DEGREES OF SUMS OF ALGEBRAIC NUMBERS IN AN ABELIAN EXTENSION

DEAN CURETON, NATALIE DEERING, EBENEZER LOBE

August 2024

Abstract. The sum of two algebraic numbers is again algebraic. In this paper we investigate the possible degrees of the sum of two algebraic numbers α and β. We fully solve this problem in the abelian case, and we work out some examples in the non-abelian case.

Contents

1. Introduction

The study of polynomial equations and their roots has long been a central focus of mathematics. Galois theory was developed in the 19th century as a way to connect the structure of roots of polynomial equations—called algebraic numbers—with the symmetries of fields. In this paper, we concern ourselves with the question of the structure of sums of algebraic numbers, utilizing Galois theory to find our answer.

Definition 1.1. An **algebraic number** is a complex number α that is the root of some nonzero polynomial with rational coefficients.

Definition 1.2. If α is an algebraic number, there exists a unique monic, irreducible polynomial with rational coefficients with α as a root. This polynomial is called the **minimal polynomial** of α. The **degree** of α is defined as the degree of its minimal polynomial.

Definition 1.3. A Galois extension E/F is called an **abelian extension** if its Galois group is abelian.

This paper aims to answer the question of which degrees of sums of algebraic numbers are possible. In particular (since the degree of α is the same as the degree of $-\alpha$), we want to investigate which triples of numbers (a, b, c) are possible as degrees of algebraic numbers α, β, and γ such that $\alpha + \beta + \gamma = 0$.

Several other authors have made progress on this question. Isaacs [4] proved that if algebraic numbers α and β have coprime degrees m and n, then $\alpha + \lambda\beta$ has degree mn for any nonzero rational number λ (the paper also discusses this result in extensions of positive characteristic rather than characteristic zero). A paper by Drungilas, Dubickas, and Smyth [2] further investigates this question in depth and provides all examples of achievable triples where α and β are at most degree 6. Virbalas [6] expands on this work by completely determining the possible values for the degree of the compositum of two number fields of the same prime degree.

Our paper focuses specifically on answering this question in the context of abelian extensions, and we are able to fully answer it in this case.

Theorem 1.4. *Let a, b, c be positive natural numbers. There exist algebraic numbers α, β and γ satisfying $\alpha + \beta + \gamma = 0$ of degrees a, b and c respectively inside an abelian extension $K/\mathbb{Q}$ if and only if $a \mid bc$, $b \mid ac$ and $c \mid ab$.*

In order to construct these algebraic numbers, we require the foundational result that every finite abelian group is a Galois group of some field extension. As such, extending our results to the non-abelian case would seem to require further knowledge about the open "inverse Galois problem" that is not yet known.

2. Preliminaries

To begin, we offer some preliminary results about Galois extensions and symmetries of algebraic numbers.

Lemma 2.1. *Let $\alpha \in K/\mathbb{Q}$, a Galois extension with $G = \mathrm{Gal}(K/\mathbb{Q})$. The set of numbers of the shape $\sigma(\alpha)$ over $\sigma \in G$ are exactly the roots of the minimal polynomial of α. In particular, the degree of α is the size of the set $\{\sigma(\alpha) \mid \sigma \in G\}$. This is often stated as "the Galois group acts transitively on the roots of an irreducible polynomial."*

Proof. Consider the orbit of α under the action of G, $\mathrm{Orb}_G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$. The stabiliser of α, $\mathrm{Stab}_G(\alpha)$, consists of all elements of G that fix α. By the Orbit-Stabiliser Theorem,

$$|G| = |\mathrm{Orb}_G(\alpha)| \cdot |\mathrm{Stab}_G(\alpha)|$$

and since $K/\mathbb{Q}$ is Galois, we know that $|G| = [K : \mathbb{Q}]$.

Since α is algebraic over $\mathbb{Q}$, we can consider the ring of polynomials in α with rational coefficients as $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$. We know that $\deg(p) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Observe that $\mathrm{Stab}_G(\alpha)$ is precisely the Galois group of K over $\mathbb{Q}[\alpha]$. Now, for any $f(\alpha) \in \mathbb{Q}[\alpha]$, where f is a polynomial with rational coefficients, we have:

$$\sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\alpha)$$

So σ fixes every element of $\mathbb{Q}[\alpha]$. Conversely, if σ fixes every element of $\mathbb{Q}[\alpha]$, it must fix α since $\alpha \in \mathbb{Q}[\alpha]$. Therefore, $|\mathrm{Stab}_G(\alpha)| = [K : \mathbb{Q}[\alpha]] = [K : \mathbb{Q}(\alpha)]$.

By the multiplicativity of field extension degrees:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

Hence we have that

$$|\mathrm{Orb}_G(\alpha)| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(p)$$

This proves that the number of conjugates of α, or $|\mathrm{Orb}_G(\alpha)|$, is equal to the degree of its minimal polynomial.

To show that these conjugates are exactly the roots of $p(x)$, we argue:

- All conjugates of α are roots of $p(x)$, as $p(\sigma(\alpha)) = \sigma(p(\alpha)) = \sigma(0) = 0$ for any $\sigma \in G$.
- The number of conjugates equals the degree of $p(x)$, so these must be all the roots.

