The Klein Four-Group

PMA3013 - Solo Investigations

Author(s)

Matteo Melis - 40324932

2025-04-22

Contents

1 Introduction

The Klein four-group V_4, named after the German mathematician Felix Klein, is the smallest non-cyclic group. It provides a fundamental example in group theory. This project investigates V_4 beyond its basic properties, exploring its realisations within modular arithmetic and its role in polynomial solvability. We first characterise the existence and enumerate the occurrences of V_4 subgroups within the unit group $\mathbb{Z}_n^*$, utilising the Chinese Remainder Theorem. We then extend this analysis to the full multiplicative semigroup $(\mathbb{Z}_n, \times)$, demonstrating a lifting technique to construct V_4 embeddings, even among non-units. Finally, we connect these structural insights to Galois Theory, highlighting how V_4's unique status as a normal subgroup of A_4 underpins the solvability of quartic equations and the contrasting impossibility for degree five and higher, as established by the Abel-Ruffini theorem.

The paper assumes the reader to have a foundational knowledge of group theory. Such knowledge can be obtained through initial chapters of 'Abstract Algebra' by Dummit and Foote [1] or similar.

2 Properties of the Klein Four-Group

Definition 2.1. The **Klein four-group**, often denoted V_4, is the abelian group of order 4:

$$V_4 = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle = \{e, a, b, ab\}, \tag{1}$$

where e is the identity element.

Remark 2.2. The above definition states that the Klein four-group is generated by two non-identity elements, meaning it is not cyclic. It can be shown quite trivially that Klein four-group is in fact the smallest non-cyclic abelian group - we will prove this later in the section.

Let us explore some standard numerical constructions of the Klein four-group over the integers and different moduli.

Example 2.3. Let $G = \mathbb{Z}_8^* = \{1, 3, 5, 7\}$. G is of course abelian since it is the group of units of a commutative ring; now notice that each element of G is its own inverse:

$$\begin{aligned} 3^2 = 9 &\equiv 1 \pmod 8, \\ 5^2 = 25 &\equiv 1 \pmod 8, \\ 7^2 = 49 &\equiv 1 \pmod 8. \end{aligned}$$

Additionally, notice that the product of any two non-identity elements generates the third non-identity element:

$$\begin{aligned} 3 \cdot 5 = 15 &\equiv 7 \pmod 8, \\ 5 \cdot 7 = 35 &\equiv 3 \pmod 8, \\ 3 \cdot 7 = 21 &\equiv 5 \pmod 8. \end{aligned}$$

Altogether we have that $G = \mathbb{Z}_8^* = \{1, 3, 5, 7\} \cong V_4$.

Example 2.4. Consider the group of units modulo 24, $\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$. Notice once again that each element has order 2, or equivalently, each element is its own inverse. Additionally, taking any two non-identity elements will generate a third non-identity element. Taking a pair of non-identity elements we find:

$$V_4 \cong \langle 5, 19 \rangle = \{1, 5, 19, 23\} \leq \mathbb{Z}_{24}^*$$

Similar checks for other pairs of non-identity elements confirm that they also generate subgroups isomorphic to V_4.

The previous examples leave the reader with several questions regarding the existence of such groups: 'For what values of n does $\mathbb{Z}_n^*$ contain a construction of V_4?', 'How many such constructions exist for each n?', 'Are there constructions outside of the group of units?'. We will work towards answering all of these questions in the coming sections.

First consider the below example to showcase that numerical constructions of V_4 can exist outside of $\mathbb{Z}_n^*$.

Example 2.5. Consider again the integers modulo 24 where we saw previously that $\mathbb{Z}_{24}^*$ contains several constructions of the Klein four-group. However, let $G = \{3, 9, 15, 21\}$ under multiplication modulo 24 and notice that none of these elements are elements of the group of units modulo 24. This can be easily verified to form a group with 9 serving as the identity. Additionally, notice that

$$\begin{aligned} 3^2 = 9 &\equiv 9 \pmod{24}, \\ 15^2 = 225 &\equiv 9 \pmod{24}, \\ 21^2 = 441 &\equiv 9 \pmod{24}. \end{aligned}$$

As mentioned, 9 serves as the identity element since $9 \cdot 3 = 3$, $9 \cdot 15 = 15$ and $9 \cdot 21 = 21$. Additionally, since this is a group, it is closed under its operation and hence taking the product of any two non-identity elements will generate the third non-identity element trivially. Altogether we have:

$$V_4 \cong G \cong \{3, 9, 15, 21\} \pmod{24}$$

Remark 2.6. This confirms there can exist additional numerical constructions of the Klein four-group outside of the group of units for a given modulo system. We will explore this in more detail in the coming sections.

Let us now take a closer look at some of the properties of the Klein four-group.

Lemma 2.7. Any group of order 4 is abelian.

Proof. Consider a group G of order 4. Suppose, towards a contradiction, that G is not abelian. Then there must exist some distinct non-identity elements $a, b \in G$ such that $ab \neq ba$. But notice that:

- $ab \neq e$ and $ba \neq e$ (since a and b don't commute, so $b \neq a^{-1}$)
- $ab \neq a$ and $ba \neq a$ (since by hypothesis $b \neq e$)
- $ab \neq b$ and $ba \neq b$ (since by hypothesis $a \neq e$)

Thus, it follows that e, a, b, ab, ba are 5 distinct elements that are all in G. But this contradicts the fact that G is of order 4. Thus, G must be abelian, as desired. □

Lemma 2.8. There are exactly two groups of order 4 up to isomorphism: $C_2 \times C_2$ and C_4.

Proof. Let G be any group such that $|G| = 4$. By Lagrange's theorem we know that for any $g \in G$ the order of g must divide 4. Since any element of order 1 is the identity element, we have two distinct cases for the non-identity elements of G:

1. G has an element g of order 4.
2. Otherwise, G has no element of order 4 meaning all non-identity elements have order 2.

In first case we can see trivially that $G = \langle g \rangle \cong C_4$. In the second case, let $G = \{e, a, b, c\}$. Since G is abelian by Lemma 2.7, $ab = c$ and $a^2 = b^2 = c^2 = e$. Altogether, a quick verification of Cayley tables confirms that G matches the structure of $C_2 \times C_2$. Thus, $G \cong C_2 \times C_2$. □

Proposition 2.9. The Klein four-group is isomorphic to $C_2 \times C_2$.

Proof. This is direct result of Lemma 2.8 since all non-identity elements of V_4 have order 2. □

Lemma 2.10. The Klein four-group is the smallest non-cyclic abelian group.

Proof. From Proposition 2.9 we know $V_4 \cong C_2 \times C_2$. We also know from Lemma 2.8 that no other group of order 4 is non-cyclic. Since any group of order less than 4 is either trivial (and thus cyclic) or has prime order (cyclic by Lagrange's Theorem), we are done. □

3 Existence of V_4 constructions in $\mathbb{Z}_n^*$

This section aims to get a concrete answer to the following question: For what values of n does there exist a multiplicative subgroup of $\mathbb{Z}_n$ that is isomorphic to the Klein four group?

To address this problem, we leverage the fact that the Klein four-group V_4 is generated by two elements, each having order 2. Thus, it is necessary to verify that in each modular system there exist two elements of order 2. A logical starting point is to restrict our search to the unit group. Since every non-identity element $a \in V_4$ satisfies $a^2 = e$, meaning these elements must be invertible.

Definition 3.1. The **Euler totient function** $\phi(n)$ is defined by

$$\phi(n) =\mid \mathbb{Z}_n^* \mid = \#\{x \in \mathbb{Z} : 0 \leq x < n, \gcd(x, n) = 1\} \tag{2}$$

Example 3.2. Let $n = 2^k$, then $\gcd(x, n) = 1$ if and only if x is odd, so

$$\phi(n) = 2^k/2 = 2^{k-1}. \tag{3}$$

Example 3.3. Let $n = p^k$ with p an odd prime and $k \in \mathbb{N}$. Then for any $x \in \mathbb{Z}_n$ we have $\gcd(x, n) = 1$ if and only if x is not a multiple of p. There are precisely p^{k-1} multiples of p (namely $1p, 2p, \ldots, p^{k-1}p$), hence

$$\phi(n) = p^k - p^{k-1} = p^{k-1}(p-1). \tag{4}$$

The above examples illustrate fundamental results in number theory. We can now wish to build on these utilities and work towards determining how many units exist in $\mathbb{Z}_n$, for any $n \in \mathbb{N}$ in a quick fashion.

