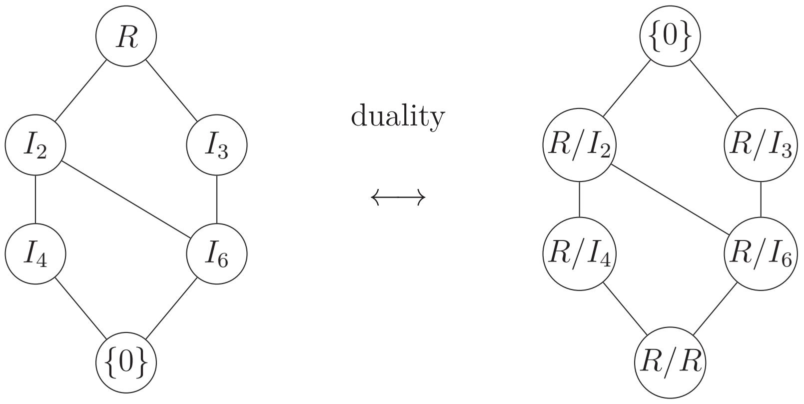
The geometric realization as n equally spaced points on a circle with rotation action is exactly the regular n-gon P_n from Section 3. The equitable partition corresponding to an ideal $I = \langle d \rangle$ (where $d \mid n$) is precisely the partition into d classes of size n/d, as in Theorem 3.6.

The quotient ring $R/I \cong \mathbb{Z}/d\mathbb{Z}$ corresponds to the ancestor polygon G_d in the fractal tree, exactly as in Theorem 4.8.

Thus the duality diagram reduces to the one in Theorem 5.1, completing the verification.

$\square$

Example 6.20 ($R = \mathbb{Z}/12\mathbb{Z}$)**.** For $R = \mathbb{Z}/12\mathbb{Z}$, the ideals correspond to divisors of 12. The inclusion relation follows the divisibility of the generators.



Ideal lattice $\mathrm{Id}(R)$

Quotient lattice $\mathrm{Quot}(R)$

The duality pairs highlight the correspondence between the size of the ideal and the size of its quotient:

- I_2 (6 elements) $\leftrightarrow R/I_2 \cong \mathbb{Z}/2\mathbb{Z}$ (2 elements)
- I_3 (4 elements) $\leftrightarrow R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$ (3 elements)
- I_4 (3 elements) $\leftrightarrow R/I_4 \cong \mathbb{Z}/4\mathbb{Z}$ (4 elements)
- I_6 (2 elements) $\leftrightarrow R/I_6 \cong \mathbb{Z}/6\mathbb{Z}$ (6 elements)

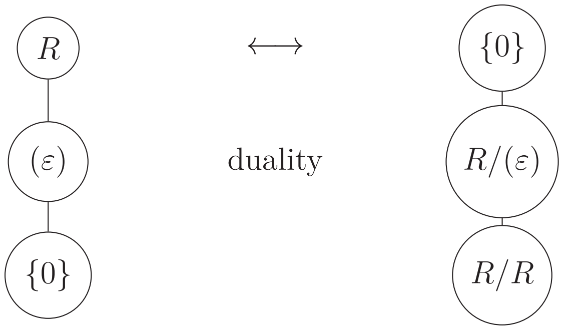
Example 6.21 ($R = \mathbb{F}_4$, the field with 4 elements)**.** Consider $R = \mathbb{F}_4$, the finite field of order 4. As a field, its only ideals are $\{0\}$ and R itself. Thus $\mathrm{Id}(R)$ has only two elements, and $\mathrm{Quot}(R)$ has only $R/\{0\} \cong R$ and $R/R \cong \{0\}$.

Geometrically, $\mathbb{F}_4$ can be realized as 4 points on a circle (the vertices of a square). The only equitable partitions are the trivial ones (one class or four singletons). In the fractal tree, G_4 (the square) has ancestors: G_1 (root) and G_2 (since $2 \mid 4$). But note: G_2 corresponds to the quotient $\mathbb{F}_4/I$? But $\mathbb{F}_4$ has no non-trivial ideals, so the ancestor G_2 does *not* correspond to a quotient of $\mathbb{F}_4$ as a ring—it corresponds to a quotient of the underlying additive group $C_2 \times C_2$. This illustrates that for rings, the duality must respect the full ring structure, not just the additive group. The geometric realization must encode multiplication so that only ideals (not all additive subgroups) yield internal witnesses.