Thus, our proof demonstrates not only that the conjugates of α are the roots of its minimal polynomial, but also that the Galois group acts transitively on these roots. □

Lemma 2.2. *Let $\alpha, \beta \in K/\mathbb{Q}$, a Galois extension with $G = \mathrm{Gal}(K/\mathbb{Q})$. The number of elements of the set of pairs $\{(\sigma(\alpha), \sigma(\beta)) \mid \sigma \in G\}$ is equal to the degree of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$.*

Proof. Let $K/\mathbb{Q}$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$, and let $\alpha, \beta \in K$. The number of distinct pairs $\{(\sigma(\alpha), \sigma(\beta)) \mid \sigma \in G\}$ corresponds to the size of the orbit of the pair (α, β) under the action of G, which is given by $\frac{|G|}{|\mathrm{Stab}_G(\alpha,\beta)|}$, where $\mathrm{Stab}_G(\alpha,\beta)$ is the stabiliser of the (α,β) pair in G. $\mathrm{Stab}_G(\alpha,\beta)$ is exactly the group $\mathrm{Gal}(K/\mathbb{Q}(\alpha,\beta))$. Therefore the number of distinct pairs is $\frac{|G|}{|\mathrm{Stab}_G(\alpha,\beta)|} = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$. □

Definition 2.3. We say an algebraic number α is **abelian** if $\alpha \in K$ for some Galois extension $K/\mathbb{Q}$ with abelian Galois group.

Lemma 2.4. *The set of abelian algebraic numbers is a field.*

Proof. Let $\alpha \in K$ and $\beta \in K'$ be two abelian algebraic numbers, such that $K/\mathbb{Q}$ and $K'/\mathbb{Q}$ are abelian extensions. Consider the composite field $K'K$ over $\mathbb{Q}$: it is Galois over $\mathbb{Q}$ with Galois group isomorphic to a subgroup of the direct product $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K'/\mathbb{Q})$. (A proof of this fact can be found in Dummit & Foote Section 14.4, Proposition 21[3].) This direct product is abelian, so any subgroup is also abelian. The Galois group of $K'K$ over $\mathbb{Q}$ is then abelian, and α, β are both contained in a larger abelian extension field. Thus, $\alpha+\beta$ and $\alpha\beta$ are both contained in $K'K$, meaning that the set of algebraic numbers is closed under field operations and is therefore a field. □

Lemma 2.5. *If α, β are algebraic numbers of degrees m and n, then the degree of $\mathbb{Q}(\alpha,\beta)$ over $\mathbb{Q}$ is a multiple of both m and n, and less than or equal to mn.*

Proof. We have that α^i for $0 \le i < m$ is a basis for the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$; similarly, β^j for $0 \le j < n$ is a basis for $\mathbb{Q}(\beta)/\mathbb{Q}$. Then, the set $\{\alpha^i\beta^j\}$ spans the space $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$, and the degree of this field extension is therefore less than or equal to mn.

By the multiplicativity of degrees of field extensions, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]m$, so $m \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$. Similarly, $n \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$. Thus, m and n both divide $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$. □

Lemma 2.6. *Let α, β be two algebraic numbers over $\mathbb{Q}$, with conjugates $\{\alpha_i\}$ and $\{\beta_j\}$ respectively. If the sums $\alpha_i+\beta_j$ are distinct for all i, j, then $\mathbb{Q}(\alpha+\beta) = \mathbb{Q}(\alpha,\beta)$.*

Proof. Let K be the Galois closure of $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$. Suppose σ is an automorphism of K that fixes $\mathbb{Q}(\alpha,\beta)$. Then, $\sigma(\alpha)=\alpha$ and $\sigma(\beta)=\beta$. Therefore, $\sigma(\alpha+\beta)=\alpha+\beta$, and σ also fixes $\mathbb{Q}(\alpha+\beta)$.

Now, suppose σ is an automorphism of K that fixes $\mathbb{Q}(\alpha+\beta)$, such that $\alpha+\beta=\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$. Since σ permutes the roots of polynomials, $\sigma(\alpha)$ must be equal to α_i for some i, and $\sigma(\beta)=\beta_j$ for some j. So, $\sigma(\alpha+\beta)=\alpha_i+\beta_j=\alpha+\beta$. But, since the sums of the conjugates of α and β are distinct by assumption, we must have $\alpha_i = \alpha$ and $\beta_j = \beta$. Thus, $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = \beta$, so σ also fixes $\mathbb{Q}(\alpha, \beta)$.

We have shown that any automorphism of K fixes $\mathbb{Q}(\alpha, \beta)$ if and only if it fixes $\mathbb{Q}(\alpha + \beta)$; in other words, we have shown that $\mathrm{Gal}(K/\mathbb{Q}(\alpha, \beta)) = \mathrm{Gal}(K/\mathbb{Q}(\alpha + \beta))$. By the fundamental theorem of Galois theory, the group of automorphisms that fix a subfield determine the subfield. Since the group of automorphisms of K that fix $\mathbb{Q}(\alpha, \beta)$ and the group of automorphisms of K that fix $\mathbb{Q}(\alpha+\beta)$ are equal, we must have that the corresponding subfields are equal. Thus, $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$ and we are done. □

Finally, we present two fundamental results without proof.