Theorem 3.4 (Chinese Remainder Theorem for $\mathbb{Z}$)**.** Let $m_1, \ldots, m_k$ be pairwise coprime positive integers and let $m = m_1 \cdot m_2 \cdot \cdots \cdot m_k$. Then

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}. \tag{5}$$

Moreover, the map $\psi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, defined by

$$\psi(x) = \big(x \bmod m_1,\ \ x \bmod m_2,\ \ \ldots,\ \ x \bmod m_k\big), \tag{6}$$

induces a ring isomorphism.

Proof. First, ψ is well-defined, because if $x \equiv y \pmod m$ then $m \mid (x-y)$, so in particular $m_i \mid (x-y)$ for each i. Hence $x \equiv y \pmod{m_i}$ for each i. The map ψ is clearly a homomorphism since $\psi(1) = (1, \ldots, 1)$ and ψ respects the ring operations by definition of the product and quotient rings. Suppose $\psi(x) = 0$. then $m_1, \ldots, m_k \mid x$, so by co-primality $m \mid x$, that is, $x \equiv 0 \pmod m$. Thus ψ is injective. Since the domain and range both have order m it follows that ψ is bijective, hence an isomorphism. □

We now extend this to work over the group of units.

Lemma 3.5. Let $n = p_1^{k_1} \cdots p_t^{k_t}$ be the prime factorisation of n. Then

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{k_t}}^*. \tag{7}$$

Proof. By Chinese Remainder Theorem, we have that

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_t^{k_t}}.$$

Now, we use the fact that if R and S are rings then $(x, y) \in R \times S$ is a unit if and only if both x and y are units, that is, $(R \times S)^* = R^* \times S^*$. Putting this together, we induce the following group isomorphism

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{k_t}}^*,$$

as required. □

Proposition 3.6. Suppose $n = p_1^{k_1} \cdots p_t^{k_t}$ is the prime factorisation of n. Then

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1). \tag{8}$$

Proof. Since $p_1^{k_1}, \ldots, p_t^{k_t}$ are pairwise coprime, by the previous lemma we have

$$\phi(n) = \prod_{i=1}^{t} \phi\big(p_i^{k_i}\big). \tag{9}$$

Hence, it suffices to recall from Example 3.3 that $\phi\big(p_i^{k_i}\big) = p_i^{k_i - 1}(p_i - 1)$. Proving the formula. □

This gives us the ability to quickly calculate the totient function of any group of units. Let's explore an example of such a calculation.

Example 3.7. Consider the ring of integers modulo 800,

$$\phi(800) = \phi(2^5)\phi(5^2) = (2^4 \cdot 1)(5^1 \cdot 4) = (16)(20) = 320.$$

Hence $|Z^*_{800}| = 320$.

We now wish to leverage the above results to work towards a final proof of our main question: For what values of n does there exist a multiplicative subgroup of $\mathbb{Z}_n$ that is isomorphic to the Klein four group?

Remark 3.8. Before we begin, an important result from group theory tells us that any cyclic group G of even order contains only one element of order 2.

Proof. Let G be a cyclic group of order n, where n is even. Then $n = 2k$ for some integer k, and we can write $G = \langle g \rangle$ for some generator $g \in G$.

By Lagrange's Theorem, the order of any element of G divides the order of the group, so all element orders divide n. In particular, since $2 \mid n$, there exists at least one element in G of order 2.

Recall a key fact about cyclic groups: for every divisor $d \mid n$, there are exactly $\varphi(d)$ elements of order d in G, where φ is Euler's totient function.

Since $2 \mid n$, there is exactly $\varphi(2) = 1$ element of order 2 in G.

Therefore, G has exactly one element of order 2. □

Intuitively, since we are looking for groups of units that contain at least two elements of order 2 - it makes sense to look at the cases where the group of units $\mathbb{Z}^*_n$ is cyclic, and rule these out immediately.

Lemma 3.9. If $k = 1$ or 2 then $\mathbb{Z}^*_{2^k}$ is a cyclic group of order 1 and 2 respectively. If $k \geq 3$, then $\mathbb{Z}^*_{2^k}$ is non-cyclic.

Proof. Firstly, it is easy to see that $\mathbb{Z}^*_2 = \{1\}$ the trivial cyclic group, and $C_2 \cong \mathbb{Z}^*_4$ since $\mathbb{Z}^*_4 = \{1, 3\}$ which is generated by 3 and has order 2.

Next, recall from our previous section that for $k = 3$, we have seen that the multiplicative group $\mathbb{Z}^*_8$ is isomorphic to the Klein four-group (i.e. non-cyclic). This serves as the base case, and we proceed by induction on k to show that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}, \tag{10}$$

for all odd numbers a, which implies that the order of any element in $\mathbb{Z}^*_{2^k}$ never attains the maximal possible value $|\mathbb{Z}^*_{2^k}| = \phi(2^k) = 2^{k-1}$ (Example 3.2) and therefore $\mathbb{Z}^*_{2^k}$ is not cyclic.

To justify the induction step, assume equation (10) holds for some k. Then there exists an integer m such that

$$a^{2^{k-2}} = 1 + m2^k.$$

Squaring both sides of this equality, we obtain

$$a^{2^{k-1}} = (1 + m2^k)^2 = 1 + m2^{k+1} + m^2 2^{2k} \equiv 1 \pmod{2^{k+1}}.$$

Thus, the induction step is justified, and it follows that $\mathbb{Z}^*_{2^k}$ remains non-cyclic for all $k \geq 3$. □

Proposition 3.10. If $k \geq 3$, then $\mathbb{Z}_{2^k}^* \cong C_2 \times C_{2^{k-2}}$. Moreover, there exists a multiplicative subgroup $S \leq \mathbb{Z}_{2^k}^*$ such that $S \cong V_4$.

Proof. Let $G = \mathbb{Z}_{2^k}^*$, where $k \geq 3$. We recall from Lemma 3.9 that $|G| = \phi(2^k) = 2^{k-1}$ and that G is non-cyclic.

Next, we define the natural homomorphism $\psi : G \to \mathbb{Z}_4^*$, which sends an element $a \in G$ to its residue modulo 4. Since $\mathbb{Z}_4^* = \{1, 3\}$ is a cyclic group of order 2 and ψ is clearly surjective, we have $|\psi(G)| = 2$. By the First Isomorphism Theorem, the kernel

$$K = \ker \psi = \{a \in G \mid a \equiv 1 \pmod 4\}$$

satisfies

$$|K| = \frac{|G|}{|\psi(G)|} = \frac{2^{k-1}}{2} = 2^{k-2}.$$

It is a standard result in elementary number theory that K is cyclic (see, for instance, an argument via binomial expansions that shows $(1+2)^{2^{k-2}} \equiv 1 \pmod{2^k}$ and that no smaller power does). Hence,

$$G \cong \psi(G) \times K \cong C_2 \times C_{2^{k-2}}.$$

Moreover, we can construct a subgroup $S \cong V_4$. Let a be the unique non-identity element of the first C_2 factor in the decomposition $G \cong C_2 \times C_{2^{k-2}}$. Let g_2 be a generator of the second factor $C_{2^{k-2}}$. The unique element of order 2 in this second factor is $b = g_2^{2^{k-3}}$. Since a and b correspond to elements in different factors of the direct product, they commute. The subgroup generated by these two distinct elements of order 2 is $S = \langle a, b \rangle = \{e, a, b, ab\}$, where e is the identity. Since $|S| = 4$ and all non-identity elements have order 2:

$$S \cong C_2 \times C_2 \cong V_4.$$

□

Lemma 3.11. If p is an odd prime and $k \in \mathbb{N}$, the group of units $\mathbb{Z}_{p^k}^*$ is cyclic.