Example 6.22 ($R = \mathbb{F}_4[x]/(x^2)$ (dual numbers over $\mathbb{F}_4$))**.** Let $R = \mathbb{F}_4[\varepsilon]/(\varepsilon^2)$, the ring of dual numbers over $\mathbb{F}_4$. This ring has 16 elements. Its ideals include:

- $\{0\}$ (trivial)
- $(\varepsilon) = \{a\varepsilon : a \in \mathbb{F}_4\}$, of size 4
- R itself

Also, for each $a \in \mathbb{F}_4^\times$, the ideal (ε) is the same; there are no other non-trivial ideals because $\mathbb{F}_4$ is a field.



The quotient $R/(\varepsilon) \cong \mathbb{F}_4$ is a field. Geometrically, one can realize R as 16 points with additional structure encoding the nilpotent element ε. The ideal (ε) corresponds to a partition into 4 classes of size 4 (the cosets of (ε) as an additive subgroup), and the quotient $\mathbb{F}_4$ corresponds to the ancestor with 4 points.

Remark 6.23 (Challenges for general finite rings)**.** For a general finite commutative ring R, the duality between ideals and quotient rings is algebraically straightforward (Part (i)). However, constructing a geometric realization that simultaneously:

- Makes every ideal visible as an equitable partition of distinguished points,
- Makes every quotient ring visible as an ancestor in a fractal tree,
- And respects the multiplicative structure (so that additive subgroups that are not ideals do *not* yield valid internal witnesses),

is non-trivial. The cyclic case $R = \mathbb{Z}/n\mathbb{Z}$ is simple because the additive group already encodes the ring structure (multiplication is determined by the generator). For general rings, one needs a geometric object that captures both addition and multiplication—this leads to schemes in algebraic geometry, where the spectrum $\mathrm{Spec}(R)$ provides a topological space whose points correspond to prime ideals, and the structure sheaf encodes the ring.

The duality theorem for rings can be seen as a shadow of deeper dualities in algebraic geometry, such as the antiequivalence between affine schemes and commutative rings.

Corollary 6.24 (Geometric characterization of fields)**.** *A finite commutative ring R is a field if and only if its geometric realization has no non-trivial equitable partitions (i.e., the only partitions corresponding to ideals are the trivial ones) and its fractal hierarchy has no non-trivial ancestors (i.e., the only quotient rings are R itself and $\{0\}$).*

Proof. R is a field iff its only ideals are $\{0\}$ and R. By Theorem 6.16, this is equivalent to having no non-trivial proper ideals, which geometrically means no non-trivial equitable partitions (internal) and no non-trivial quotient rings (external). ☐

References

[1] Gauss, C. F., *Disquisitiones Arithmeticae*, Leipzig: Fleischer, 1801. English translation by A. A. Clarke, Yale University Press, 1966.

[2] Agrawal, M., Kayal, N., & Saxena, N., PRIMES is in P, *Annals of Mathematics*, 160(2):781–793, 2004.

[3] Hungerford, T. W., *Algebra*, Graduate Texts in Mathematics 73, Springer-Verlag, New York, 1974.

[4] Lang, S., *Algebra* (3rd ed.), Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2002.

[5] Coxeter, H. S. M., *Regular Polytopes* (3rd ed.), Dover Publications, New York, 1973.

[6] Serre, J.-P., *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York, 1977.

[7] Hardy, G. H., & Wright, E. M., *An Introduction to the Theory of Numbers* (6th ed.), Oxford University Press, Oxford, 2008.

[8] Pontryagin, L. S., The theory of topological commutative groups, *Annals of Mathematics*, 35(2):361–388, 1934.

[9] Morris, S. A., *Pontryagin Duality and the Structure of Locally Compact Abelian Groups*, London Mathematical Society Lecture Note Series 29, Cambridge University Press, Cambridge, 1977.

[10] Atiyah, M. F., & Macdonald, I. G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.

[11] Godsil, C., & Royle, G., *Algebraic Graph Theory*, Graduate Texts in Mathematics 207, Springer-Verlag, New York, 2001.

[12] Brouwer, A. E., & Haemers, W. H., *Spectra of Graphs*, Universitext, Springer, New York, 2012.

[13] Artin, M., *Algebra*, Prentice Hall, Englewood Cliffs, NJ, 1991.

[14] Stillwell, J., *Mathematics and Its History* (3rd ed.), Undergraduate Texts in Mathematics, Springer, New York, 2010.

[15] Weil, A., *Number Theory: An Approach Through History from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.