Lemma 2.7. *For every finite abelian group G there exists a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) = G$.*

Proof. A proof can be found in Dummit & Foote Section 14.5, Corollary 28 [3]. □

Theorem 2.8 (Normal basis theorem)**.** *For every Galois extension $K/\mathbb{Q}$ there exists an element $\theta \in K$ such that the elements $\{\sigma(\theta) \mid \sigma \in G\}$ are a basis for $K/\mathbb{Q}$ as a vector space.*

Proof. A proof can be found in J.S. Milne's Fields and Galois Theory, page 68 [5]. □

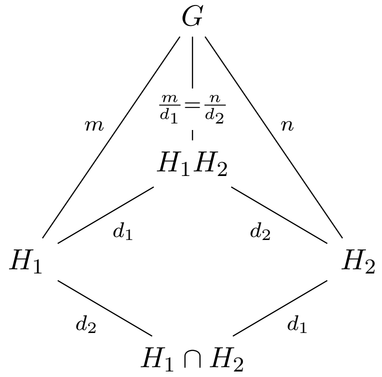
With these results, we can begin to answer questions about the sums of algebraic numbers. Importantly, note that $\mathbb{Q}(\alpha+\beta)$ is a subfield of $\mathbb{Q}(\alpha, \beta)$, meaning we can use results from Galois theory to investigate the degree of $\alpha + \beta$.

3. Proof of Main Theorem

We begin with a group-theoretic result that will be crucial in our analysis:

Lemma 3.1. *If G is a finite group, for subgroups H_1 and H_2 of index m and n where H_1 is normal, the possible indices of $H_1 \cap H_2 \subseteq G$ are precisely the natural numbers d such that $\mathrm{lcm}(m, n) \mid d \mid mn$. In particular, if G is abelian, the possible indices of $H_1 \cap H_2 \subseteq G$ are precisely the numbers d above.*

Proof. Since H_1 is normal, $H_1 H_2$ is a subgroup of G. By the second (diamond) isomorphism theorem, we have the following lattice of subgroups:



From this, we see that $[G : H_1 \cap H_2] = md_2 = nd_1$, so both m and n divide the index and thus $\text{lcm}(m, n)$ divides the index.

In addition, the index of H_1H_2 in G must be an integer, so d_1 must divide m and d_2 must divide n. Thus, nd_1 and md_2 must divide mn, but these are equal to $[G : H_1 \cap H_2]$. So, $[G : H_1 \cap H_2] \mid mn$ and we are done. □

This lemma provides insight into the structure of subgroup intersections, which we can apply to Galois theory due to the correspondence between subgroups of the Galois group and intermediate fields. We now translate this group-theoretic result into the language of field extensions:

Lemma 3.2. *Let $\alpha, \beta \in K$ where $K/\mathbb{Q}$ is an abelian extension. If $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree m and $\mathbb{Q}(\beta)/\mathbb{Q}$ has degree n, the possible degrees of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ are exactly the values of d with $\text{lcm}(m, n) \mid d \mid mn$.*

Proof. By the previous Lemma 3.1 and the duality of the lattice of subgroups of $\text{Gal}(K/\mathbb{Q})$ and the lattice of subfields of $\mathbb{Q}(\alpha, \beta)$, we must have that the possible degrees of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ are exactly the values of d with $\text{lcm}(m, n) \mid d \mid mn$.

We now shall show that any number d of the form above is achievable by some α and β given m and n. Let us begin by fixing some d such that $\text{lcm}(m, n) \mid d \mid mn$.

Let $H = C_{mn/d}$, the cyclic group of order mn/d. Then, let $H_1 = H \times C_{d/m} \cong C_n$, $H_2 = H \times C_{d/n} \cong C_m$, and $G = H_1 \times H_2 \cong C_{mn}$. We see that H_1 has index m in G, H_2 has index n in G, and $H = H_1 \cap H_2$ has index d in G.

By Lemma 2.7, there is some (abelian) Galois extension $K/\mathbb{Q}$ with (abelian) Galois group G. The fundamental theorem of Galois theory then tells us that there exist intermediate fields E_1 and E_2 between K and $\mathbb{Q}$ corresponding to the groups H_1 and H_2. By the primitive element theorem (see Dummit & Foote Section 14.4 Theorem 25 [3]), there exist α and β such that $E_1 = \mathbb{Q}(\alpha)$ and $E_2 = \mathbb{Q}(\beta)$; these numbers are necessarily algebraic since they generate finite extensions of $\mathbb{Q}$ (their Galois groups are finite). Then, the corresponding fixed field of the subgroup $H = H_1 \cap H_2$ is the composite of E_1 and E_2; namely, $\mathbb{Q}(\alpha, \beta)$. This field is Galois over $\mathbb{Q}$ since it is an intermediate field of an abelian extension. The degree $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is then equal to the index of $H_1 \cap H_2$ in G, which is exactly d. Thus, we have found algebraic numbers α and β of degrees m and n respectively such that $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ has degree d. □

Now, we demonstrate a property of Galois conjugates to further our understanding of the behavior of algebraic numbers:

Lemma 3.3. *The difference of two Galois conjugates of an algebraic number cannot be rational.*