Proof. (Sketch) It can be shown by induction on k that for an odd prime p, the element $p+1$ has multiplicative order p^{k-1} modulo p^k. Let $a = p+1$. We know that Z_p^* is cyclic, so it has a generator r whose order modulo p is $p-1$. Now consider r as an element in $Z_{p^k}^*$. Let $o = \text{ord}_{p^k}(r)$ be its order modulo p^k. Since $r^o \equiv 1 \pmod{p^k}$, it follows that $r^o \equiv 1 \pmod p$. Because $\text{ord}_p(r) = p-1$, we must have $(p-1)|o$. Since $(p-1)$ divides the order o of r in $Z_{p^k}^*$, the element $b = r^{o/(p-1)}$ has order exactly $p-1$ in $Z_{p^k}^*$. We are in the abelian group $Z_{p^k}^*$ and there exists an element $a = p+1$ of order p^{k-1} and an element $b = r^{o/(p-1)}$ of order $p-1$. Since p is prime, $\gcd(p^{k-1}, p-1) = 1$. Therefore, the product ab must have order $p^{k-1}(p-1) = \phi(p^k)$, which is the order of $Z_{p^k}^*$. Therefore, $Z_{p^k}^*$ must be cyclic. □

Remark 3.12. The above is a sketch of a proof that $\mathbb{Z}_{p^k}^*$, for p an odd prime and $k \in \mathbb{N}$, is cyclic. It leans on some properties of abelian groups and number theoretic results. This is an equivalent statement to a classic number theoretic result that says for p an odd prime and $k \in \mathbb{N}$, there exists primitive roots modulo p^k. For readers interested in viewing a more concrete proof to the above sketch, one can find such a proof in most elementary number theory books; for example Ireland and Rosen's: a Classical Introduction to Modern Number Theory. [2]

Theorem 3.13. $\mathbb{Z}_n^*$ is cyclic if and only if n is of the form 1, 2, 4, p^k, or $2p^k$, where p is an odd prime and $k \in \mathbb{N}$. Moreover, there exists at least one subgroup $S \leq \mathbb{Z}_n^*$ such that $S \cong V_4$ if and only if n is not of the described form.

Proof. We have shown previously through Lemma 3.9 and 3.11 that the forward implication holds true for $n = 2$, 4, p^k. It can be quickly verified for $n = 2p^k$ since $\mathbb{Z}_{2p^k}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{p^k}^* \cong \mathbb{Z}_{p^k}^*$. If $n = 1$ this is a classical result that the group of units of the integers is cyclic.

To see the converse, let n be some integer not of the specified form. We have already shown in Lemma 3.9 and Proposition 3.10 that the statement holds true for $n = 2^k$ with $k \geq 3$, so let us assume it does not take this form either. If n is not of any of the aforementioned forms, we have two possibilities:

1. n has at least two distinct odd prime factors $p_1^{k_1}, p_2^{k_2}$ with $k_i \geq 1$.
2. n has 2^{k_1} and at least one odd prime p^{k_2} with $k_1 \geq 2$ and $k_2 \geq 1$ in its prime factorisation.

Decomposing the group structure using the Chinese Remainder Theorem for both cases we have:

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \mathbb{Z}_{p_2^{k_2}}^* \times \cdots \tag{11}$$

or,

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{2^{k_1}}^* \times \mathbb{Z}_{p^{k_2}}^* \times \cdots \tag{12}$$

We have shown previously that $\mathbb{Z}_{p_i^{k_i}}^*$ is a cyclic group of even order containing exactly one element of order 2. Additionally, for $k = 2$ we know $\mathbb{Z}_{2^k}^*$ contains one element of order 2, and and for $k \geq 3$ we know $\mathbb{Z}_{2^k}^*$ contains three elements of order 2 (and thus contains a V_4 subgroup itself, see Prop. 3.10) Altogether, in either case, $\mathbb{Z}_n^*$ contains at least two commuting, distinct elements of order 2, meaning there exists $S \leq \mathbb{Z}_n^*$ such that $S \cong V_4$ as required. □

Example 3.14. Let $n = 50$. Giving the prime decomposition $n = 2 \cdot 5^2$. We know from Theorem 3.13 that $\mathbb{Z}_{50}^*$ will not contain a subgroup isomorphic to the Klein four-group. To see this explicitly, consider

$$\mathbb{Z}_{50}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{25}^* \cong C_1 \times C_4 \times C_5 \cong C_4 \times C_5.$$

Letting g_1 be the generators of C_4 we know $(g_1)^2$ is an element of order 2 in C_4, however, there is no such element in C_5. Meaning, we don't have two unique elements of order 2 and hence we cannot impose an embedding of the Klein four-group in $\mathbb{Z}_{50}^*$.

Example 3.15. Let $n = 70$. Giving the prime decomposition $n = 2 \cdot 5 \cdot 7$. In this case, n is not of the form 1, 2, 4, p^k or $2p^k$ and hence from Theorem 3.13 that $\mathbb{Z}_{70}^*$ must contain a subgroup isomorphic to the Klein four-group. We confirm this by the following

$$\mathbb{Z}_{70}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_5^* \times \mathbb{Z}_7^* \cong C_1 \times C_4 \times C_6 \cong C_4 \times C_6.$$

In a similar vein to our previous example, let g_1 and g_2 be the generators of C_4 and C_6 respectively. Then $(g_1)^2$ is an element of order 2 in C_4 and $(g_2)^3$ is an element of order 2 in C_6. Hence

$$V_4 \cong \langle (g_1)^2, (g_2)^3 \rangle = \{1, (g_1)^2, (g_2)^3, (g_1)^2(g_2)^3\} \leq \mathbb{Z}_{70}^* \tag{13}$$

4 How many V_4 constructions exist in $\mathbb{Z}_n^*$?

From the previous section we know for which values of n there exists a construction of the Klein four-group in $\mathbb{Z}_n^*$; we now move towards an analytical question of how many such constructions there are for each n.

Let the prime factorization of n be:

$$n = 2^k \prod_{i=1}^{r} p_i^{e_i} \tag{14}$$

where p_i are distinct odd primes, $k \geq 0$, $r \geq 0$, and where $e_i \geq 1$ for each i (if $r \geq 1$). By the Chinese Remainder Theorem, the group of units decomposes as:

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^* \tag{15}$$

The structure of these factors is known:

- For an odd prime p_i, the group $\mathbb{Z}_{p_i^{e_i}}^*$ is cyclic of order $\phi(p_i^{e_i}) = p_i^{e_i-1}(p_i-1)$. So, $\mathbb{Z}_{p_i^{e_i}}^* \cong C_{p_i^{e_i-1}(p_i-1)}$.
- The structure of $\mathbb{Z}_{2^k}^*$ depends on k:
  - If $k = 0$ or $k = 1$, $\mathbb{Z}_{2^k}^*$ is the trivial group $\{1\} \cong C_1$.
  - If $k = 2$, $\mathbb{Z}_4^* = \{1, 3\} \cong C_2$.
  - If $k \geq 3$, $\mathbb{Z}_{2^k}^* \cong C_2 \times C_{2^{k-2}}$.