Proof. Let $\alpha = \alpha_1$ be an algebraic number contained in a Galois extension $K/\mathbb{Q}$, and let $\{\alpha_i \mid 1 \leq i \leq n\}$ be the finite set of its Galois conjugates. Suppose $\alpha_k - \alpha_\ell = \theta$ for $1 \leq k, \ell \leq n$ where θ is rational (and clearly nonzero); without loss of generality, assume θ is positive. The Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set $\{\alpha_i\}$, so choose $\sigma \in G$ to be the automorphism that sends α_ℓ to the conjugate of α with the largest real part—call it α_r. Then, $\sigma(\alpha_k - \alpha_\ell) = \sigma(\theta) = \theta$, since θ is rational. But now, $\sigma(\alpha_k - \alpha_\ell) = \sigma(\alpha_k) - \sigma(\alpha_\ell) = \sigma(\alpha_k) - \alpha_r$, and $\alpha_r + \theta = \sigma(\alpha_k)$. Thus, $\sigma(\alpha_k)$ has larger real part than α_r, contradicting our choice of σ. This proves the lemma. □

With this result in hand, we can now prove a key lemma about the degree of the sum of two algebraic numbers with coprime degrees:

Lemma 3.4. *Let α and β be algebraic numbers of degree m and n, each inside an abelian extension of $\mathbb{Q}$. If $gcd(m, n) = 1$ then the degree of $\alpha + \beta$ is mn.*

Proof. By Lemma 2.5, we see that the degree of $\mathbb{Q}(\alpha, \beta)$ must be exactly mn. Then, by Lemma 2.6, if the sums of conjugates of α and β are distinct, then $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$ and the degree of $\alpha + \beta$ is equal to the degree $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$.

We first note that both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are Galois over $\mathbb{Q}$, as they are intermediate fields of an abelian extension. Suppose $\alpha_i + \beta_j = \alpha_k + \beta_\ell$, where α_i, α_k are conjugates of α and β_j, β_ℓ are conjugates of β. Let $\theta = \alpha_i - \alpha_k = \beta_\ell - \beta_j$. Since $\mathbb{Q}(\alpha)$ is Galois, every conjugate of α is in this field and thus θ is in the field as well. Similarly, $\theta \in \mathbb{Q}(\beta)$. By the multiplicativity of degrees, we must have then that the degree of θ divides both of m and n. However, since $\gcd(m, n) = 1$, the degree of θ must be 1 and θ is therefore rational. By Lemma 3.3, the difference $\alpha_i - \alpha_k$ cannot be rational, a contradiction. Therefore, the sums of conjugates are distinct, and the degree of $\alpha + \beta$ is mn. □

It is worth noting that the above result also holds for non-abelian algebraic numbers; this was proven by Isaacs [4]. The proof requires representation theory, and we do not concern ourselves with it in this paper.

We now have a powerful tool for constructing algebraic numbers with specific degrees. We thus can extend this result to consider triples of algebraic numbers that sum to zero:

Lemma 3.5. *Let $K/\mathbb{Q}$ be an abelian extension, and assume there exist $\alpha, \beta, \gamma \in K/\mathbb{Q}$ satisfying $\alpha + \beta + \gamma = 0$, of degrees a, b and c respectively. Similarly, let $K'/\mathbb{Q}$ be abelian and let $\alpha', \beta', \gamma' \in K/\mathbb{Q}$ satisfying $\alpha'+\beta'+\gamma' = 0$, of degrees a', b' and c' respectively. If $gcd(abc, a'b'c') = 1$, there exists an abelian extension $K''/\mathbb{Q}$ and $\alpha'', \beta'', \gamma'' \in K''$ satisfying $\alpha'' + \beta'' + \gamma'' = 0$, of degrees aa', bb' and cc'.*

Proof. Let K'' be the composite field $K'K$, and let $\alpha'' = \alpha + \alpha', \beta'' = \beta + \beta'$, and $\gamma'' = \gamma + \gamma'$. By Lemma 2.4, $\alpha'', \beta'', \gamma''$ are contained in $K'K$, which is an abelian extension of $\mathbb{Q}$. Note that $\alpha''+\beta''+\gamma'' = (\alpha+\beta+\gamma)+(\alpha'+\beta'+\gamma') = 0$. Since $\gcd(a, a') = \gcd(b, b') = \gcd(c, c') = 1$, by Lemma 3.4, α'' has degree aa', β'' has degree bb', and γ'' has degree cc'. We are done. □

To complete our toolkit, we need one final result about algebraic numbers of prime power degrees:

Lemma 3.6. *If p is a prime number and s, t, and u are nonnegative integers with $s \leq t + u$, $t \leq s + u$ and $u \leq t + s$, then there exist α, β and γ inside an abelian extension $K/\mathbb{Q}$ satisfying $\alpha + \beta + \gamma = 0$, of degrees p^s, p^t and p^u respectively.*

Proof. Let G be defined as follows;

$$G = H_A \times H_B \times H_C,$$

where

$$H_A = C_{p^a}$$
$$H_B = C_{p^b}$$
$$H_C = C_{p^c},$$

with a, b, c as nonnegative integers to be chosen later. By Lemma 2.7, there exists a Galois extension $K/\mathbb{Q}$ such that its Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is G. By the normal basis theorem (Theorem 2.8), we can find $\theta \in K$ such that $\sigma(\theta)$'s are all linearly independent, and hence construct α, β as follows:

$$\alpha = \sum_{\sigma \in H_A} \sigma(\theta) \text{ and } \beta = \sum_{\sigma \in H_B} \sigma(\theta)$$