Therefore, the full decomposition depends on the value of k. For instance, if $k \geq 3$:

$$\mathbb{Z}_n^* \cong (C_2 \times C_{2^{k-2}}) \times C_{p_1^{e_1-1}(p_1-1)} \times \cdots \times C_{p_r^{e_r-1}(p_r-1)} \tag{16}$$

The structure of the subgroup of elements of order 2 in $\mathbb{Z}_n^*$ determines the number of possible V_4 constructions. This structure is isomorphic to a direct product of cyclic groups of order 2, $(\mathbb{Z}/2\mathbb{Z})^s$. The value of s, representing the number of C_2 factors in this decomposition, depends on the prime factorization of n. Specifically, each distinct odd prime factor p_i contributes one C_2 factor. The contribution from the 2^k part depends on k: none for $k = 0, 1$, one for $k = 2$, and two for $k \geq 3$. Summing these contributions gives:

$$s := \begin{cases} r & \text{if } k = 0 \text{ or } k = 1 \\ r+1 & \text{if } k = 2 \\ r+2 & \text{if } k \geq 3 \end{cases} \tag{17}$$

The subgroup of elements of order 2 in $\mathbb{Z}_n^*$, let's call it $E = \{x \in \mathbb{Z}_n^* \mid x^2 = 1\}$, consists of the identity element and all elements whose order is exactly 2. Based on the structure derived from the decomposition (15) and the definition of s, this subgroup E is isomorphic to the direct product of s copies of the cyclic group of order 2:

$$E \cong C_2 \times \cdots \times C_2 = (\mathbb{Z}/2\mathbb{Z})^s.$$

This group can be viewed as an s-dimensional vector space over the field $\mathbb{F}_2$ which contains exactly 2^s elements.

One element in E is the identity element of $\mathbb{Z}_n^*$. The other $2^s - 1$ elements are the elements of order exactly 2. A subgroup isomorphic to the Klein four-group V_4 consists of the identity element and three distinct elements of order 2, say a, b, c, satisfying $c = ab$. Such a subgroup is uniquely determined by choosing any two distinct elements from the set $\{a, b, c\}$.

Therefore, to find the number of distinct V_4 subgroups, we first count the number of ways to choose an unordered pair of distinct elements of order 2 from the $2^s - 1$ available elements. This count is given by $\binom{2^s-1}{2}$. However, each specific V_4 subgroup $\{1, a, b, ab\}$ is generated by any pair chosen from its three non-identity elements (i.e. $V_4 \cong \langle a, b\rangle = \langle a, ab\rangle = \langle b, ab\rangle$). This means our initial count of pairs has counted each unique V_4 subgroup exactly 3 times. To get the true number of distinct subgroups isomorphic to V_4, we must divide this count by 3.

Definition 4.1. Let n be an integer whose prime factorisation is

$$n \;=\; 2^k \prod_{i=1}^{r} p_i^{e_i},$$

where p_i are distinct odd primes, $k \geq 0$, $r \geq 0$, and where $e_i \geq 1$ for each i (if $r \geq 1$). Let s be defined as:

$$s := \begin{cases} r & \text{if } k = 0 \text{ or } k = 1 \\ r + 1 & \text{if } k = 2 \\ r + 2 & \text{if } k \geq 3 \end{cases}$$

Then $\mathbb{Z}_n^*$ contains a subgroup isomorphic to the Klein four-group V_4 if and only if $s \geq 2$. In that case, the *number of distinct subgroups* of $\mathbb{Z}_n^*$ that are isomorphic to V_4 is given by

$$\frac{1}{3}\binom{2^s \;-\; 1}{\quad 2\quad} \;=\; \frac{\left(2^s - 1\right)\left(2^s - 2\right)}{6}.$$

Let's now verify the above formula with some examples. Consider our previous initial example over the integers modulo 8:

Example 4.2. Let $n = 8$. Computing the prime factorisation we have:

$$8 = 2^3,$$

here, $k = 3$ and there are no odd prime factors (so $r = 0$). Hence,

$$s = r + 2 = 2.$$

Hence, the number of V_4 subgroups is:

$$\#V_4 = \frac{(2^2 - 1)(2^2 - 2)}{6} = \frac{(4 - 1)(4 - 2)}{6} = \frac{3 \cdot 2}{6} = 1.$$

Thus, $\mathbb{Z}_8^*$ contains exactly one subgroup isomorphic to V_4. This aligns with our expectation since $\mathbb{Z}_8^*$ is itself isomorphic to the Klein four-group.

Example 4.3. Let $n = 60$. Computing the prime factorisation we have:

$$60 = 2^2 \cdot 3 \cdot 5,$$

here, $k = 2$ and we have two odd prime factors giving $r = 2$. Hence,

$$s = r + 1 = 2 + 1 = 3.$$

Hence, the number of V_4 subgroups in $\mathbb{Z}_n^*$:

$$\#V_4 = \frac{(2^3 - 1)(2^3 - 2)}{6} = \frac{(8 - 1)(8 - 2)}{6} = \frac{7 \cdot 6}{6} = 7.$$

Thus, $\mathbb{Z}_{60}^*$ contains exactly seven unique subgroups isomorphic to V_4. It is not difficult to verify this manually, let us consider the group of units modulo 60 which is given by

$$\mathbb{Z}_{60}^* = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}.$$

Moreover, the subgroup of elements of order two, is given by

$$S = \{a \in \mathbb{Z}_{60}^* : a^2 \equiv 1 \pmod{60}\} = \{1, 11, 19, 29, 31, 41, 49, 59\}.$$

the unique unordered V_4 constructions from this subgroup are:

- $\langle 11, 19\rangle = \{1, 11, 19, 29\} \cong V_4$
- $\langle 11, 31\rangle = \{1, 11, 31, 41\} \cong V_4$
- $\langle 11, 49\rangle = \{1, 11, 49, 59\} \cong V_4$
- $\langle 19, 31\rangle = \{1, 19, 31, 49\} \cong V_4$
- $\langle 19, 41\rangle = \{1, 19, 41, 59\} \cong V_4$
- $\langle 29, 31\rangle = \{1, 29, 31, 59\} \cong V_4$
- $\langle 29, 41\rangle = \{1, 29, 41, 49\} \cong V_4$

As expected we have 7 unique constructions of V_4.

5 Lifting V_4 Embeddings from $\mathbb{Z}_k^*$ to $\mathbb{Z}_n$

Up to now, we have restricted our search for constructing V_4 in $\mathbb{Z}_n$ to the group of units $\mathbb{Z}_n^*$, since every element there has an inverse and the group structure is readily available. Nevertheless, a construction of V_4 requires only that the group have a well-defined identity (which need not be 1) and every non-identity element of the group is self inverse. This observation enables us to extend our search to embeddings into the multiplicative semigroup $(\mathbb{Z}_n, \times)$, thereby considering images that need not lie in $\mathbb{Z}_n^*$.

This section explores such embeddings by leveraging the Chinese Remainder Theorem to lift a subgroup isomorphic to V_4 from a smaller unit group into the multiplicative semigroup $(\mathbb{Z}_n, \times)$, even when the image lies outside $\mathbb{Z}_n^*$.

Theorem 5.1 (Lifting V_4 Embeddings)**.** Let n, k, m be positive integers such that $n = km$ with k and m coprime. Let $\psi : \mathbb{Z}_n \to \mathbb{Z}_k \times \mathbb{Z}_m$ be the canonical ring isomorphism given by the Chinese Remainder Theorem, where

$$\psi(x) = (x \bmod k,\ x \bmod m).$$

for $x \in \mathbb{Z}_n$. Let $\pi_k : \mathbb{Z}_k \times \mathbb{Z}_m \to \mathbb{Z}_k$ be the projection onto the first component, where

$$\pi_k(a, b) = a,$$

for $a \in \mathbb{Z}_k$, $b \in \mathbb{Z}_m$. Let $\pi = \pi_k \circ \psi$ be the natural ring homomorphism $\pi : \mathbb{Z}_n \to \mathbb{Z}_k$, given by

$$\pi(x) = x \pmod k.$$

Suppose H is a subgroup of the multiplicative group of units $\mathbb{Z}_k^*$ such that $H \cong V_4$, the Klein four-group. Then, there exists a subgroup $\tilde{H}$ of the multiplicative semigroup $(\mathbb{Z}_n, \times)$ such that:

1. $\tilde{H}$ is isomorphic to V_4 (and thus $\tilde{H} \cong H$).
2. The restriction of the projection map π to $\tilde{H}$, denoted $\pi|_{\tilde{H}} : \tilde{H} \to H$, is a group isomorphism.
3. The elements of $\tilde{H}$ need not be units in $\mathbb{Z}_n$.

Proof. **Part 1**. Let $H \leq \mathbb{Z}_k^*$ be the subgroup $H \cong V_4$. Let $e_k = 1 \pmod k$ be the identity element in $\mathbb{Z}_k^*$ and H. Consider the element $c \in \mathbb{Z}_m$, let c be some fixed idempotent element, i.e., $c^2 \equiv c \pmod m$. (Note: $c = 0$ and $c = 1$ are always idempotents in $\mathbb{Z}_m$). Define the set $H'_{\text{pairs}} \subseteq \mathbb{Z}_k \times \mathbb{Z}_m$ as:

$$H'_{\text{pairs}} = \{(h, c) \mid h \in H\}$$

We claim that H'_{pairs} is a group under component-wise multiplication.

- **Identity:** The element $(e_k, c) \in H'_{\text{pairs}}$ acts as the identity. For any $(h, c) \in H'_{\text{pairs}}$:

  $$(e_k, c) \cdot (h, c) = (e_k h, c^2) = (h, c) \quad \text{and} \quad (h, c) \cdot (e_k, c) = (h e_k, c^2) = (h, c)$$

  this holds since c is idempotent.

- **Closure:** For $(h_1, c), (h_2, c) \in H'_{\text{pairs}}$:

  $$(h_1, c) \cdot (h_2, c) = (h_1 h_2, c^2) = (h_1 h_2, c)$$

  Since $h_1, h_2 \in H$, their product $h_1 h_2 \in H$ as H is a group. Thus, $(h_1 h_2, c) \in H'_{\text{pairs}}$.

- **Inverses:** Let $(h, c) \in H'_{\text{pairs}}$. Since $H \cong V_4$, every element $h \in H$ satisfies $h^2 = e_k$.

  $$(h, c) \cdot (h, c) = (h^2, c^2) = (e_k, c)$$

Thus, every element (h, c) is its own inverse, and the inverse exists within H'_{pairs}. Therefore, H'_{pairs} forms a subgroup of the multiplicative semigroup $(\mathbb{Z}_k \times \mathbb{Z}_m, \times)$.

We now show that $H'_{\text{pairs}} \cong H \cong V_4$. Define the map $\varphi : H \to H'_{\text{pairs}}$ by $\varphi(h) = (h, c)$.

- φ is a homomorphism: $\varphi(h_1h_2) = (h_1h_2, c) = (h_1h_2, c^2) = (h_1, c)(h_2, c) = \varphi(h_1)\varphi(h_2)$. Additionally, $\varphi(e_k) = (e_k, c)$.
- φ is injective: If $\varphi(h_1) = \varphi(h_2)$, then $(h_1, c) = (h_2, c)$, which implies $h_1 = h_2$.
- φ is surjective: By definition any $(h, c) \in H'_{\text{pairs}}$ has $h \in H$ and $\varphi(h) = (h, c)$.

Thus, φ is a group isomorphism, meaning $H'_{\text{pairs}} \cong H \cong V_4$.

Since $\psi : \mathbb{Z}_n \to \mathbb{Z}_k \times \mathbb{Z}_m$ is a ring isomorphism, its inverse $\psi^{-1} : \mathbb{Z}_k \times \mathbb{Z}_m \to \mathbb{Z}_n$ exists and is also a ring isomorphism (preserving multiplication). Define $\tilde{H}$ as the image of H'_{pairs} under ψ^{-1}, i.e.

$$\tilde{H} = \psi^{-1}(H'_{\text{pairs}}) = \{\psi^{-1}(h, c) \mid h \in H\}$$

Since ψ^{-1} is a multiplicative isomorphism, it maps the subgroup H'_{pairs} of $(\mathbb{Z}_k \times \mathbb{Z}_m, \times)$ to a subgroup $\tilde{H}$ of the multiplicative semigroup $(\mathbb{Z}_n, \times)$. Furthermore, $\tilde{H} \cong H'_{\text{pairs}}$, and therefore $\tilde{H} \cong H \cong V_4$.

Part 2. Consider the projection map $\pi : \mathbb{Z}_n \to \mathbb{Z}_k$, defined by $\pi(x) = x \pmod k$, which equals $\pi_k \circ \psi$. Let $\tilde{x} \in \tilde{H}$. Then $\tilde{x} = \psi^{-1}(h, c)$ for some unique $h \in H$. Applying π:

$$\pi(\tilde{x}) = \pi(\psi^{-1}(h, c)) = (\pi_k \circ \psi)(\psi^{-1}(h, c)) = \pi_k(\psi(\psi^{-1}(h, c))) = \pi_k(h, c) = h$$

This shows π maps $\tilde{x} \in \tilde{H}$ to the corresponding $h \in H$. The map $\pi|_{\tilde{H}} : \tilde{H} \to H$ acts as the inverse of the isomorphism $h \mapsto \psi^{-1}(h, c)$. Since $\pi|_{\tilde{H}}$ maps the elements $\psi^{-1}(h, c) \in \tilde{H}$ bijectively back to the corresponding elements $h \in H$, and π is a homomorphism, the restriction $\pi|_{\tilde{H}}$ is a group isomorphism.

Part 3. An element $\tilde{x} = \psi^{-1}(h, c) \in \mathbb{Z}_n$ is a unit if and only if its image $\psi(\tilde{x}) = (h, c)$ is a unit in $\mathbb{Z}_k \times \mathbb{Z}_m$, meaning $h \in \mathbb{Z}_k^*$ and $c \in \mathbb{Z}_m^*$. While $h \in \mathbb{Z}_k^*$ holds by hypothesis ($H \leq \mathbb{Z}_k^*$), we can choose an idempotent c that is not a unit in $\mathbb{Z}_m$. For example, if $m > 1$, in any case we will have the two trivial idempotents 0 and 1, since 1 is always a unit in $\mathbb{Z}_m$, we choose $c = 0 \pmod m$. Since 0 is not a unit, the elements $(h, 0)$ are not units in $\mathbb{Z}_k \times \mathbb{Z}_m$, and their preimages $\tilde{x} = \psi^{-1}(h, 0)$ in $\tilde{H}$ are not units in $\mathbb{Z}_n$. □

Remark 5.2. In summary, Theorem 5.1 shows that if $H \leq \mathbb{Z}_k^*$ is isomorphic to V_4, then by the Chinese Remainder Theorem we can lift H to a group $\tilde{H} \subseteq \mathbb{Z}_n$ (with $n = km$ and $\gcd(k, m) = 1$) satisfying $\tilde{H} \cong V_4$. This is achieved by choosing an idempotent $c \in \mathbb{Z}_m$ to form $H'_{\text{pairs}} = \{(h, c) : h \in H\} \subset \mathbb{Z}_k \times \mathbb{Z}_m$, and its image under the inverse CRT isomorphism $\psi^{-1} : \mathbb{Z}_k \times \mathbb{Z}_m \to \mathbb{Z}_n$ yields $\tilde{H} = \psi^{-1}(H'_{\text{pairs}})$. Also, even though $\tilde{H}$ is a group isomorphic to V_4, which of course has well defined inverses, it need not be a restricted to containing only elements of $\mathbb{Z}_n^*$. Moreover, the natural projection $\pi : \mathbb{Z}_n \to \mathbb{Z}_k$, defined by $\pi(x) = x \pmod k$, restricts to an isomorphism $\pi|_{\tilde{H}} : \tilde{H} \to H$. Thus, the lifting produces a copy of V_4 in $\mathbb{Z}_n$ that naturally corresponds to the original subgroup $H \leq \mathbb{Z}_k^*$.

Remark 5.3. Additionally, Theorem 5.1 tells us that there are as many such $\tilde{H}$ corresponding to a given H, as there are idempotent elements in $\mathbb{Z}_m$. Moreover, in any case we will always have at least one lifting (setting $c = 0$) that lies outside of the group of units $\mathbb{Z}_n^*$.