Observe that α is exactly fixed by the automorphisms in H_A: for $\tau \in$ G,

$$\tau(\alpha) = \sum_{\sigma \in H_A} \tau \circ \sigma(\theta) = \sum_{\sigma \in \tau(H_A)} \sigma(\theta),$$

while $\alpha = \sum_{\sigma \in H_A} \sigma(\theta)$, so

$$\alpha = \tau(\alpha) \iff H_A = \tau(H_A) \iff \tau \in H_A.$$

the same idea applying to $\tau(\beta)$. Hence,

$$G_\alpha = H_A \text{ and } G_\beta = H_B,$$

where $G_\alpha = \{\sigma \in G : \sigma(\alpha) = \alpha\}$ and $G_\beta = \{\sigma \in G : \sigma(\beta) = \beta\}$ are the subgroups of G that fix α and β respectively. Therefore, we have that

$$\deg(\alpha) = \frac{|G|}{|G_\alpha|} = \frac{p^{a+b+c}}{p^a} = p^{b+c} \text{ and}$$
$$\deg(\beta) = \frac{|G|}{|G_\beta|} = \frac{p^{a+b+c}}{p^b} = p^{a+c}.$$

Now we compute the degree of $\gamma = -(\alpha + \beta)$. We have $\deg(\gamma) = \deg(-(\alpha + \beta)) = \deg(\alpha + \beta)$. But

$$\begin{aligned}\alpha + \beta &= \sum_{\sigma \in H_A} \sigma(\theta) + \sum_{\sigma \in H_B} \sigma(\theta) \\ &= \sum_{\sigma \in H_A \cap H_B} 2\sigma(\theta) + \sum_{\sigma \in (H_A \cup H_B) \setminus H_A \cap H_B} \sigma(\theta).\end{aligned}$$

For some automorphism $\tau \in G$,

$$\begin{aligned}\tau(\alpha + \beta) &= \sum_{\sigma \in H_A \cap H_B} 2\tau \circ \sigma(\theta) + \sum_{\sigma \in (H_A \cup H_B) \setminus H_A \cap H_B} \tau \circ \sigma(\theta) \\ &= \sum_{\sigma \in \tau(H_A \cap H_B)} 2\sigma(\theta) + \sum_{\sigma \in \tau[(H_A \cup H_B) \setminus H_A \cap H_B]} \sigma(\theta).\end{aligned}$$

Suppose that $\tau(\alpha + \beta) = \alpha + \beta$. Looking at the terms with coefficient 2:

$$\sum_{\sigma \in \tau(H_A \cap H_B)} 2\sigma(\theta) = \sum_{\sigma \in H_A \cap H_B} 2\sigma(\theta),$$

implying that τ maps $H_A \cap H_B$ onto itself, i.e., $\tau(H_A \cap H_B) = H_A \cap H_B$. For this to be true, we must have $\tau \in H_A \cap H_B$. Conversely, suppose $\tau \in H_A \cap H_B$. Then, $\tau(\alpha) = \alpha$ (because $\tau \in H_A$) and $\tau(\beta) = \beta$ (because $\tau \in H_B$). Therefore $\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta) = \alpha + \beta$, and hence:

$$\tau(\alpha+\beta) = \alpha+\beta \iff \tau \in H_A \cap H_B.$$

Therefore

$$G_\gamma = H_A \cap H_B = \{e\},$$

since the subgroup intersection is precisely $\{(x, e_{H_B}, e_{H_C}) \mid x \in H_A\} \cap \{(e_{H_A}, y, e_{H_C}) \mid y \in H_B\} = \{(e_{H_A}, e_{H_B}, e_{H_C})\}$ where these are the identities of the subgroups H_A, H_B, H_C respectively. Now,

$$\deg(\alpha+\beta) = \deg(\gamma) = \frac{|G|}{|G_\gamma|} = \frac{p^{a+b+c}}{1} = p^{a+b+c},$$

so we have

$$\begin{aligned}\deg(\alpha) &= p^{b+c} = p^s\\ \deg(\beta) &= p^{a+c} = p^t\\ \deg(\gamma) &= p^{a+b+c} = p^u.\end{aligned}$$

Now it suffices to find a, b, c such that:

$$\begin{aligned}b + c &= s\\ a + c &= t\\ a + b + c &= u.\end{aligned}$$

Solving the system above gives:

$$\begin{aligned}a &= u - s\\ b &= u - t\\ c &= t + s - u.\end{aligned}$$

Choosing u to be the largest of the exponents ($u = a + b + c$), we can always find *nonnegative* $a, b, c \in \mathbb{Z}$ which obey the above. □

With these lemmas established, we are now ready to prove our main theorem. The proof will utilize the tools we've developed to construct triples of algebraic numbers with the desired properties, and show that these are the only possible configurations in abelian extensions.