Example 5.4. Let us revisit our original Example (2.5) with our new found insights. Let $n = 24$ and choose $k = 8$ and $m = 3$. Note $\gcd(8, 3) = 1$ and $n = km$. The Chinese Remainder Theorem gives a

ring isomorphism $\psi : \mathbb{Z}_{24} \cong \mathbb{Z}_8 \times \mathbb{Z}_3$. Take $H = \mathbb{Z}_8^* = \{1, 3, 5, 7\}$. We know $H \cong V_4$. Let's choose the idempotent element $c = 0$ in $\mathbb{Z}_3$ and form the set of pairs $H'_{\text{pairs}} = \{(h, c) \mid h \in H\} \subseteq \mathbb{Z}_8 \times \mathbb{Z}_3$:

$$H'_{\text{pairs}} = \{(1, 0), (3, 0), (5, 0), (7, 0)\}$$

This H'_{pairs} forms a group isomorphic to $H \cong V_4$ under component-wise multiplication in $\mathbb{Z}_8 \times \mathbb{Z}_3$. The identity element is $(1, 0)$.

Now, we lift this back to $\mathbb{Z}_{24}$ using the inverse CRT map $\psi^{-1} : \mathbb{Z}_8 \times \mathbb{Z}_3 \to \mathbb{Z}_{24}$. We need to find $x \in \mathbb{Z}_{24}$ for each pair $(h, 0)$ such that $x \equiv h \pmod 8$ and $x \equiv 0 \pmod 3$.

$$\begin{aligned}
(1, 0) &\Rightarrow x \equiv 1 \pmod 8, \quad x \equiv 0 \pmod 3 \Rightarrow x = 9, \\
(3, 0) &\Rightarrow x \equiv 3 \pmod 8, \quad x \equiv 0 \pmod 3 \Rightarrow x = 3, \\
(5, 0) &\Rightarrow x \equiv 5 \pmod 8, \quad x \equiv 0 \pmod 3 \Rightarrow x = 21, \\
(7, 0) &\Rightarrow x \equiv 7 \pmod 8, \quad x \equiv 0 \pmod 3 \Rightarrow x = 15.
\end{aligned}$$

The resulting lifted group is $\tilde{H} = \{9, 3, 21, 15\}$. The identity element in $\tilde{H}$ is $9 = \psi^{-1}(1, 0)$. This is precisely of the form of our earlier Example (2.5) where we confirmed $\tilde{H} \cong V_4$.

Remark 5.5. The previous example explicitly shows a construction of V_4 within $(\mathbb{Z}_{24}, \times)$ whose elements are not in $\mathbb{Z}_{24}^*$ through choosing the idempotent $c = 0$, which is not a unit in $\mathbb{Z}_3$. If we chose $c = 1$, which is a unit modulo 3, this would not be the case. In fact we would have a subgroup of the group of units, namely: $\tilde{H} = \{1, 19, 13, 7\}$.

Example 5.6. Let $n = 60$. We choose $k = 12$ and $m = 5$. Note $\gcd(12, 5) = 1$ and $n = km$. We have the CRT isomorphism $\psi : \mathbb{Z}_{60} \cong \mathbb{Z}_{12} \times \mathbb{Z}_5$. The group of units $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ is isomorphic to V_4. Let $H = \mathbb{Z}_{12}^*$. Choose the idempotent $c = 0$ in $\mathbb{Z}_5$. Form the set of pairs $H'_{\text{pairs}} = \{(h, 0) \mid h \in H\} \subseteq \mathbb{Z}_{12} \times \mathbb{Z}_5$:

$$H'_{\text{pairs}} = \{(1, 0), (5, 0), (7, 0), (11, 0)\}$$

This forms a group isomorphic to V_4 with identity $(1, 0)$. Lift back to $\mathbb{Z}_{60}$ using ψ^{-1}. Find $x \in \mathbb{Z}_{60}$ such that $x \equiv h \pmod{12}$ and $x \equiv 0 \pmod 5$.

$$\begin{aligned}
(1, 0) &\Rightarrow x = 25, \\
(5, 0) &\Rightarrow x = 5, \\
(7, 0) &\Rightarrow x = 55, \\
(11, 0) &\Rightarrow x = 35.
\end{aligned}$$

The resulting lifted group is $\tilde{H} = \{25, 5, 55, 35\}$. The identity element in $\tilde{H}$ is $25 = \psi^{-1}(1, 0)$. Additionally notice that:

$$\begin{aligned}
5^2 = 25 &\equiv 25 \pmod{60}, \\
35^2 = 1225 &\equiv 25 \pmod{60}, \\
55^2 = 3025 &\equiv 25 \pmod{60}.
\end{aligned}$$

Since we know $\tilde{H}$ is a group of order 4 and each element is self inverse, the closure property of the group must yield that the product of any two non-identity elements generates the third. Altogether, we have that $\tilde{H} \cong V_4$. Again, these elements are not units in $\mathbb{Z}_{60}$ because $c = 0$ was chosen.

Let us now consider an example where we choose an idempotent element other than 0.

Example 5.7. Let $n = 120$. We choose $k = 8$ and $m = 15$. Note $\gcd(8, 15) = 1$ and $n = km$. We have the CRT isomorphism $\psi : \mathbb{Z}_{120} \cong \mathbb{Z}_8 \times \mathbb{Z}_{15}$. Let $H = \mathbb{Z}_8^* = \{1, 3, 5, 7\} \cong V_4$. The ring $\mathbb{Z}_{15}$ has idempotents other than 0 and 1. For example, $6^2 = 36 \equiv 6 \mod 15$. Let's choose the idempotent $c = 6$ in $\mathbb{Z}_{15}$. Form the set of pairs $H'_{\text{pairs}} = \{(h, 6) \mid h \in H\} \subseteq \mathbb{Z}_8 \times \mathbb{Z}_{15}$:

$$H'_{\text{pairs}} = \{(1, 6), (3, 6), (5, 6), (7, 6)\}$$

This forms a group isomorphic to V_4 with identity $(1, 6)$. We now lift back to $\mathbb{Z}_{120}$ using ψ^{-1}. We do so by finding $x \in \mathbb{Z}_{120}$ such that $x \equiv h \mod 8$ and $x \equiv 6 \mod 15$.

$$\begin{aligned}(1, 6) &\Rightarrow x = 81,\\ (3, 6) &\Rightarrow x = 51,\\ (5, 6) &\Rightarrow x = 21,\\ (7, 6) &\Rightarrow x = 111.\end{aligned}$$

The resulting lifted group is $\tilde{H} = \{81, 51, 21, 111\}$. The identity element in $\tilde{H}$ is $81 = \psi^{-1}(1, 6)$. Additionally notice that:

$$\begin{aligned}21^2 = 441 &\equiv 81 \pmod{120},\\ 51^2 = 2601 &\equiv 81 \pmod{120},\\ 111^2 = 12321 &\equiv 81 \pmod{120}.\end{aligned}$$

Similarly to our previous example, we know $\tilde{H}$ is a group of order 4 and each element is self inverse. Hence, $\tilde{H} \cong V_4$. Note that for all $\tilde{h} \in \tilde{H}$, $\gcd(\tilde{h}, 120) = 3 \neq 1$. This is preserved from our choice of idempotent $c = 6$ from $\mathbb{Z}_{15}$ with $\gcd(6, 15) = 3$. This example demonstrates using a non-trivial idempotent, $c \neq 0$, still results in a lifted group of non-units provided $\gcd(c, m) \neq 1$.

In this final example, we demonstrate how to lift multiple V_4 subgroups from a single modulus system to a larger one. By applying the same mapping approach, we obtain distinct constructions of $\tilde{H}$ in the multiplicative semigroup, depending on the choice of the original subgroup H.