Theorem 1.4. *Let a, b, c be positive natural numbers. There exist algebraic numbers α, β and γ satisfying $\alpha+\beta+\gamma = 0$ of degrees a, b and c respectively inside an abelian extension $K/\mathbb{Q}$ if and only if $a \mid bc$, $b \mid ac$ and $c \mid ab$.*

Proof. We shall demonstrate the reverse direction first; suppose $a \mid bc$, $b \mid ac$, and $c \mid ab$. Let p be some prime, and let e_a, e_b, e_c be the largest integers such that $p^{e_a} \mid a$, $p^{e_b} \mid b$, and $p^{e_c} \mid c$. In this case, we must have $p^{e_a} \mid bc = p^{e_b}p^{e_c}\frac{bc}{p^{e_b}p^{e_c}}$. Since $\frac{bc}{p^{e_b}p^{e_c}}$ is an integer not divisible by p, we must have $p^{e_a} \mid p^{e_b+e_c}$, so $e_a \leq e_b + e_c$. Similarly, $e_b \leq e_a + e_c$ and $e_c \leq e_a + e_b$. Now, by Lemma 3.6, there exist $\alpha_p, \beta_p, \gamma_p$ inside an abelian extension $K_p/\mathbb{Q}$ satisfying $\alpha_p + \beta_p + \gamma_p = 0$ of degrees $p^{e_a}, p^{e_b}, p^{e_c}$ respectively.

We can repeat this process for all primes p dividing one of a, b, and c, obtaining a collection of triples $\{\alpha_p, \beta_p, \gamma_p\} \subset K_p/\mathbb{Q}$ satisfying the above. Now, since powers of different primes are coprime, we may progressively apply Lemma 3.5 to pairs of triples in the collection to obtain α, β, γ inside an abelian extension $K/\mathbb{Q}$ satisfying $\alpha+\beta+\gamma = 0$ of degrees $\prod_p p^{e_a}, \prod_p p^{e_b}$, and $\prod_p p^{e_c}$ respectively. But these products are precisely a, b and c by our definitions of e_a, e_b, and e_c. This proves the reverse direction.

We shall now show the forward direction: suppose α, β, γ are algebraic numbers satisfying $\alpha + \beta + \gamma = 0$ of degrees a, b, and c respectively inside an abelian extension $K/\mathbb{Q}$. By symmetry, we must only demonstrate that $c \mid ab$. We know that $\mathbb{Q} \subset \mathbb{Q}(\alpha + \beta) \subset \mathbb{Q}(\alpha, \beta)$, and by Lemma 3.2, we know that $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ must have degree dividing ab. By the multiplicativity of degrees, we also know that $\mathbb{Q}(\alpha + \beta)$ must have degree diving ab as well. Now, we know that the degree of γ is equal to the degree of $-\gamma = \alpha + \beta$; thus, the degree of γ, which is c, must divide ab and we are done. □

4. The Non-Abelian Case

If we allow the algebraic numbers to be non-abelian there are several additional constructions we can make. For example, some possible triples of degrees for α, β and γ are $(3, 3, 6)$ and $(4, 4, 6)$. These examples are not possible in the abelian case because the divisibility condition in Theorem 1.4 is not satisfied.

Note that Lemma 2.5 still holds in non-abelian extensions: if α, β are contained in a Galois extension $K/\mathbb{Q}$, $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree m, and $\mathbb{Q}(\beta)/\mathbb{Q}$ has degree n, the degree of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ must be some d with $\operatorname{lcm}(m, n) \mid d \leq mn$. Thus, the degree of $\alpha + \beta$ must be a divisor of some multiple of $\operatorname{lcm}(m, n)$. Beyond this fact, our proofs rely heavily on Lemma 2.7, of which a generalization is not known for non-abelian groups (the so-called "inverse Galois problem).

Despite this, we are still able to demonstrate some elementary examples of triples that are only possible in the non-abelian case. In particular, we will show that it is possible to find triples α, β and γ of degrees $(n, n, n(n-1))$, which includes the $(3,3,6)$ case, or $(n,n,\frac{n(n-1)}{2})$, which includes the $(4,4,6)$ case.

Lemma 4.1. *Let f be an irreducible degree n polynomial, and let $\alpha_1,\dots,\alpha_n$ be the roots of n. Suppose that the action of Galois group on the set of roots is 2-transitive (meaning for every $i_1 \neq j_1, i_2 \neq j_2 \in \{1,\dots,n\}$ there is some $\sigma \in G$ where $\sigma(\alpha_{i_1}) = \alpha_{i_2}, \sigma(\alpha_{j_1}) = \alpha_{j_2}$). Then*

(i) The degree of $\alpha_i + 2\alpha_j$ is $n(n-1)$.

Further, if we assume the Galois group is the symmetric group S_n we have:

(ii) The degree of $\alpha_i - \alpha_j$ is $n(n-1)$.

(iii) The degree of $\alpha_i + \alpha_j$ is $\frac{n(n-1)}{2}$.

Lemma 4.2. *Suppose a monic, irreducible polynomial $f \in \mathbb{Q}[x]$ has two roots α_1 and α_2 where $\alpha_2/\alpha_1 \in \mathbb{Q}$. Then $\alpha_2/\alpha_1 \in \{1,-1\}$.*

Proof. Since f is irreducible, it is the minimal polynomial of α_1. If $m = \alpha_2/\alpha_1$, then α_1 is a root of $f(mx)$, since $f(m\alpha_1) = f(\alpha_2) = 0$. Then α_1 is a root of the polynomial $f(x) - \frac{f(mx)}{m^k}$, where k is the degree of f. If m is rational, this polynomial has rational coefficients and degree less then f. Since f is the minimal polynomial of α_1, $f(x) - \frac{f(mx)}{m^k}$ must be the zero polynomial. By plugging in $x=0$, we see that $f(0) - \frac{f(0)}{m^k} = f(0)(1-\frac{1}{m^k}) = 0$. Since f is irreducible $f(0) \neq 0$. This means $m^k = 1$ which means $|m| = 1$. Since m is real, $m = 1$ or -1, as desired. □

Proof of Lemma 4.1. We begin with case *(i)*. Let us verify that for distinct ordered pairs $(i_1,j_1),(i_2,j_2)$,

$$\alpha_{i_1} + 2\alpha_{j_1} \neq \alpha_{i_2} + 2\alpha_{j_2}$$

Suppose by contradiction that $\alpha_{i_1} + 2\alpha_{j_1} = \alpha_{i_2} + 2\alpha_{j_2}$. Then

$$\alpha_{i_1} - \alpha_{i_2} = 2(\alpha_{j_2} - \alpha_{j_1}) = -2(\alpha_{j_1} - \alpha_{j_2})$$

Because $i_1 = i_2 \iff j_1 = j_2$, we have $i_1 \neq i_2$ and $j_1 \neq j_2$. Since the action of G is 2-transitive we can find a $\sigma \in G$ where $\sigma(\alpha_{i_1}) = \alpha_{j_1}$ and $\sigma(\alpha_{i_2}) = \alpha_{j_2}$; here, $\sigma(\alpha_{i_1} - \alpha_{i_2}) = \alpha_{j_1} - \alpha_{j_2}$, so $\alpha_{i_1} - \alpha_{i_2}$ and $\alpha_{j_1} - \alpha_{i_2}$ are conjugates. However the quotient, $\frac{\alpha_{i_1} - \alpha_{i_2}}{\alpha_{j_1} - \alpha_{j_2}} = -2$, is rational but not equal to 1 or -1, which contradicts Lemma 4.2. We conclude that $\alpha_{i_1} + 2\alpha_{j_1} = \alpha_{i_2} + 2\alpha_{j_2}$ implies $(i_1,j_1) = (i_2,j_2)$, so the elements of the form $\alpha_i + 2\alpha_j$ are distinct. From the action of G being 2-transitive, we know that elements of this form (where $i \neq j$) are conjugates. So each $\alpha_i + 2\alpha_j$ has exactly $n(n-1)$ distinct conjugates. Using Lemma 2.1 we see that this implies the degree of $\alpha_i + 2\alpha_j$ is $n(n-1)$.

Consider now case *(ii)*. We begin similarly: suppose $\alpha_{i_1} - \alpha_{j_1} = \alpha_{i_2} - \alpha_{j_2}$ for distinct ordered pairs $(i_1, j_1), (i_2, j_2)$ where $i_1 \neq j_1$ and $i_2 \neq j_2$. Then, $\alpha_{i_1} + \alpha_{j_2} = \alpha_{j_1} + \alpha_{i_2}$. Without loss of generality, we can say that $j_2 \neq i_1$ and $j_2 \neq j_1$ by distinctness of the ordered pairs. Since the Galois group is the full symmetric group, there exists an automorphism σ that fixes $\alpha_{i_1}, \alpha_{j_1}$, and α_{i_2}, but not α_{j_2}. Applying this automorphism to both sides of the equation above, we arrive at a contradiction. Thus, $\alpha_{i_1} - \alpha_{j_1} = \alpha_{i_2} - \alpha_{j_2}$ implies $(i_1, j_1) = (i_2, j_2)$, and elements of the form $\alpha_i - \alpha_j$ are distinct. By a similar argument to case *(i)*, we see that elements of this form have $n(n-1)$ conjugates, so the degree of $\alpha_i - \alpha_j$ is $n(n-1)$.

For case *(iii)*, note that the above gives that $\alpha_{i_1} + \alpha_{i_2} = \alpha_{j_1} + \alpha_{j_2}$ implies $\{i_1, i_2\} = \{j_1, j_2\}$ where these are sets rather than ordered pairs. Thus, elements of the form $\alpha_i + \alpha_j$ are distinct up to a reordering of i and j. Elements of this form therefore have degree $\frac{n(n-1)}{2}$. □

Importantly, there exist polynomials of every degree with full symmetric group as Galois group (see Dummit & Foote page 649 [3]). Thus, the triples $(n, n, n(n-1))$ and $(n, n, \frac{n(n-1)}{2})$ are always achievable for every n.

4.1. **Example: (3, 3, 6).** We proceed using the strategy of case *(i)* of Lemma 4.1.

Let $\alpha = \sqrt[3]{2}$, and let β be a conjugate of 2α. Both α and β have degree 3, as they are roots of the irreducible cubics $x^3 - 2$ and $x^3 - 16$ respectively. Note that β must be of the form $2\omega\sqrt[3]{2}$, where ω is a root of $\frac{x^3-1}{x-1} = x^2+x+1$.

We now want to show that $\gamma = \alpha + \beta$ is of degree 6. Let G be the Galois group of the splitting field of $x^3 - 2$; then, by transitivity (Lemma 2.1), there exists some $\sigma \in G$ such that $\sigma(\alpha) = \omega\alpha$ and thus $2\sigma(\alpha) = \beta$.