Example 5.8. Let's reconsider our previous example with $n = 120$. But this time we choose $k = 24$ and $m = 5$. Note $\gcd(24, 5) = 1$ and $n = km$. We have the CRT isomorphism $\psi : \mathbb{Z}_{120} \cong \mathbb{Z}_{24} \times \mathbb{Z}_5$. Additionally, a quick calculation of Definition 4.1 with $s = 3$ (since $24 = 2^3 \cdot 3$) tells us that $\mathbb{Z}_{24}^*$ has $\frac{(2^3-1)(2^3-2)}{6} = 7$ unique V_4 subgroups. Let us define two such subgroups and lift them both. Let $H_1, H_2 \leq \mathbb{Z}_{24}^*$ and choose

$$\begin{aligned}H_1 &= \langle 5, 7\rangle = \{1, 5, 7, 11\} \cong V_4,\\ H_2 &= \langle 11, 13\rangle = \{1, 11, 13, 23\} \cong V_4.\end{aligned}$$

Choosing the trivial idempotent $c = 0$ from the ring $\mathbb{Z}_5$. Form two set of pairs $H'_{\text{pairs}} = \{(h_1, 0) \mid h_1 \in H_1\} \subseteq \mathbb{Z}_{24} \times \mathbb{Z}_5$ and $H''_{\text{pairs}} = \{(h_2, 0) \mid h_2 \in H_2\} \subseteq \mathbb{Z}_{24} \times \mathbb{Z}_5$:

$$\begin{aligned}H'_{\text{pairs}} &= \{(1, 0), (5, 0), (7, 0), (11, 0)\},\\ H''_{\text{pairs}} &= \{(1, 0), (11, 0), (13, 0), (23, 0)\}.\end{aligned}$$

Both form a group isomorphic to V_4 with identity $(1,0)$. We now lift back to $\mathbb{Z}_{120}$ using ψ^{-1}:

$$\begin{aligned}(1,0) &\Rightarrow x = 25,\\ (5,0) &\Rightarrow x = 5,\\ (7,0) &\Rightarrow x = 55,\\ (11,0) &\Rightarrow x = 35,\\ (13,0) &\Rightarrow x = 85,\\ (23,0) &\Rightarrow x = 95.\end{aligned}$$

The resulting lifted groups are $\tilde{H}_1 = \{25, 5, 55, 35\}$ and $\tilde{H}_2 = \{25, 35, 85, 95\}$. The identity element in both $\tilde{H}_1$ and $\tilde{H}_2$ is $25 = \psi^{-1}(1,0)$. Additionally, in a similar fashion to our previous examples both $\tilde{H}_1$ and $\tilde{H}_2$ can easily be verified to be isomorphic to V_4. Additionally, no element of either group is a unit modulo 120 since we chose $c = 0$ as our idempotent element from $\mathbb{Z}_5$, which of course lies outside the group of units modulo 5.

6 V_4's Relevance in Polynomial Solvability

The existence of a general formula for solving polynomial equations by radicals, like the quadratic formula, is not guaranteed for all degrees. While formulas exist for degrees 3 and 4, no analogous general formula exists for degree 5 or higher. This fundamental limitation is deeply connected to the algebraic structure of permutations of the polynomial's roots, specifically the solvability of its Galois group. To understand this connection, we first need the concept of a solvable group.

Definition 6.1 (Solvable Group)**.** A group G is called *solvable* if it has a normal series $\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_k = G$ such that each factor group G_{i+1}/G_i is abelian.

The bridge between polynomial equations and group theory is provided by Galois Theory [1], specifically the following fundamental theorem:

Theorem 6.2. A polynomial $f(x)$ is solvable by radicals if and only if its Galois group is solvable.

Proof. Omitted. This is a well known result that can be found in most Galois Theory textbooks. Alternatively for quick access one can view this proof in the following short report on Galois Theory and it's connection to radical polynomial solvability here [4]. □

It is a known result from Galois theory that the Galois group of the general polynomial of degree n (whose coefficients are indeterminates) over a field like $\mathbb{Q}$ is the symmetric group S_n. Therefore, Theorem 6.2 tells us that the general polynomial of degree n is solvable by radicals if and only if S_n is a solvable group. Our task now reduces to determining the solvability of S_n.

The solvability of S_n is intimately tied to the structure of its unique index 2 subgroup, the alternating group A_n. Since $S_n/A_n \cong \mathbb{Z}_2$, which is abelian, S_n is solvable if and only if A_n is solvable. A key property influencing solvability is whether a group is simple (has no non-trivial proper normal subgroups).

[1] For readers interested in further study, a working knowledge of Galois Theory can be obtained through a textbook such as 'A Course in Galois Theory' by Garling [3].

We note that $A_2 = \{e\}$ is trivial and $A_3 \cong \mathbb{Z}_3$ is cyclic (hence simple and solvable). The case $n = 4$ is special. For $n \geq 5$, however, A_n exhibits the property of simplicity. To establish the simplicity of A_n for $n \geq 5$, we use the following lemmas regarding 3-cycles.

Lemma 6.3. A_n is generated by 3-cycles.

Proof. First notice that if i, j, k are distinct, then

$$(ijk) = (ik)(ij) \in A_n,$$

so that A_n contains every 3-cycle. So it suffices to show that every product $\tau_1\tau_2$ of a pair of transpositions is a product of 3-cycles. If τ_1 and τ_2 are not disjoint, the computation above shows that their product is a 3-cycle. On the other hand, if $\tau_1 = (ij)$, $\tau_2 = (rs)$ with i, j, r, s distinct, then

$$\tau_1\tau_2 = (ij)(ir)(ri)(rs) = (jir)(irs).$$

□

Lemma 6.4. If $n \geq 5$, then all 3-cycles are conjugate in A_n.

Proof. Because of the identity

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)), \tag{18}$$

all cycles of any given length are conjugate in S_n. We must show that when $r = 3$, we can always take σ to be even. So let (ijk) and (rst) be 3-cycles, and choose $\sigma \in S_n$ so that $\sigma(ijk)\sigma^{-1} = (rst)$. If σ is even there's nothing to prove, so suppose σ is odd. Because $n \geq 5$, we can find $a, b \in \{1, 2, \ldots, n\}$ so that a, b, i, j, k are all distinct. Then (ab) commutes with (ijk), $\sigma(ab)$ is even and

$$(\sigma(ab))(ijk)(\sigma(ab))^{-1} = \sigma(ab)(ijk)(ab)\sigma^{-1} = \sigma(ijk)\sigma^{-1} = (rst).$$

□

Lemma 6.5. Suppose $n \geq 5$. If a normal subgroup N of A_n contains a 3-cycle, then $N = A_n$.

Proof. Let $N \triangleleft A_n$. If N contains a 3-cycle, normality implies N contains all of its conjugates in A_n. This means N contains every 3-cycle, by Lemma 6.4. Lemma 6.3 then tells us that $N = A_n$. □

These lemmas lead to the main theorem regarding the structure of A_n.

Theorem 6.6. If $n \neq 4$, then the alternating group A_n is simple.

Proof. (Sketch) The cases $n = 2$ and $n = 3$ were addressed earlier (A_2 is trivial, $A_3 \cong \mathbb{Z}_3$ is simple). Assume $n \geq 5$ and let $N \triangleleft A_n$ be a non-trivial normal subgroup. We need to show $N = A_n$. The standard proof involves showing that N must contain a 3-cycle. The provided proof sketch is standard: Choose $\sigma \in N, \sigma \neq e$, with the maximum number of fixed points. Consider $\tau = (a\,b\,c)$ for some a, b, c. Look at the commutator $\rho = \sigma\tau\sigma^{-1}\tau^{-1} \in N$. One shows that unless σ is a 3-cycle, ρ can be chosen to be non-identity and have more fixed points than σ, or σ^2 is a 3-cycle. This leads to a contradiction with the choice of σ, unless σ was already a 3-cycle. Assume the proof step that N must contain a 3-cycle. Then by Lemma 6.5, we conclude that $N = A_n$. Thus, for $n \geq 5$, A_n has no non-trivial proper normal subgroups and is simple. □

Remark 6.7. If one wishes to read a fully complete proof to the above sketch, it can be found in the following overview of alternating groups [5].