Since α is the only real root of $x^3 - 2$, $\sigma(\alpha)$ is a solution of an irreducible quadratic in $\mathbb{Q}(\alpha)[x]$; thus, $[\mathbb{Q}(\alpha, \sigma(\alpha)) : \mathbb{Q}(\alpha)] = 2$. Since there are 2 conjugates of α that are not equal to itself, we can deduce that the action of the Galois group on the roots of $x^3 - 2$ is 2-transitive. Now, using 4.1, this implies that the degree of $\alpha + 2\sigma(\alpha)$, which is just $\alpha + \beta$, is equal to 6. We are done.

4.2. **Example: (4, 4, 6).** We now may utilize case *(iii)*.

We start with the following degree 4 polynomial:

$$f(x) = x^4 - x - 1.$$

We shall show that if α and β are distinct roots of f, then α and β are of degree 4 and $\alpha + \beta$ is of degree 6. This can be deduced by computing the

Galois group of f, which is S_4 [1], but we will use a direct computation to obtain the degree of the numbers.

To begin, given a monic polynomial with integer coefficients and roots $\alpha_1, \ldots, \alpha_k$, the polynomial

$$\prod_{1 \leq i < j \leq k} (x - (\alpha_i + \alpha_j))$$

also has integer coefficients; this follows from an argument of symmetric polynomials. In particular, for $f(x) = x^4 - x - 1 = (x-a)(x-b)(x-c)(x-d)$,

$$g(x) = (x-(a+b))(x-(a+c))(x-(a+d))(x-(b+c))(x-(b+d))(x-(c+d))$$

also has integer coefficients.

Using a numerical approximation, we find that $g(x) = x^6 + 4x^2 - 1$. If we now show that f and g are irreducible, we will have demonstrated that the degrees of α and β are 4 and the degree of $\alpha + \beta$ is 6.

We begin with the irreducibility of f. Consider $\bar{f} = x^4 - x - 1 \in \mathbb{F}_2[x]$. Note that $\bar{f}(0) = \bar{f}(1) = 1$, so this polynomial has no roots in $\mathbb{F}_2$ and must split into two irreducible quadratics if it is not irreducible itself. The only irreducible quadratic in $\mathbb{F}_2[x]$ is the polynomial $x^2 + x + 1$, and its square is $x^4 + x^2 + 1 \neq x^4 - x - 1$. Thus, $\bar{f}$ is irreducible in $\mathbb{F}_2[x]$, meaning f is irreducible in $\mathbb{Z}[x]$ and also in $\mathbb{Q}[x]$ by Gauss' lemma.

Let us now show that $g(x)$ is irreducible. We have $g(x) = h(x^2)$ where $h(y) = y^3 + 4y - 1$. Here, h is irreducible, since it has degree 3 and no rational roots (using the rational root theorem).

Let g_1 be a factor of g and α be a root of g_1 (so that it is also a root of g). Since α^2 is a root of h, we know that $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 3$ (since h is irreducible). We also have that $\mathbb{Q}(\alpha) \supset \mathbb{Q}(\alpha^2) \supset \mathbb{Q}$, which implies that the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a multiple of 3. So, the only way g can be reducible is if it is a the product of two degree 3 polynomials, g_1 and g_2.

Now we finish with an argument over $\mathbb{F}_3[x]$. Since $\mathbb{F}_3$ is a field, $\mathbb{F}_3[x]$ is a principal ideal domain and thus a unique factorization domain.

Notice that $h(2) \equiv 0 \bmod 3$. So $(x - 2)$ is a factor of $h(x)$ mod 3, which makes $(x^2 - 2)$ a factor of $g(x)$ over $\mathbb{F}_3[x]$. If we assume g is reducible and thus $g = g_1 g_2$ by the above, then this same factorization still holds over $\mathbb{F}_3[x]$. Because 2 is not a square mod 3, $x^2 - 2$ is irreducible over $\mathbb{F}_3[x]$. So $x^2 - 2$ has to divide either g_1 or g_2. But then $\frac{g_i}{x^2-2}$ is a linear factor of $g(x)$ over $\mathbb{F}_3[x]$, which is impossible since it can be verified g has no roots in $\mathbb{F}_3$. Therefore, $g(x)$ must be irreducible.

In conclusion, we have shown that the triple $(4, 4, 6)$ is achievable by distinct roots of the polynomial $x^4 - x - 1$.

Acknowledgments. The authors would like to thank Rodrigo Sanches Angelo for his invaluable mentorship during this project, and Dr. Lernik Asserian and the Stanford University Research Institute in Mathematics (SURIM) 2024 program for the opportunity to conduct this research.

References

[1] K. Conrad, *Galois groups of cubics and quartics (not in characteristic 2)*. `https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf`. Accessed: 2024-08-30.

[2] P. Drungilas, A. Dubickas, and C. Smyth, *A degree problem for two algebraic numbers and their sum*, Publicacions Matemàtiques, (2012), pp. 413 – 448.

[3] D. S. Dummit and R. M. Foote, *Abstract algebra*, Wiley, New York, 3rd ed., 2004.

[4] I. M. Isaacs, *Degrees of sums in a separable field extension*, Proceedings of the American Mathematical Society, 25 (1970), pp. 638–641.

[5] J. S. Milne, *Fields and Galois theory (v5.10)*, 2022. Available at `www.jmilne.org/math/`.

[6] P. Virbalas, *Compositum of two number fields of prime degree*, New York Journal of Mathematics, 29 (2023), pp. 171–192.