The case $n = 4$ is different. A_4 is not simple.

Proposition 6.8. The Klein four-group $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of the alternating group A_4.

Proof. The elements of V_4 consist of the identity and all permutations in S_4 with cycle structure $(2, 2)$. Conjugation within S_n (and thus within A_n) preserves cycle structure. Let $\sigma \in A_4$ and $v \in V_4$. Then $\sigma v \sigma^{-1}$ must have the same cycle structure as v. If $v = e$, $\sigma e \sigma^{-1} = e \in V_4$. If v has structure $(2, 2)$, then $\sigma v \sigma^{-1}$ also has structure $(2, 2)$. Since V_4 contains all elements of S_4 with this structure, $\sigma v \sigma^{-1}$ must be in V_4. Therefore, V_4 is closed under conjugation by elements of A_4, so $V_4 \triangleleft A_4$. □

Now we can determine the solvability of S_n for all relevant degrees $n \geq 2$.

Lemma 6.9. S_n is solvable if and only if n is of the form 2, 3 or 4.

Proof. Let's prove this by explicitly checking each case.

(Case $n = 2$): $S_2 \cong \mathbb{Z}_2$. This group is cyclic, hence abelian, and therefore solvable. The trivial normal series $\{e\} \triangleleft S_2$ has the single factor group $S_2/\{e\} \cong S_2$, which is abelian.

(Case $n = 3$): S_3 has order 6. The alternating group $A_3 \cong \mathbb{Z}_3$ is normal in S_3. We have the normal series $\{e\} \triangleleft A_3 \triangleleft S_3$. The factor groups are:

- $A_3/\{e\} \cong A_3 \cong \mathbb{Z}_3$, which is abelian.
- S_3/A_3. Since $|S_3| = 6$ and $|A_3| = 3$, the quotient group has order $6/3 = 2$. Thus $S_3/A_3 \cong \mathbb{Z}_2$, which is abelian.

Since all factor groups are abelian, S_3 is solvable.

(Case $n = 4$): We have the chain of subgroups $\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$. Let's examine the factor groups:

- $V_4/\{e\} \cong V_4$. V_4 is abelian ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2$).
- A_4/V_4. Since $|A_4| = 12$ and $|V_4| = 4$, the quotient group has order $12/4 = 3$. Any group of order 3 is isomorphic to $\mathbb{Z}_3$, which is abelian.
- S_4/A_4. Since $|S_4| = 24$ and $|A_4| = 12$, the quotient group has order $24/12 = 2$. Any group of order 2 is isomorphic to $\mathbb{Z}_2$, which is abelian.

Since all factor groups in this normal series are abelian, S_4 is solvable.

(Case $n \geq 5$): by Theorem 6.6, A_n is simple. A simple group is solvable if and only if it is abelian. However, for $n \geq 3$, A_n is non-abelian (e.g., in A_5, $(123)(124) = (13)(24)$ while $(124)(123) = (14)(23)$). Since A_n ($n \geq 5$) is simple and non-abelian, it is not solvable. Because A_n is a subgroup of S_n, if S_n were solvable, A_n would also have to be solvable (subgroups of solvable groups are solvable). Since A_n is not solvable, S_n cannot be solvable for $n \geq 5$. □

This brings us to the final conclusion regarding polynomial equations.

Theorem 6.10 (Abel-Ruffini)**.** The general polynomial of degree n is not solvable by radicals for $n \geq 5$.

Proof. Recall that the general polynomial of degree n, $f(x) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$, has Galois group S_n over the field $\mathbb{Q}(s_1, \ldots, s_n)$. By Theorem 6.2, this polynomial is solvable by radicals if and only if its Galois group, S_n, is solvable. As established by Lemma 6.9 above, S_n is solvable for $n \leq 4$, but it is not solvable for $n \geq 5$ (due to the non-abelian simplicity of A_n for $n \geq 5$). Therefore, the general polynomial of degree n is not solvable by radicals for $n \geq 5$. □

Ultimately, the existence of a general polynomial formula hinges on the solvability of the symmetric group S_n, which is determined by the structure of the alternating group A_n. While A_n is simple for $n = 3$ and $n \geq 5$, the case $n = 4$ is distinct. As demonstrated, V_4 is a normal subgroup of A_4, preventing A_4 from being simple. This allows the formation of the normal series $\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$, whose factor groups ($V_4$, $A_4/V_4 \cong \mathbb{Z}_3$, and $S_4/A_4 \cong \mathbb{Z}_2$) are all abelian. The existence of V_4 is thus the key feature enabling this decomposition into abelian factors, making S_4 solvable and permitting the quartic formula. For $n \geq 5$, the lack of such a non-trivial normal subgroup within the simple A_n makes S_n unsolvable, proving the Abel-Ruffini theorem.

7 Conclusions and Further Research

This project has explored the Klein four-group V_4, establishing it as the unique non-cyclic abelian group of order four. By analysing its intrinsic properties and examining its numerical constructions within $\mathbb{Z}_n$, we have demonstrated that V_4 not only serves as a fundamental example in group theory but also emerges naturally in various algebraic settings. Our approach, which leverages the Chinese Remainder Theorem to decompose $\mathbb{Z}_n^*$, has allowed us to characterise the precise conditions under which a subgroup isomorphic to V_4 exists and to derive an explicit formula for counting such embeddings in $\mathbb{Z}_n^*$. Additionally, we explored further embeddings in $\mathbb{Z}_n$ with images outside of $\mathbb{Z}_n^*$ and explored the role of V_4 in the existence of general formulae of solvability of quintic vs quartic polynomials. Beyond everything we have seen here, several directions emerge for future investigation:

Generalisations to Other Non-Cyclic Groups: A natural direction for further work is to extend the methods used for studying embeddings of V_4 to other small non-cyclic groups. A particularly interesting case is the elementary abelian 2-group of rank 3,

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

which is a non-cyclic abelian group of order 8. Just as we characterised and counted embeddings of V_4 in $\mathbb{Z}_n^*$ using the Chinese Remainder Theorem, one could determine the precise conditions under which a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ appears in $\mathbb{Z}_n^*$. This would involve analysing the unit group structure, identifying when it admits an elementary abelian 2-subgroup of rank 3, and deriving an explicit formula for counting such embeddings. The transition from order 4 to order 8 introduces new and interesting challenges to help deepen our knowledge of group structures and algebraic frameworks.

Geometric and Combinatorial Interpretations: Developing geometric models or combinatorial frameworks that illustrate the interplay between V_4 and symmetry groups may yield new insights into its applications in algebra and number theory. One possible direction is to examine the action of V_4 on geometric objects, such as tessellations or polytopes, where its structure naturally arises in the study of symmetry. Additionally, combinatorial constructions, such as Cayley graphs or lattice

embeddings, could offer alternative perspectives on how V_4 interacts with other algebraic structures. These approaches could reveal new structural properties of V_4 and provide a deeper understanding of its role in broader algebraic and number-theoretic contexts.

References

[1] David S. Dummit and Richard M. Foote. Introduction to Group Theory. In *Abstract Algebra*, chapter 1. John Wiley & Sons, 3rd edition, 2004.

[2] Kenneth Ireland and Michael Rosen. The structure of $U(\mathbb{Z}/n\mathbb{Z})$. In *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*, chapter 4, pages 39–49. Springer, 2nd edition, 1990.

[3] D. J. H. Garling. The theory of fields, and Galois theory. In *A Course in Galois Theory*, chapter 4. John Wiley & Sons, 1987.

[4] Mishal Mrinal. Galois theory and the Abel-Ruffini theorem, 2019. University of Chicago REU Program Paper. Accessed: March 25, 2025 Viewable here.

[5] R. C. Daileda. The alternating group. Accessed: March 27, 2025 Viewable here.